PUBLIC (PUBLIQUE)

Plateforme SAP BusinessObjects Business Intelligence

Version du document : 4.3 Support Package 4 – 2023-12-07

Guide d'administration de la plateforme de Business Intelligence

© 2024 SAP SE ou société affiliée SAP. Tous droits réservés.

THE BEST RUN SAP

Contenu

1 Historique du document. 21

2 Démarrage. 23

2.1 A propos de ce guide. 23

Public concerné par ce guide. 23

A propos de la plateforme de Business Intelligence. 23

Variables. 24

Terminologie. 24

2.2 Avant de commencer. 26

Notions clés. 26

Outils d'administration clés. 29

Tâches clés. 32

3 Architecture. 35

3.1 Présentation de l'architecture. 35

Schéma des composants. 36

Niveaux d'architecture. 37

Bases de données. 38

Serveurs, hôtes et clusters. 39

Serveurs d'applications Web. 40

Kits de développement logiciel. 45

Sources de données. 47

Authentification et connexion unique. 48

Intégration SAP. 49

Contrôle de version intégrée. 50

3.2 Serveurs, services, nœuds et hôtes. 51

Modifications des serveurs depuis la version XI 3.1. 53

Services. 55

Catégories de service. 61

Types de serveurs. 64

Serveurs. 68

3.3 Applications client. 70

Installées avec les outils client de la plateforme SAP BusinessObjects Business Intelligence 71

Installées avec la plateforme SAP BusinessObjects Business Intelligence. 73

Disponibles séparément. 74

Clients d'applications Web. 75

3.4 Workflows de traitement. 78
Démarrage et authentification. 78
Objets de programme. 80
Crystal Reports. 81
Web Intelligence. 85
Analysis. 87
3.5 Intégration à la barre de lancement SAP Fiori sur le SAP Enterprise Portal. 88

4 Assistant de configuration du système. 90
4.1 Introduction à l'Assistant de configuration du système. 90
4.2 Indication des produits utilisés. 90
4.3 Sélection d'un modèle de déploiement. 92
4.4 Indication des emplacements des dossiers de données. 94
4.5 Révision des modifications. 95
4.6 Fichiers journaux et fichiers de réponse. 96
Utilisation d'un fichier de réponse. 96

5 Gestion des licences. 101
5.1 Gestion des clés de licence. 101
Pour afficher les informations de licence. 101
Pour ajouter une clé de licence. 101
Pour visualiser l'activité du compte actuel. 102

6 Gestion des utilisateurs et des groupes. 103
6.1 Présentation de la gestion des comptes. 103
Gestion des utilisateurs. 103
Gestion des groupes. 104
Types d'authentification disponibles. 105
6.2 Gestion des comptes Enterprise et des comptes généraux. 106
Pour créer un compte d'utilisateur. 106
Pour modifier un compte d'utilisateur. 107
Pour supprimer un compte d'utilisateur. 108
Pour créer un groupe. 109
Pour modifier les propriétés d'un groupe. 109
Pour afficher les membres d'un groupe. 109
Pour ajouter des sous-groupes. 110
Pour définir l'appartenance à un groupe. 110
Pour supprimer un groupe. 111
Pour ajouter des utilisateurs ou groupes d'utilisateurs en bloc. 111
Pour activer le compte Guest. 112
Ajout d'utilisateurs à des groupes. 112
Modification des paramètres de mot de passe. 114

Octroi d'un droit d'accès à des utilisateurs et à des groupes. 116
Contrôle de l'accès aux boîtes de réception des utilisateurs. 116
Configuration des options de la zone de lancement BI façon Fiori. 117
Gestion des attributs des utilisateurs système 120
Classement des attributs utilisateur entre plusieurs options d'authentification. 121
Pour ajouter un nouvel attribut utilisateur. 122
Modifications des attributs utilisateur personnalisés. 123
6.3 Gestion des alias. 124
Pour créer un utilisateur et ajouter un alias tiers. 124
Pour créer un alias pour un utilisateur existant. 124
Pour affecter un alias d'un autre utilisateur. 125
Pour supprimer un alias. 126
Pour désactiver un alias. 126

7 Définition des droits. 128
7.1 Fonctionnement des droits sur la plateforme de BI. 128
Niveaux d'accès. 128
Définition de droits avancés. 129
Héritage. 130
Droits spécifiques au type. 135
Détermination des droits effectifs. 136
7.2 Gestion des paramètres de sécurité des objets dans la CMC. 137
Pour visualiser les droits d'un utilisateur ou groupe principal sur un objet. 138
Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet 138
Pour modifier les droits d'un utilisateur ou groupe principal sur un objet. 139
Définition des droits sur un dossier de niveau supérieur dans la plateforme de BI. 140
Vérification des paramètres de sécurité pour un utilisateur ou un groupe principal. 140
7.3 Utilisation des niveaux d'accès. 143
Choisir entre les niveaux d'accès *Visualiser* et *Visualiser à la demande*. 145
Pour copier un niveau d'accès existant. 146
Pour créer un niveau d'accès 146
Pour renommer un niveau d'accès. 147
Pour supprimer un niveau d'accès. 147
Pour modifier les droits d'un niveau d'accès. 147
Suivi de la relation entre niveaux d'accès et objets. 148
Gestion des niveaux d'accès sur différents sites. 149
7.4 Rupture de l'héritage. 150
Désactiver l'héritage. 151
7.5 Utilisation des droits pour déléguer l'administration. 152
Choisir entre les options « *Modifier les droits des utilisateurs sur les objets* ». 153
Droits de propriétaire. 155

7.6 Récapitulatif des recommandations concernant l'administration des droits. 155

8 Sécurisation de la plateforme de BI. 157

8.1 Présentation de la sécurité 157

8.2 Utilisation sécurisée des objets de programme. 157

8.3 Planification de récupération d'urgence. 158

8.4 Recommandations générales pour la sécurité de votre déploiement. 159

8.5 Configuration de la sécurité pour les serveurs tiers fournis. 160

8.6 Relation de confiance active. 160

Jetons de connexion. 160

Système de ticket pour la sécurité distribuée. 161

8.7 Sessions et suivi de session. 162

Suivi de session du CMS. 162

Gestion des sessions. 163

Script permettant d'effacer les sessions obsolètes. 164

8.8 Protection de l'environnement. 164

Du navigateur Web au serveur Web. 165

Serveur Web vers la plateforme de BI. 165

Protection contre les tentatives de connexion malveillantes. 165

Restrictions relatives aux mots de passe. 166

Restrictions relatives aux connexions. 166

Restrictions relatives aux utilisateurs. 166

Restrictions relatives au compte Guest. 167

8.9 Audit des modifications de la configuration de sécurité 167

8.10 Extensions de traitement. 167

8.11 Interface d'analyse anti-virus. 168

Activation de l'analyse anti-virus. 168

8.12 Sécurité des données de la plateforme de BI. 169

Modes de sécurité du traitement des données. 169

Comptes Administrateur. 172

Droits de connexion. 172

8.13 Cryptographie sur la plateforme de BI. 173

Utilisation de clés de cluster. 174

Agents de cryptographie. 176

Gestion des clés de cryptage dans la CMC. 177

8.14 Protection et confidentialité des données. 181

Glossaire. 182

Consentement de l'utilisateur. 183

Rapport d'informations. 184

Journalisation d'accès en lecture. 184

Suppression des données personnelles. 185

Journal des modifications. 186

8.15 Configuration des serveurs principaux pour SSL. 186
Pour créer le fichier de configuration par défaut. 187
Création de fichiers de clé et de certificat. 188
Configuration de SSL lorsque le certificat est géré par une autorité de certification. 190
Configuration du protocole SSL. 192
8.16 Description de la communication entre les composants de la plateforme de BI. 197
Présentation des serveurs de la plateforme de BI et des ports de communication. 197
Communication entre les composants de la plateforme de BI 200
8.17 Configuration de la plateforme de BI pour les pare-feu. 211
Pour configurer le système pour des pare-feu. 211
Débogage d'un déploiement équipé d'un pare-feu. 214
8.18 Exemples de scénarios classiques de pare-feu. 216
Exemple - Niveau application déployé sur un réseau distinct. 216
Exemple : Client lourd et niveau base de données séparés des serveurs de la plateforme de BI par un pare-feu. 218
8.19 Paramètres de pare-feu pour les environnements intégrés. 220
Instructions propres au pare-feu pour l'intégration SAP. 221
Configuration du pare-feu pour l'intégration JD Edwards EnterpriseOne. 223
Instructions propres au pare-feu pour Oracle EBS. 224
Configuration du pare-feu pour l'intégration PeopleSoft Enterprise. 225
Configuration du pare-feu pour l'intégration Siebel. 227
8.20 Plateforme de BI et serveurs proxy inverses 228
Description du déploiement des applications Web. 228
8.21 Configuration des serveurs proxy inverses pour les applications Web de la plateforme de Business Intelligence. 229
Instructions détaillées relatives à la configuration des serveurs proxy inverses. 229
Pour configurer le serveur proxy inverse. 230
Pour configurer le serveur proxy inverse Apache 2.2 pour la plateforme de BI 230
Pour configurer le serveur proxy inverse WebSEAL 6.0 pour la plateforme de BI 231
Pour configurer Microsoft ISA 2006 pour la plateforme de BI 232
8.22 Configuration spéciale de la plateforme de BI dans les déploiements de serveurs proxy inverses 234
Activation du proxy inverse pour les services Web. 234
Activation du chemin racine des cookies de session pour ISA 2006. 236
Activation du proxy inverse pour SAP BusinessObjects Live Office. 238

9 Authentification. 240
9.1 Options d'authentification dans la plateforme de BI. 240
Authentification primaire. 240
Plug-ins de sécurité. 241
Connexion unique à la plateforme de BI. 242
9.2 Authentification Enterprise. 245

Présentation de l'authentification Enterprise. 245
Paramètres d'authentification Enterprise. 245
Modification des paramètres d'Enterprise. 247
Authentification SAML 2.0. 248
Pour établir une authentification sécurisée entre SAP NetWeaver Java Application Server et la plateforme de BI. 261
Pour utiliser l'authentification SAML 2.0 avec SAP NetWeaver Java Application Server. 265
Activation de l'authentification sécurisée. 265
Configuration de l'authentification sécurisée pour l'application Web. 268
9.3 Authentification LDAP. 277
Utilisation de l'authentification LDAP. 277
Configuration de l'authentification LDAP. 279
Mappage des groupes LDAP. 291
9.4 Authentification Windows AD. 301
Utilisation de l'authentification Windows AD. 301
Préparation du contrôleur de domaine. 302
Configuration de l'authentification AD dans la CMC. 303
Configuration du service de la plateforme de BI pour l'exécution du SIA. 311
Configuration du serveur d'applications Web pour l'authentification AD. 314
Configuration de la connexion unique. 323
Dépannage de l'authentification Windows AD. 340
9.5 Authentification SAP. 342
Configuration de l'authentification SAP 342
Création d'un compte utilisateur pour la plateforme de BI. 343
Connexion aux systèmes d'autorisation de SAP. 344
Définition des options d'authentification SAP. 346
Importation de rôles SAP. 350
Configuration de la communication réseau sécurisée (SNC). 354
Configuration de la connexion unique au système SAP. 368
Configuration de la connexion unique pour SAP Crystal Reports et SAP NetWeaver. 372
9.6 Authentification PeopleSoft. 373
Présentation. 373
Activation de l'authentification PeopleSoft Enterprise. 373
Mappage de rôles PeopleSoft à la plateforme de BI. 374
Planification de mises à jour utilisateur. 377
Utilisation de la passerelle de sécurité PeopleSoft. 379
9.7 Authentification JD Edwards. 389
Présentation générale. 389
Activation de l'authentification JD Edwards EnterpriseOne. 389
Mappage de rôles JD Edwards EnterpriseOne à la plateforme de BI. 390
Planification de mises à jour utilisateur. 392

9.8 Authentification Siebel. . . . 394
Activation de l'authentification Siebel. . . . 394
Mappage de rôles à la plateforme de BI. . . . 395
Planification de mises à jour utilisateur. . . . 398
9.9 Authentification Oracle EBS. . . . 400
Activation de l'authentification Oracle EBS. . . . 400
Mappage de rôles Oracle E-Business Suite à la plateforme de BI. . . . 401
Démappage de rôles . . . 405
Personnalisation des droits pour les groupes et utilisateurs Oracle EBS mappés . . . 406
Configuration de la connexion unique pour SAP Crystal Reports et Oracle EBS. . . . 407
9.10 Authentification X.509. . . . 408
Authentification X.509 pour la zone de lancement BI. . . . 408
Authentification X.509 pour les services Web. . . . 416
Authentification X.509 pour la CMC. . . . 419
9.11 Authentification OpenID Connect. . . . 422
Activation de l'authentification OpenID Connect. . . . 422

10 Référence de la source de données. . . . 423
10.1 Mappage des références de connexion étendu. . . . 423
Création d'une référence de la source de données. . . . 424
Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la CMC. . . . 425
Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la zone de lancement BI. . . . 425
Définition des références de connexion à une base de données par rapport à une référence de la source de données pour un groupe. . . . 426
Association d'une référence de la source de données à la connexion OLAP. . . . 427

11 Administration du serveur. . . . 428
11.1 Utilisation de la zone de gestion Serveurs de la CMC. . . . 428
11.2 Gestion des serveurs à l'aide de scripts sous Windows . . . 431
11.3 Gestion des serveurs sous Unix . . . 431
11.4 Affichage et modification du statut d'un serveur. . . . 431
Visualisation de l'état des serveurs. . . . 431
Démarrage, arrêt et redémarrage d'un serveur. . . . 433
Arrêt d'un Central Management Server. . . . 435
Activation et désactivation de serveurs. . . . 436
11.5 Ajout, clonage ou suppression de serveurs. . . . 437
Ajout, clonage et suppression de serveurs. . . . 437
11.6 Ajout d'en-têtes Internet personnalisés. . . . 440
11.7 Mise en cluster de Central Management Servers. . . . 441
Mise en cluster de Central Management Servers. . . . 441
11.8 Gestion des groupes de serveurs. . . . 446

Création d'un groupe de serveurs. 447
Conversion d'un groupe de serveurs exclusif en groupe de serveurs non exclusif et vice versa. 449
Utilisation des sous-groupes de serveurs. 450
Modification de l'appartenance d'un serveur à un groupe. 451
Accès en administration à un serveur ou à un groupe de serveurs accordé aux utilisateurs 452
Mappage d'un groupe d'utilisateurs à un groupe de serveurs. 454
Mappage d'un dossier à un groupe de serveurs. 457
Présentation de la gestion des droits sur le groupe de serveurs. 459
11.9 Configuration des serveurs de traitement adaptif (APS, Adaptive Processing Servers) pour les systèmes de production. 464
11.10 Évaluation des performances du système. 465
Surveillance des serveurs de la plateforme de BI. 465
Analyse des performances du serveur. 465
Affichage des performances du système. 466
Journalisation des activités du serveur. 466
11.11 Configuration des paramètres des serveurs. 467
Pour modifier les propriétés d'un serveur. 468
Pour appliquer les paramètres de service à plusieurs serveurs. 468
Utilisation des modèles de configuration. 469
11.12 Configuration des paramètres réseau du serveur. 471
Options d'environnement réseau. 472
Options d'identification de l'hôte du serveur 472
Configuration d'un ordinateur multi-résident. 474
Configuration des numéros de port. 477
11.13 Gestion des nœuds. 480
Utilisation des nœuds. 480
Ajout d'un nœud. 482
Recréation d'un nœud. 487
Suppression d'un nœud. 490
Renommer un nœud. 493
Déplacement d'un nœud. 495
Paramètres de script. 499
Ajout des dépendances de serveurs Windows. 504
Modification des références de connexion utilisateur pour un nœud. 504
11.14 Renommage d'un ordinateur dans un déploiement de plateforme de BI. 505
Modification du nom des clusters. 505
Modification des adresses IP. 505
Renommage des ordinateurs. 507
11.15 Utilisation des bibliothèques tierces 32 bits et 64 bits avec la plateforme de BI. 510
11.16 Gestion des espaces réservés de nœuds et de serveurs. 511

Visualisation des espaces réservés de serveur. 511
Visualisation et modification des espaces réservés d'un nœud. 511

12 Gestion des bases de données du Central Management Server (CMS). 513
12.1 Gestion des connexions à la base de données système du CMS. 513
Sélection de SQL Anywhere comme base de données du CMS. 513
Sélection de SAP HANA comme base de données du CMS. 514
12.2 Sélection d'une base de données CMS (nouvelle ou existante). 515
Pour sélectionner une base de données de CMS nouvelle ou existante sous Windows. 517
Pour sélectionner une base de données de CMS nouvelle ou existante sous UNIX. 517
12.3 Recréation de la base de données système du CMS. 518
Pour recréer la base de données système du CMS sous Windows. 518
Pour recréer la base de données système du CMS sous UNIX. 519
12.4 Copie de données d'une base de données système d'un CMS dans une autre. 520
Préparation de la copie d'une base de données système du CMS. 521
Pour copier une base de données système du CMS sous Windows. 522
Copie de données d'une base de données système du CMS sous UNIX. 522
12.5 Pilote de base de données du CMS (Central Management Server). 523

13 Gestion des serveurs conteneurs d'applications Web (WACS). 524
13.1 WACS. 524
Serveur conteneur d'applications Web (WACS). 524
Ajout ou suppression de serveurs WACS à votre déploiement. 527
Ajout ou suppression de services aux serveurs WACS. 530
Configuration HTTPS/SSL. 532
Méthodes d'authentification prises en charge. 536
Configuration d'AD Kerberos pour un serveur WACS 536
Configuration de la connexion unique Kerberos AD 544
Configuration des services Web RESTful. 546
Configuration des serveurs WACS dans votre environnement informatique. 556
Configuration des propriétés d'applications Web. 559
Dépannage. 560
Propriétés des serveurs WACS. 564

14 Sauvegarde et restauration de votre système. 565
14.1 Présentation de la sauvegarde et de la restauration. 565
14.2 Terminologie. 565
14.3 Cas d'utilisation de la sauvegarde et de la restauration. 567
14.4 Sauvegardes. 568
Sauvegarde du système entier. 569
Sauvegarde des paramètres du serveur. 572
Sauvegarde du contenu BI. 575

14.5 Restauration du système. . . . 576
Restauration de votre système entier. . . . 576
Restauration des paramètres de serveur. . . . 583
Restauration du contenu BI. . . . 586
14.6 Scripts BackupCluster et RestoreCluster. . . . 586

15 Copie de votre déploiement de la plateforme de BI. . . . 590
15.1 Présentation de la copie du système. . . . 590
15.2 Terminologie. . . . 590
15.3 Cas d'utilisation de la copie du système. . . . 591
15.4 Planification de la copie du système. . . . 591
15.5 Remarques et restrictions. . . . 592
15.6 Procédure de copie de système. . . . 594
Pour exporter depuis un système source. . . . 594
Pour importer dans un système cible. . . . 598

16 Gestion des promotions. . . . 602
16.1 Bienvenue dans la gestion des promotions. . . . 602
Présentation. . . . 602
Fonctionnalités. . . . 602
Droits d'accès à l'application. . . . 603
Prise en charge de WinAD dans la gestion des promotions. . . . 604
16.2 Introduction à l'outil de gestion des promotions. . . . 604
Accès à l'outil de gestion de la promotion. . . . 604
Composants de l'interface utilisateur. . . . 605
Utilisation de l'option Paramètres. . . . 607
16.3 Utilisation de l'outil de gestion des promotions. . . . 614
Création et suppression de dossiers. . . . 615
Permet de créer un travail. . . . 616
Pour créer un travail en copiant un travail existant. . . . 619
Pour rechercher un travail. . . . 619
Pour modifier un travail. . . . 620
Pour ajouter un InfoObject à un travail. . . . 621
Pour gérer les dépendances d'un travail. . . . 622
Pour rechercher des objets dépendants. . . . 623
Promotion d'un travail quand les référentiels sont connectés. . . . 624
Promotion d'un travail à l'aide d'un fichier LCMBIAR. . . . 627
Pour planifier une promotion de travail. . . . 630
Pour afficher l'historique d'un travail. . . . 632
Pour reprendre un travail. . . . 632
16.4 Promotion du contenu d'un référentiel entier à l'aide de l'outil de gestion des promotions. . . . 635
Préparation des systèmes source et cible. . . . 635

Stratégies de migration. 637
16.5 Étapes de promotion d'un système entier. 638
Pour promouvoir les utilisateurs et les groupes d'utilisateurs (Travail 1). 638
Pour promouvoir des objets dépendants (Travail 2). 639
Pour promouvoir des objets principaux (Travail 3). 640
Post-promotion. 641
16.6 Utilisation de l'option Ligne de commande. 641
Pour exécuter l'outil de ligne de commande sous Windows. 642
Pour exécuter l'outil de ligne de commande sous Unix. 643
Paramètres d'outil de ligne de commande. 643
Exemple de fichier de propriétés. 667
16.7 Utilisation du CTS (Change and Transport System) amélioré. 668
Prérequis. 668
Pour configurer la plateforme de BI et l'intégration CTS+. 669
Pour promouvoir un travail à l'aide de CTS. 676
16.8 Utilisation de l'assistant de gestion des promotions 679
Exclusion d'objets de la promotion. 680
Quand utiliser l'assistant de gestion des promotions. 681
Scénario. 682
Objets. 684
Dépendances. 688
Résumé. 689
(Facultatif) Fichier des propriétés. 690
Assistant de gestion des promotions sous Linux. 693

17 Gestion des versions. 694
17.1 Pour gérer différentes versions d'un InfoObject. 694
Droits d'accès à l'application de la gestion des versions. 694
Sauvegarde et restauration des fichiers Subversion. 695
17.2 Gestion de différentes versions de ressources BI. 696
17.3 Démarrage et arrêt manuels de Subversion sous Unix. 698
17.4 Fichiers requis pour Subversion sous Solaris 10 et RedHat Linux 5. 698
17.5 Utilisation de Apache SubVersion comme système de gestion des versions. 698
17.6 Utilisation de Git comme système de gestion des versions. 699
17.7 Paramètres du système de gestion des versions par défaut. 700
17.8 Comparaison de différentes versions du même travail. 701
17.9 Mise à niveau du contenu de SubVersion. 701
17.10 Configuration de Subversion pour les Job Server de traitement groupés. 702
Option A : configurer l'ordinateur Subversion principal avant de réaliser une opération du système de gestion des versions. 702
Option B : configurer Subversion après la création d'un répertoire de copie de travail par le système de gestion des versions. 703

Configuration d'autres ordinateurs Subversion. 704

18 Gestion des applications. 705

18.1 Désactivation du message pop-up RGPD. 705

18.2 Gestion des applications via la CMC. 707

Présentation. 707

Paramètres courants pour les applications. 708

Paramètres spécifiques aux applications. 710

18.3 Gestion des applications à l'aide des propriétés de la couche sémantique. 770

18.4 Gestion des applications via les propriétés du fichier BOE.war. 771

Fichier war BOE. 771

18.5 Personnalisation des points d'entrée de connexion de la zone de lancement BI et OpenDocument 789

Emplacements des fichiers Zone de lancement BI et OpenDocument. 789

Pour définir une page de connexion personnalisée. 790

Pour ajouter l'authentification sécurisée à la connexion. 791

18.6 Personnalisation des interfaces utilisateur d'application. 792

Web Intelligence. 792

Zone de lancement BI. 798

18.7 Configuration des services Web RESTful de la plateforme de BI sur le serveur Web. 799

18.8 Gestion hybride des utilisateurs. 802

18.9 Mise en service de vos utilisateurs sur site dans SAP Analytics Cloud. 803

Établissement de la connexion entre le système sur site et le Cloud. 803

18.10 Création des références de connexion du client OAuth dans SAP Analytics Cloud. 805

18.11 Configuration du système source. 805

18.12 Configuration du système cible. 807

18.13 Mise en service de vos utilisateurs et groupes d'utilisateurs pour SAP Analytics Cloud. 807

18.14 Visualisation d'utilisateurs mis en service dans SAP Analytics Cloud. 808

18.15 Modèles d'exemple. 808

19 Gestion des connexions et des univers. 813

19.1 Gestion des connexions. 813

Pour supprimer une connexion d'univers. 813

19.2 Gestion des univers. 814

Pour supprimer des univers. 814

20 Studio d'administration BI. 816

20.1 Cockpit d'administration. 817

Cockpit d'administration. 817

BI et Serveurs. 818

BI sur des instances de document. 819

Utilisateurs et sessions dans BI. 820

BI et Utilisation du contenu. 820

BI et Applications. 821
20.2 Surveillance. 821
Terminologie de la surveillance. 822
Configuration de la prise en charge de la base de données pour la surveillance. 826
Propriétés de configuration. 834
Intégration à d'autres applications. 841
Prise en charge de cluster pour serveur de surveillance. 842
Dépannage. 842
20.3 Différence visuelle. 846
Comparaison d'objets ou de fichiers à l'aide de la différence visuelle. 846
Comparaison d'objets ou de fichiers à l'aide du système de gestion des versions. 847
20.4 Autorisation des éléments HTML. 848
Pour modifier la liste des éléments HTML autorisés. 851

21 Reporting du CMS. 852
21.1 Reporting du CMS. 852
Architecture de la plateforme SAP BusinessObjects. 852
Structure de la base de données système du CMS. 853
À propos des InfoObjects. 855
21.2 Aperçu du reporting du CMS. 857
21.3 Connexion de la base de données du CMS. 858
21.4 Kit d'exemples de reporting du CMS. 859
Importation du kit d'exemples de reporting du CMS avec l'outil de gestion des promotions. 860
Exemple d'univers du CMS 861
Extension de l'exemple d'univers du CMS. 861
21.5 Création d'un rapport sur le CMS. 861

22 Assistant du workflow. 863
22.1 Public visé. 864
22.2 Compréhension de l'architecture. 865
22.3 Glossaire. 866
22.4 À propos de l'installation et de la mise à jour. 868
22.5 Configuration de l'Assistant du workflow. 869
Configuration de base. 869
22.6 Gestion des droits d'Assistant du workflow via la Central Management Console. 871
22.7 Utilisation de l'Assistant du workflow. 877
À propos des modèles de tâche standard. 877
À propos des modèles de workflow standard. 888
À propos des modèles de tâche personnalisés. 888
Gestion de modèles de workflow. 889
Gestion de scénarios et affichage des résultats. 890
Explication des états des modèles de tâche, modèles de workflow et scénarios. 896

Utilisation de Systèmes. . . . 898
Flux de processus de bout en bout de l'Assistant du workflow. . . . 901
22.8 Vérification des fichiers journaux. . . . 901

23 Corbeille. . . . 902
23.1 Corbeille. . . . 902
Restauration d'un élément de la corbeille. . . . 902
Suppression définitive des éléments de la corbeille. . . . 903
Activation du nettoyage automatique de la Corbeille. . . . 903

24 Audit. . . . 905
24.1 Présentation. . . . 905
24.2 Page Audit de la CMC. . . . 911
Statut de l'audit. . . . 912
Configuration des événements d'audit. . . . 913
Paramètres de configuration des magasins de données d'audit. . . . 917
24.3 Evénements d'audit. . . . 919
Audit events and details. . . . 928

25 Événements. . . . 950
25.1 À propos des événements. . . . 950
Notifications d'utilisateur. . . . 951

26 Recherche de plateformes. . . . 955
26.1 Description de la recherche de plateformes. . . . 955
SDK de recherche de plateformes. . . . 955
Environnement en cluster. . . . 956
26.2 Installation de la recherche de plateformes. . . . 956
Déploiement d'OpenSearch. . . . 956
Configuration du proxy inverse. . . . 958
Configuration des propriétés de l'application dans la CMC. . . . 958
26.3 Utilisation de la recherche de plateformes. . . . 966
Indexation de contenu dans le référentiel CMS. . . . 966
Liste d'échecs d'indexation. . . . 967
Recherche des résultats. . . . 968
26.4 Intégration de la recherche de plateformes à SAP NetWeaver Enterprise Search. . . . 974
Création d'un connecteur dans SAP NetWeaver Enterprise Search . . . 974
Importation du rôle d'un utilisateur dans la plateforme de BI. . . . 975
26.5 Recherche depuis SAP NetWeaver Enterprise Search. . . . 976
26.6 Audit. . . . 976
26.7 Dépannage. . . . 977
Auto-guérison. . . . 977
Scénarios de problèmes. . . . 978

27 Fédération. 980
27.1 Fédération. 980
27.2 Terminologie Fédération. 981
27.3 Gestion des droits de sécurité. 983
Droits requis sur le site d'origine. 983
Droits requis sur le site de destination. 984
Droits spécifiques à Fédération. 985
Réplication de la sécurité sur un objet. 986
Réplication de la sécurité à l'aide des niveaux d'accès.. 987
27.4 Options de types et de mode de réplication. 987
Réplication unidirectionnelle 987
Réplication bidirectionnelle 988
Actualiser à partir du site d'origine ou Actualiser à partir de la destination. 988
27.5 Réplication d'utilisateurs et de groupes tiers. 990
27.6 Réplication des univers et des connexions d'univers. 991
27.7 Gestion des listes de réplication. 992
Création de listes de réplication. 993
Modification des listes de réplication. 995
27.8 Gestion des connexions à distance. 996
Création de connexions à distance. 996
Modification des connexions à distance. 998
27.9 Gestion des travaux de réplication. 999
Création de travaux de réplication. 999
Planification de travaux de réplication. 1001
Modification des travaux de réplication. 1001
Visualisation d'un journal après un travail de réplication. 1002
27.10 Gestion du nettoyage des objets. 1003
Utilisation du nettoyage des objets. 1003
Limites du nettoyage des objets. 1004
Fréquence de nettoyage des objets. 1004
27.11 Gestion de la détection et de la résolution des conflits. 1005
Résolution des conflits de réplication unidirectionnelle. 1005
Résolution des conflits de réplication bidirectionnelle. 1007
27.12 Utilisation des services Web dans Fédération. 1010
Variables de session 1011
Mise en cache des fichiers 1011
Déploiement personnalisé 1012
27.13 Planification à distance et instances exécutées localement. 1013
Planification à distance. 1013
Instances exécutées localement. 1014
Partage d'instances. 1015

27.14 Importation et promotion de contenu répliqué. 1016
Importation de contenu répliqué. 1016
Importation de contenu répliqué et réplication continue 1017
Promotion de contenu à partir d'un environnement de test. 1018
Redirection d'un site de destination. 1018
27.15 Meilleures pratiques. 1018
Limites de la version actuelle. 1022
Dépannage des messages d'erreur. 1023

28 Configurations supplémentaires pour les environnements Enterprise Resource Planning 1028
28.1 Configurations pour l'intégration SAP NetWeaver. 1028
Intégration avec SAP Business Warehouse (BW). 1028
28.2 Configuration pour l'intégration JD Edwards. 1074
Configuration de la connexion unique pour SAP Crystal Reports. 1074
Configuration de SSL (Secure Sockets Layer) pour les intégrations JD Edwards. 1075
28.3 Configuration pour l'intégration PeopleSoft Enterprise. 1076
Configuration de la connexion unique pour SAP Crystal Reports et PeopleSoft Enterprise. 1076
Configuration de la communication Secure Sockets Layer. 1077
Ajustement des performances pour les systèmes PeopleSoft. 1079
28.4 Configuration pour l'intégration Siebel. 1081
Configuration de Siebel pour l'intégration à la plateforme SAP BI. 1081
Création de l'élément de menu Crystal Reports. 1081
Reconnaissance contextuelle. 1083
Configuration de la connexion unique pour SAP Crystal Reports et Siebel. 1085
Configuration de la communication Secure Sockets Layer. 1086

29 Gestion et configuration des journaux. 1088
29.1 Journalisation des traces de composant. 1088
29.2 Niveaux du journal de suivi. 1088
29.3 Configuration du suivi pour les serveurs. 1089
Pour définir le niveau de journalisation dans la CMC. 1090
Pour définir le niveau de journalisation de plusieurs serveurs dans la CMC. 1090
Pour configurer le suivi de serveur à l'aide du fichier Bo_trace.ini. 1091
29.4 Configuration du suivi pour les applications Web. 1093
Définition du niveau de journalisation de suivi des applications Web dans la CMC. 1094
Configuration des paramètre de suivi de serveur à l'aide du fichier `BO_trace.ini`. 1094
29.5 Configuration du traçage pour les applications clientes de la plateforme de BI 1099
29.6 Configuration du suivi des messages d'erreur. 1100
29.7 Pour activer des fichiers journaux contenant les informations détaillées sur les messages d'erreur 1100

30 Intégration à SAP Solution Manager. 1102

30.1 Présentation de l'intégration. 1102
30.2 Liste de vérification de l'intégration SAP Solution Manager. 1102
30.3 Gestion de l'enregistrement du répertoire du paysage système. 1103
Enregistrement de la plateforme de BI dans le paysage système. 1103
Déclenchement de l'enregistrement SLD. 1105
Nettoyage du serveur SLD avant une installation de correctif. 1105
Connexion de la connectivité SLD 1106
Nom d'hôte virtuel. 1106
30.4 Gestion des agents Solution Manager Diagnostics. 1107
Présentation de Solution Manager Diagnostics (SMD). 1107
Utilisation des agents SMD. 1107
Compte utilisateur SMAdmin. 1108
30.5 Gestion de l'instrumentation des performances. 1109
Instrumentation de performances pour la plateforme de BI. 1109
Configuration de l'instrumentation de performances pour la plateforme de BI. 1109
Instrumentation de performances pour le niveau Web. 1110
Fichiers journaux d'instrumentation 1111
30.6 Suivi avec le Passeport SAP. 1111

31 Administration de la ligne de commande. 1113
31.1 Scripts UNIX. 1113
Utilitaires de script. 1113
Modèles de scripts. 1119
Scripts utilisés par la plateforme de BI. 1119
31.2 Scripts Windows. 1121
ccm.exe. 1121
31.3 Lignes de commande des serveurs. 1124
Présentation des lignes de commande. 1124
Options standard communes à tous les serveurs. 1124
Central Management Server 1125
Crystal Reports Processing Server et Crystal Reports Cache Server. 1127
Job Servers. 1128
Serveur de traitement adaptatif. 1129
Report Application Server. 1129
Web Intelligence Processing Server. 1131
Input et Output File Repository Servers. 1132
Event Server. 1134

32 Repository Diagnostic Tool. 1135
32.1 Présentation du Repository Diagnostic Tool. 1135
32.2 Utilisation du Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel). 1136
Pour utiliser l'outil de diagnostic de référentiel. 1136

Paramètres du Repository Diagnostic Tool. 1137
32.3 Incohérences entre le CMS et le FRS. 1146
32.4 Incohérences dans les métadonnées du CMS. 1146
32.5 Gestion du SDK Restful dans l'application Web BOE. 1149

33 HSTS (Strict Transport Security) HTTP. 1151
33.1 Configuration de HSTS (Strict Transport Security) HTTP. 1151

34 Annexe relative aux droits. 1153
34.1 A propos de l'annexe relative aux droits. 1153
34.2 Droits généraux. 1153
Droits sur la destination. 1157
34.3 Droits sur les types d'objet spécifiques. 1158
Droits d'accès aux dossiers. 1158
Catégories. 1158
Rapports Crystal. 1159
Documents Web Intelligence. 1159
Utilisateurs et groupes. 1160
Niveaux d'accès. 1162
Droits d'univers (.unv). 1162
Droits d'univers (.unx). 1164
Niveaux d'accès aux objets d'univers. 1165
Droits de connexion. 1166
Applications. 1168

35 Annexe relative aux propriétés des serveurs. 1176
35.1 A propos de l'annexe relative aux propriétés des serveurs. 1176
Propriétés courantes du serveur. 1176
Propriétés des services principaux. 1178
Propriétés des services de connectivité. 1189
Propriétés des services Crystal Reports. 1193
Propriétés d'Analysis Services. 1202
Propriétés des services de fédération de données. 1203
Propriétés des services Web Intelligence. 1204

36 Annexe métrique système. 1212
36.1 A propos de l'annexe Métriques du serveur. 1212
Métriques communes du serveur. 1212
Métriques du Central Management Server. 1214
Métrique du serveur de connexion. 1218
Métriques de l'Event Server 1218
Métriques du File Repository Server. 1218
Métriques du serveur de traitement adaptatif. 1219

Métriques de serveurs conteneurs d'applications Web. 1223
Métriques d'Adaptative Job Server. 1224
Métriques de Crystal Reports Server. 1226
Métriques de Web Intelligence Server 1228

37 Annexe relative aux espaces réservés de nœuds et de serveurs. 1230
37.1 Espaces réservés de nœud et de serveur. 1230

38 Annexe relative au schéma de magasin de données d'audit. 1240
38.1 Présentation. 1240
38.2 Diagramme de schéma. 1240
38.3 Auditing Data Store Tables. 1240

39 Annexe relative au schéma de la base de données de surveillance. 1248
39.1 Schéma de la base de données des tendances. 1248

40 Annexe relative à la feuille de calcul Copie du système. 1251
40.1 Feuille de calcul Copie du système. 1251

1 Historique du document

Le tableau suivant fournit un récapitulatif des principales modifications apportées au document.

Version	Date	Description
Plateforme SAP BusinessObjects Business Intelligence 4.3 SP3	Décembre 2022	Mise à jour des rubriques suivantes avec le nouveau champ de longueur maximale du mot de passe pour l'authentification Enterprise : • Paramètres d'authentification Enterprise [page 245] • Pour créer un compte d'utilisateur [page 106] • Modification des paramètres généraux de mot de passe [page 115] • Pour modifier les paramètres généraux de mot de passe [page 247] • Introduction de l'activation de l'option Utiliser un chemin d'accès relatif pour utiliser l'URL relative du navigateur.
Plateforme SAP BusinessObjects Business Intelligence 4.3 SP2	Décembre 2021	Ajout de Configuration du serveur d'autorisation [page 765]. Mise à jour de Personnalisation des éléments d'interface Web Intelligence par groupe d'utilisateurs ou dossiers [page 792].

Plateforme SAP BusinessObjects Business Intelligence 4.3 SP1	Décembre 2020	• Ajout des nouvelles rubriques suivantes :
		  • Une rubrique sur la personnalisation de l'interface utilisateur Web Intelligence. Voir Personnalisation des éléments d'interface Web Intelligence par groupe d'utilisateurs ou dossiers [page 792].
		  • Script permettant d'effacer les sessions obsolètes [page 164].
		  • Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la zone de lancement BI [page 425]
		  • Configuration SSL JMX [page 838]
		• Mise à jour de deux rubriques :
		  • Chemins de mise à niveau [page 31].
		  • Droits sur la destination [page 1157] pour les *Options de destination* et les *Propriétés de destination de courrier électronique* avec le nouveau champ *Répondre à* pour tous les scénarios de publication.

Version	Date	Description
Plateforme SAP BusinessObjects Business Intelligence 4.3	Juin 2020	• SAP BusinessObjects Explorer, SAP BusinessObjects Dashboards, l'outil de conversion de rapport, l'outil de gestion de mise à niveau et BI Widgets sont obsolètes dans la version 4.3. • Ajout d'une nouvelle rubrique Assistant du workflow [page 863].

2 Démarrage

2.1 A propos de ce guide

Ce guide fournit des informations et des procédures pour le déploiement et la configuration de la plateforme SAP BusinessObjects Business Intelligence (la « plateforme de BI »). Les procédures décrivent les tâches courantes. Des informations d'ordre conceptuel et des détails techniques se rapportent aux questions plus élaborées.

Pour en savoir plus sur l'installation de ce produit, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*.

2.1.1 Public concerné par ce guide

Ce guide porte sur le déploiement et la configuration de la plateforme de BI. Il est recommandé de consulter ce guide si vous réalisez l'une des tâches suivantes :

- Planification de votre premier déploiement
- Configuration de votre premier déploiement
- Apport d'importantes modifications à l'architecture d'un déploiement existant
- Amélioration des performances du système

Ce guide s'adresse aux administrateurs système responsables de la configuration, de la gestion et de la maintenance d'une installation de la plateforme de BI. La maîtrise de votre système d'exploitation et de votre environnement réseau est des plus utiles, tout comme une connaissance générale des technologies relatives à la gestion des serveurs d'applications Web et à la rédaction de scripts. Toutefois, afin de tenir compte des différents niveaux d'expérience en matière d'administration, ce guide tente de fournir suffisamment d'informations contextuelles et conceptuelles pour clarifier l'ensemble des fonctions et des tâches d'administration.

2.1.2 A propos de la plateforme de Business Intelligence

La plateforme de BI (Business Intelligence) est une solution souple et évolutive permettant de fournir des informations aux utilisateurs finaux sous diverses formes, notamment des tableaux de bord et des rapports interactifs via n'importe quelle application Web, notamment un intranet, un extranet, Internet ou un portail d'entreprise.

Suite intégrée spécialisée dans le reporting, l'analyse et la diffusion d'informations, la plateforme offre des avantages concrets qui dépassent le simple cadre de l'entreprise.

Elle permet également aux utilisateurs finaux d'augmenter leur productivité tout en réduisant les tâches administratives.

Par exemple, elle utilisée pour diffuser des rapports de ventes hebdomadaires, fournir aux clients des services personnalisés ou intégrer des informations importantes dans des portails d'entreprise.

2.1.3 Variables

Les variables suivantes sont utilisées dans ce guide.

Variable	Description
`<REPINSTALL >`	Répertoire dans lequel est installée la plateforme de BI. Sous Windows, le répertoire par défaut est : `C:\Program Files (x86)\SAP BusinessObjects\`.
`<REPPLATEFORME64>`	Nom de votre système d'exploitation Unix. Les valeurs acceptées sont les suivantes : • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
`<REPSCRIPT>`	Répertoire où sont situés les scripts pour la gestion de la plateforme de BI. Sous Windows, le répertoire est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. Sous Unix, le répertoire est `<REPINSTALL>/sap_bobj/enterprise_xi40/<REPPLATEFORME64>/scripts`.

2.1.4 Terminologie

La documentation de la plateforme de BI utilise la terminologie suivante :

Terme	Définition
Produits de modules complémentaires	Produits utilisant la plateforme de BI mais disposant de leur propre programme d'installation.
Magasin de données d'audit	Base de données utilisée pour stocker les données d'audit
Plateforme de BI	Abréviation pour Plateforme SAP BusinessObjects Business Intelligence

Terme	Définition
Base de données fournie, serveur d'applications Web fourni	Base de données ou serveur d'applications Web accompagnant la plateforme de BI
Cluster (nom)	Au moins deux serveurs CMS (Central Management Servers) travaillant ensemble et utilisant une seule base de données du CMS.
Cluster (verbe)	Pour créer un cluster : 1. Installez un CMS et une base de données du CMS sur l'ordinateur A. 2. Installez un CMS sur l'ordinateur B. 3. Dirigez le CMS installé sur l'ordinateur B vers la base de données du CMS installée sur l'ordinateur A.
Clé de cluster	Utilisée pour déchiffrer les clés de la base de données du CMS. Vous pouvez changer de clé de cluster dans le CCM mais vous ne pouvez pas réinitialiser la clé comme un mot de passe. Elle renferme un contenu chiffré et il est essentiel de ne pas la perdre.
CMS	Abréviation pour Central Management Server
Base de données du CMS	Base de données utilisée par le CMS pour stocker les informations relatives à la plateforme de BI
Déploiement	Logiciel de la plateforme de BI installé, configuré et exécuté sur un ou plusieurs ordinateurs.
Installation	Une instance des fichiers de la plateforme de BI créée par le programme d'installation sur un ordinateur
Ordinateur	Ordinateur sur lequel le logiciel de la plateforme de BI est installé
Version principale	Version complète du logiciel
Version secondaire	Version comportant certains composants du logiciel
Nœud	Groupe de serveurs de la plateforme de BI qui s'exécutent sur le même ordinateur et sont gérés par le même SIA (Server Intelligence Agent)
Correctif	Petite mise à jour concernant une version de Support Package spécifique

Terme	Définition
Promotion	Processus de transfert de contenu BI entre des déploiements de même version principale (par exemple, de 4.3 vers 4.3) à l'aide de l'application de gestion des promotions
Serveur	Un processus de la plateforme de BI. Un serveur héberge un ou plusieurs services
Server Intelligence Agent	Processus gérant un groupe de serveurs, notamment l'arrêt, le démarrage et le redémarrage des serveurs
Support Package	Mises à jour logicielle concernant une version secondaire ou principale
Serveur d'applications Web	Serveur traitant du contenu dynamique
Mise à niveau	La planification, la préparation, la migration et le post-traitement nécessaires à la réalisation d'un processus de migration
ONE Installer	ONE Installer est un package d'installation qui prend en charge plusieurs scénarios d'installation de BI, tels que la nouvelle installation d'un package de services ou d'un correctif, n'importe quelle mise à jour de correctif à correctif et n'importe quelle mise à jour de package de services à correctif.

2.2 Avant de commencer

2.2.1 Notions clés

2.2.1.1 Server Intelligence

Server Intelligence est un composant central de la plateforme de BI. Les modifications des processus des serveurs appliquées dans la CMC (Central Management Console) sont répercutées sur les objets serveur correspondants par le CMS (Central Management Server). Le SIA (Server Intelligence Agent) est utilisé pour redémarrer ou arrêter automatiquement un serveur lorsqu'il rencontre une condition inattendue ; un administrateur y accède lorsqu'il gère un nœud.

Le CMS stocke les informations relatives aux serveurs dans la base de données système du CMS, si bien que vous pouvez facilement restaurer les paramètres par défaut des serveurs. Comme le SIA interroge périodiquement le CMS pour demander des informations sur les serveurs qu'il gère, le SIA connaît l'état dans lequel doivent être les serveurs et le moment où appliquer une action.

> **Remarque**
>
> Une installation de la plateforme de BI est une instance unique des fichiers de la plateforme de BI créée par le programme d'installation sur un ordinateur. Une instance d'installation de la plateforme de BI ne peut être utilisée qu'au sein d'un seul cluster. Les nœuds appartenant à différents clusters qui partagent la même installation de la plateforme de BI ne sont pas pris en charge parce que ce type de déploiement ne peut pas se voir appliquer des correctifs ou des mises à jour. Seules les plateformes Unix prennent en charge plusieurs installations du logiciel sur le même ordinateur. Si chaque installation est exécutée sous un compte utilisateur unique et est installée dans un dossier distinct, les installations ne partagent aucun fichier. Rappelez-vous que tous les ordinateurs du cluster doivent avoir le même niveau de version et de correctif.

Informations associées

Serveurs, hôtes et clusters [page 39]

2.2.1.2 Serveurs, services, nœuds et hôtes

La plateforme de BI utilise les termes serveur et service pour désigner les deux types de logiciels s'exécutant sur un ordinateur de la plateforme de BI.

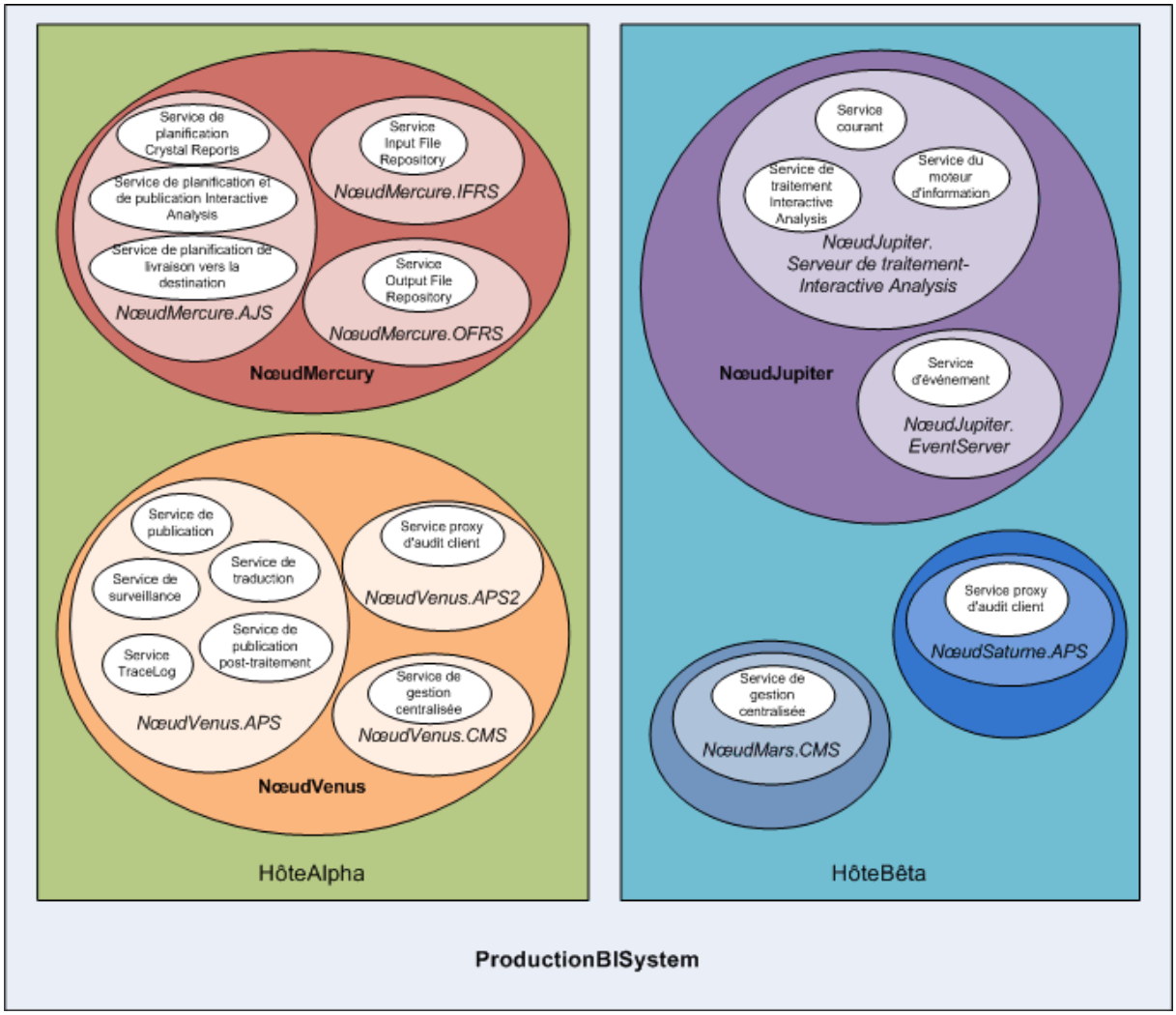
Le terme « serveur » sert à décrire un processus au niveau du système d'exploitation (appelé démon sur certains systèmes) qui héberge un ou plusieurs services. Par exemple, le CMS (Central Management Server) et le serveur de traitement adaptatif (Adaptive Processing Server) sont des serveurs. Un serveur s'exécute sous un compte système spécifique et possède son propre ID de processus (PID).

Un service est un sous-système de serveur qui exécute une fonction spécifique. Le service s'exécute dans l'espace mémoire de son serveur sous l'ID de processus du conteneur parent (serveur). Par exemple, le service de planification Web Intelligence est un sous-système qui s'exécute sur l'Adaptive Job Server.

Un nœud est un ensemble de serveurs de la plateforme de BI qui s'exécutent tous sur le même hôte et sont gérés par le même SIA (Server Intelligence Agent). Un même hôte peut contenir un ou plusieurs nœuds.

La plateforme de BI peut être installée sur un seul ordinateur, répartie sur plusieurs ordinateurs d'un intranet ou sur un réseau étendu (WAN).

Le diagramme suivant illustre une hypothèse d'installation de la plateforme de BI. Le nombre d'hôtes, nœuds, serveurs et services, ainsi que le type des serveurs et services, varient en dans les installations réelles.



Deux hôtes forment le cluster nommé ProductionBISystem :

- L'hôte nommé HostAlpha comporte l'installation de la plateforme de BI et est configuré de sorte à contenir deux nœuds :
  - NodeMercuy contient un Adaptive Job Server (`NodeMercury.AJS`) avec les services de planification et publication de rapports, un Input File Repository Server (`NodeMercury.IFRS`) avec un service de stockage des rapports d'entrée, ainsi qu'un Output File Repository Server (`NodeMercury.OFRS`) avec un service de stockage des rapports de sortie.
  - NodeVenus contient un serveur de traitement adaptatif (`NodeVenus.APS`) avec des services fournissant des fonctions de publication, de surveillance et de traduction, un serveur de traitement adaptatif (`NodeVenus.APS2`) avec un service d'audit client, ainsi qu'un Central Management Server (`NodeVenus.CMS`) avec un service fournissant les services du CMS.
- L'hôte nommé HostBeta comporte l'installation de la plateforme de BI et est configuré de sorte à contenir trois nœuds :
  - NodeMars contient un Central Management Server (`NodeMars.CMS`) avec un service fournissant les services du CMS. Le fait d'avoir le CMS sur deux ordinateurs permet d'avoir des fonctionnalités d'équilibrage des charges, d'atténuation et de basculement.

- NodeJupiter contient un serveur de traitement Web Intelligence (`NodeJupiter.Web Intelligence`) avec un service assurant le reporting Web Intelligence et un Event Server (`NodeJupiter.EventServer`) assurant la surveillance des rapports des fichiers.
- NodeSaturn contient un serveur de traitement adaptatif (`NodeSaturn.APS`) avec un service fournissant l'audit client.

2.2.2 Outils d'administration clés

2.2.2.1 Assistant de configuration du système

L'Assistant de configuration du système est un outil disponible pour configurer simplement et rapidement votre déploiement de la plateforme de BI. L'Assistant vous guide pour les options de configuration de base, amenant à un déploiement qui fonctionne à l'aide de paramètres courants comme :

- les serveurs du produit à démarrer automatiquement avec la plateforme de BI ;
- le choix d'optimiser votre déploiement pour des performances maximales ou pour des ressources matérielles limitées ;
- les emplacements des dossiers système.

Par défaut, l'Assistant s'exécute automatiquement quand vous vous connectez à la CMC (Central Management Console), mais vous pouvez modifier ce paramètre dans l'Assistant. Vous pouvez également démarrer l'Assistant à tout moment depuis la zone *Gérer* de la CMC.

> ⓘ Remarque
>
> Dans les systèmes de production, il est de rigueur de définir l'Assistant de sorte qu'il ne s'exécute pas automatiquement afin d'éviter une reconfiguration accidentelle.

> ⓘ Remarque
>
> Il est recommandé d'effectuer une sauvegarde complète avant d'utiliser l'Assistant pour apporter des modifications au système existant.

2.2.2.2 Central Management Console (CMC)

La CMC (Central Management Console) est un outil Web à utiliser pour effectuer les tâches administratives (dont la gestion des utilisateurs, du contenu et des serveurs) et pour configurer les paramètres de sécurité. La CMC étant une application Web, vous pouvez effectuer toutes les tâches d'administration dans un navigateur Web, sur tout ordinateur pouvant se connecter au serveur d'applications Web.

Seuls les membres du groupe Administrateurs peuvent modifier les paramètres de gestion, à moins que les droits pour le faire ne soient explicitement accordés à un utilisateur. Des rôles peuvent être affectés dans la CMC afin d'accorder des droits d'utilisateurs pour effectuer des tâches administratives mineures comme la gestion des utilisateurs d'un groupe ou des rapports dans les dossiers appartenant à une équipe.

2.2.2.3 Central Configuration Manager (CCM)

Le CCM (Central Configuration Manager) est un outil de gestion de nœuds et de dépannage de serveurs proposé sous deux formes. Dans un environnement Microsoft Windows, le CCM permet de gérer des serveurs locaux et distants via son interface utilisateur graphique ou depuis une ligne de commande. Dans un environnement Unix, le script shell du CCM (`ccm.sh`) permet de gérer les serveurs à partir de la ligne de commande.

Le CCM vous permet de créer et de configurer des nœuds et de démarrer ou arrêter votre serveur d'applications Web, s'il s'agit du serveur d'applications Web Tomcat fourni par défaut. Sous Windows, il permet également de configurer des paramètres réseau, tels que le cryptage SSL (Secure Socket Layer). Ces paramètres s'appliquent à tous les serveurs d'un même nœud.

> **Remarque**
>
> La plupart des tâches de gestion des serveurs sont à présent gérées via la CMC, et non via le CCM. Désormais, le CCM est utilisé pour le dépannage et la configuration des nœuds.

2.2.2.4 Repository Diagnostic Tool

L'outil de diagnostic de référentiel permet d'analyser, de diagnostiquer et de réparer les incohérences qui peuvent se produire entre la base de données système du CMS (Central Management Server) et le stockage des fichiers FRS (File Repository Servers). Vous pouvez définir une limite pour le nombre d'erreurs trouvées et réparées par le RDT avant l'arrêt.

Le RDT doit être utilisé après la restauration du système de la plateforme de BI.

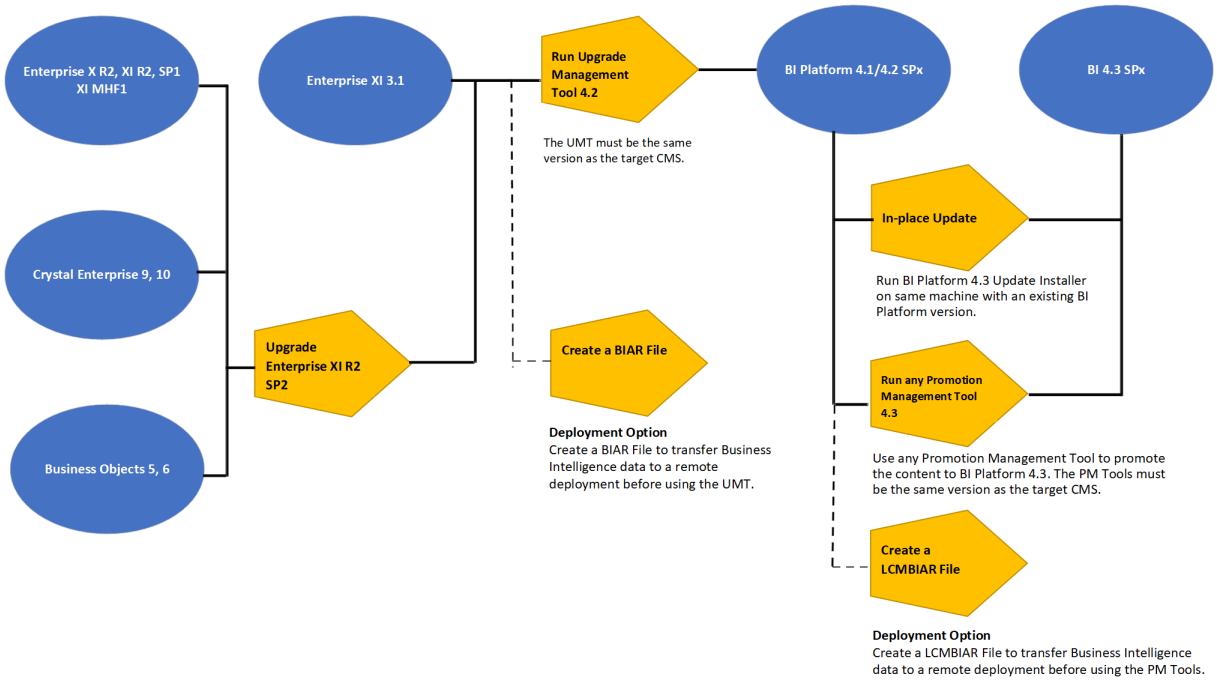
> **Remarque**
>
> Sur les systèmes de production, il est de rigueur d'exécuter régulièrement le RDT mais en désactivant l'option « repair » pour rechercher d'éventuels problèmes sous-jacents d'état du système. N'exécutez le RDT avec l'option de réparation activée que si vous êtes sûr de vouloir que le RDT effectue des réparations sur le système.

2.2.2.5 Outil de gestion de mise à niveau

UMT est obsolète dans la version BI 4.3. Pour en savoir plus, voir la note SAP 2801797

2.2.2.6 Chemins de mise à niveau

Il est possible de faire migrer les données du système et le contenu Business Intelligence des versions précédentes de BI 4.x vers la plateforme SAP BusinessObjects Business Intelligence 4.3.



L'outil de gestion de mise à niveau est obsolète dans la plateforme SAP BusinessObjects Business Intelligence 4.3, mais vous pouvez suivre les chemins de mise à niveau ci-dessous pour passer à la version 4.3.

Dans le cas d'un déploiement antérieur, suivez ces instructions pour mettre à niveau le déploiement existant vers la plateforme de BI 4.3 :

1. Si votre déploiement existant est XI R2, XI MHF1, XI R2 SP1, BusinessObjects 5/6 ou Crystal Enterprise 9/10, vous devez d'abord passer à la version XI R2 SP2 (ou supérieure) et poursuivre à partir de l'étape 3.
2. Si votre déploiement existant est XI 3.x, vous pouvez passer directement à l'étape 3.
3. Installez BI 4.1/4.2 SPx sur un ordinateur distinct et exécutez l'outil de gestion de mise à niveau depuis la version 4.1/4.2 SPx pour migrer le contenu des versions susmentionnées vers le niveau de BI 4.1/4.2.
4. Une fois que votre contenu est au niveau de BI 4.1/4.2 SPx, vous pouvez choisir l'une des méthodes suivantes pour passer à la version 4.3.
   1. Exécutez le logiciel d'installation de mise à jour de BI 4.3.x sur l'ordinateur au niveau 4.1/4.2 ou
   2. Installez BI 4.3 sur un ordinateur distinct et utilisez l'outil de gestion des promotions à partir de BI 4.3.x pour promouvoir le contenu du niveau BI 4.1/4.2 SPx vers le niveau BI 4.3.x.

> **Remarque**
>
> 1. Pour promouvoir le contenu du niveau BI 4.1/4.2 SPx vers le niveau BI 4.3.x, la version de l'outil de gestion des promotions doit être identique à la version du CMS cible.
> 2. Pour en savoir plus, voir le Guide de migration de BusinessObjects 5/6 vers XI 3.1 et le Guide d'installation de la plateforme de BI pour votre version, disponible à l'adresse https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US
> 3. L'outil de gestion de mise à niveau ne met à niveau que le serveur et les fonctionnalités de niveau Web du déploiement. Pour plus d'informations sur l'UMT, voir le Guide de mise à niveau de la plateforme de Business Intelligence pour votre version, disponible à l'adresse https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US.

2.2.3 Tâches clés

Selon votre situation, vous pouvez consulter des sections spécifiques de ce guide et accéder à d'autres ressources disponibles. Pour chacune des situations ci-après, une liste de tâches suggérées et de rubriques à consulter vous est proposée.

Informations associées

Planification ou exécution de votre premier déploiement [page 32]
Configuration de votre déploiement [page 33]
Amélioration des performances du système [page 33]
Central Management Console (CMC) [page 29]

2.2.3.1 Planification ou exécution de votre premier déploiement

Si vous planifiez ou effectuez votre premier déploiement de la plateforme de BI, il est conseillé de lire ces sections du guide :

- Pour vous familiariser avec les composants de la plateforme de BI, lisez la rubrique « Présentation de l'architecture »
- « Description de la communication entre les composants de la plateforme de BI »
- « Présentation de la sécurité »
- Si vous prévoyez d'utiliser une authentification tierce, lisez « Options d'authentification dans la plateforme de BI »
- Après l'installation, lisez « Utilisation de la zone de gestion Serveurs de la CMC »

Pour en savoir plus sur l'installation de la plateforme de BI, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*. Pour évaluer vos besoins et concevoir l'architecture de déploiement

la plus appropriée à votre entreprise, lisez le *Guide de planification de la plateforme SAP BusinessObjects Business Intelligence*.

Informations associées

Présentation de l'architecture [page 35]
Communication entre les composants de la plateforme de BI [page 200]
Présentation de la sécurité [page 157]
Options d'authentification dans la plateforme de BI [page 240]
Utilisation de la zone de gestion Serveurs de la CMC [page 428]

2.2.3.2 Configuration de votre déploiement

Si vous avez terminé l'installation de la plateforme de BI et que vous devez effectuer les tâches de configuration initiales, telles que la configuration du pare-feu et la gestion des utilisateurs, nous vous recommandons de lire les sections suivantes.

Informations associées

Introduction à l'Assistant de configuration du système [page 90]
Communication entre les composants de la plateforme de BI [page 200]
Présentation de la sécurité [page 157]
Surveillance [page 821]

2.2.3.3 Amélioration des performances du système

Pour évaluer l'efficacité de votre déploiement et l'affiner afin de maximiser les ressources, lisez les sections suivantes :

- Si vous souhaitez utiliser un modèle de déploiement pour configurer votre système, lisez « Introduction à l'Assistant de configuration du système ».
- Si vous souhaitez surveiller le système existant, lisez « A propos de la surveillance ».
- Pour les tâches de gestion quotidienne et les procédures d'utilisation des serveurs dans la CMC, consultez « Utilisation de la zone de gestion Serveurs de la CMC ».

Informations associées

Introduction à l'Assistant de configuration du système [page 90]
Surveillance [page 821]
Utilisation de la zone de gestion Serveurs de la CMC [page 428]

2.2.3.4 Utilisation des objets dans la CMC

Un objet est un document ou un fichier créé sur la plateforme de BI ou un autre logiciel, stocké et géré dans le référentiel de la plateforme de BI. Si vous utilisez des objets dans la CMC, lisez les sections suivantes :

- Pour en savoir plus sur la configuration des utilisateurs et des groupes dans la CMC, voir « Présentation de la gestion des comptes ».
- Pour définir une sécurité sur les objets, voir « Fonctionnement des droits sur la plateforme de BI ».
- Pour obtenir des informations générales sur l'utilisation des objets, voir le *Guide de l'utilisateur de la plateforme SAP BusinessObjects Business Intelligence*.

Informations associées

Présentation de la gestion des comptes [page 103]
Fonctionnement des droits sur la plateforme de BI [page 128]

3 Architecture

3.1 Présentation de l'architecture

Cette section décrit les composants de l'architecture globale de la plateforme, ainsi que les composants système et de service qui constituent la plateforme SAP BusinessObjects Business Intelligence. Ces informations permettent aux administrateurs de mieux comprendre les bases du système et d'élaborer un plan de déploiement, de gestion et de maintenance du système.

> **Remarque**
>
> Pour afficher une liste des plateformes, langues, bases de données, serveurs d'applications Web, serveurs Web et d'autres systèmes pris en charge par cette version, voir la *Product Availability Matrix* (PAM) à l'adresse http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540.

> **Remarque**
>
> Etant donné que la Matrice de disponibilité des produits est constamment actualisée, référez-vous toujours à sa version en ligne au lieu d'une copie téléchargée.

La plateforme de Business Intelligence est conçue pour fournir des performances élevées dans une large gamme de scénarios utilisateur et de déploiement. Vous pouvez transférer les opérations de traitement et de planification consommatrices de temps processeur en créant des serveurs dédiés pour héberger des services spécifiques. L'architecture est conçue pour répondre aux besoins de quasiment tout déploiement BI et est suffisamment flexible pour passer de quelques utilisateurs avec un seul outil à des dizaines de milliers d'utilisateurs avec plusieurs outils et interfaces.

Les développeurs peuvent intégrer la plateforme de BI aux autres systèmes technologiques de votre organisation à l'aide d'API (Application Programming Interfaces) de services Web, Java ou .NET.

Les utilisateurs finaux peuvent accéder aux rapports, en créer, en modifier et interagir avec ceux-ci à l'aide d'outils et d'applications spécialisés, notamment :

- Les clients installés par le programme d'installation des outils client de la plateforme de BI :
  - Web Intelligence Rich Client
  - Gestionnaire de vues d'entreprise
  - Outil de conception d'univers
  - Query as a Web Service
  - Outil de conception d'information (anciennement Information Designer)
  - Outil de gestion de la traduction (anciennement Gestionnaire de traduction)
- Clients disponibles séparément :
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (anciennement Voyager)
  - Espaces de travail BI (anciennement Dashboard Builder)

Les services informatiques peuvent utiliser les outils de gestion de systèmes et de données suivants :

- Visualiseurs de rapports
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel)
- Outil d'administration de fédération de données
- Outil de conception d'univers (anciennement Universe Designer)
- SAP BusinessObjects Mobile

Pour garantir la flexibilité, la fiabilité et l'évolutivité, les composants de la plateforme de BI peuvent être installés sur un ou plusieurs ordinateurs. Dans certains cas, vous pouvez même installer deux versions différentes de la plateforme de BI simultanément sur le même ordinateur, bien que cette configuration soit uniquement recommandée dans le cadre du processus de mise à niveau ou à des fins de test.

Les processus serveur peuvent être étendus verticalement (c'est-à-dire qu'un ordinateur exécute plusieurs processus côté serveur, voire tous) pour réduire les coûts ou étendus horizontalement (c'est-à-dire que les processus serveur sont répartis entre au moins deux ordinateurs en réseau) pour améliorer les performances. Il est également possible d'exécuter plusieurs versions redondantes d'un même processus serveur sur plusieurs ordinateurs de sorte que le traitement puisse se poursuivre si un problème survient au niveau du premier processus.

> **Remarque**
>
> Bien qu'il soit possible d'utiliser à la fois des plateformes Windows et Unix ou Linux, il est recommandé de ne pas utiliser de systèmes d'exploitation différents pour les processus CMS (Central Management Server).

3.1.1 Schéma des composants

La plateforme SAP BusinessObjects Business Intelligence désigne une plateforme de Business Intelligence (BI) qui fournit des outils d'analyse et de reporting au niveau de l'entreprise pour faciliter la remise des informations. Les données peuvent être analysées à partir d'un grand nombre de systèmes de bases de données pris en charge (y compris des systèmes OLAP de texte ou multidimensionnels) et les rapports BI peuvent être publiés dans différents formats sur divers systèmes de publication.

Le schéma d'architecture illustre les composants de la plateforme de BI, y compris les serveurs et les outils client, ainsi que d'autres produits d'analyse, composants d'application Web et bases de données pouvant faire partie d'un paysage de la plateforme de BI. Diagramme d'architecture BI 4.3.

La plateforme de BI effectue des rapports à partir d'une connexion en lecture seule aux bases de données de votre organisation et utilise ses propres bases de données pour stocker ses informations de configuration, d'audit et autres informations opérationnelles. Les rapports BI créés par le système peuvent être envoyés vers de nombreuses destinations, y compris les systèmes de fichiers et courriers électroniques, ou être accessibles par le biais de sites Web ou de portails.

La plateforme de BI est un système autonome qui peut exister sur un seul ordinateur (par exemple, sous forme de petit environnement de développement ou d'environnement de test de pré-production) ou qui peut être mis à l'échelle dans un cluster de plusieurs ordinateurs exécutant différents composants (par exemple, sous forme d'environnement de production à grande échelle).

3.1.2 Niveaux d'architecture

La plateforme SAP BusinessObjects de Business Intelligence peut être considérée comme une série de niveaux conceptuels :

Niveau client

Le niveau client contient toutes les applications de bureau client qui interagissent avec la plateforme de BI pour fournir diverses capacités de reporting, d'analyse et d'administration. Parmi les exemples : Central Configuration Manager (programme d'installation de la plateforme de BI), outil de conception d'information (programme d'installation des outils client de la plateforme de BI) et SAP Crystal Reports (disponible et installé séparément).

À compter de la version SAP BI 4.3, les applications de bureau client (Web Intelligence Rich Client, Outil de conception d'information, Outil de conception d'univers, ...) sont des applications 64 bits. Elles ne sont plus des applications 32 bits.

Niveau Web

Le niveau Web contient des applications Web déployées sur un serveur d'applications Web Java. Les applications Web fournissent les fonctionnalités de la plateforme de BI aux utilisateurs finaux via un navigateur Web. Les exemples d'applications Web comprennent l'interface Web d'administration de la CMC (Central Management Console) et la zone de lancement BI.

Le niveau Web contient également des services Web. Les services Web fournissent les fonctionnalités de la plateforme de BI aux outils logiciels via le serveur d'applications Web, par exemple l'authentification de session, la gestion des droits utilisateur, la planification, la recherche, l'administration, le reporting et la gestion des requêtes. Par exemple, Live Office est un produit qui utilise les services Web pour intégrer le reporting de la plateforme de BI à certains produits Microsoft Office.

Niveau gestion

Le niveau de gestion (également nommé niveau d'intelligence) coordonne et commande tous les composants qui constituent la plateforme de BI. Il comprend le CMS (Central Management Server) et l'Event Server, ainsi que les services associés. Le CMS gère la sécurité et les informations de configuration, adresse les demandes de service aux serveurs, gère l'audit, ainsi que la base de données système du CMS. L'Event Server gère les événements basés sur des fichiers qui se produisent dans un niveau de stockage donné.

Niveau stockage

Le niveau de stockage est responsable de la gestion des fichiers tels que les documents et les rapports.

L'Input File Repository Server gère les fichiers contenant les informations utilisées dans les rapports, comme les types de fichiers suivants : `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, `.unv` et `.unx`.

> **Remarque**
>
> La taille du stockage de fichier Input File Repository Server n'est pas gérée par le système ; toutefois, un administrateur doit gérer un plan de maintenance et de surveillance.

L'Output File Repository Server gère les rapports créés par le système, comme les types de fichiers suivants : `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

Le niveau de stockage gère également la mise en mémoire cache des rapports afin d'économiser les ressources système lorsque les utilisateurs accèdent aux rapports.

Niveau traitement

Le niveau de traitement analyse les données et génère les rapports ainsi que d'autres types de sortie. Il s'agit du seul niveau qui accède directement aux bases de données contenant les données des rapports. Ce niveau comprend l'Adaptive Job Server, le serveur de connexion (64 bits) et des serveurs de traitement comme le serveur de traitement adaptatif ou le serveur de traitement Crystal Reports.

Niveau données

Le niveau de données comprend les serveurs hébergeant la base de données système du CMS et le magasin de données d'audit. Il comprend également tous les serveurs de base de données contenant des données relationnelles, OLAP ou autres destinées aux applications de reporting et d'analyse.

3.1.3 Bases de données

La plateforme de BI utilise plusieurs bases de données différentes.

- Base de données de reporting
  Elle fait référence aux données de votre entreprise. Il s'agit des données sources faisant l'objet des analyses et rapports de la suite SAP BusinessObjects Business Intelligence. Le plus souvent, les données sont stockées dans une base de données relationnelle, mais elles peuvent également être contenues dans des fichiers texte, des documents Microsoft Office ou des systèmes OLAP.
- Base de données système du CMS
  La base de données système du CMS est utilisée pour stocker des informations de la plateforme de BI telles que les renseignements d'utilisateur, de serveur, de dossier, de document, de configuration et d'authentification. La gestion de cette base de données, parfois connue sous le nom de *référentiel système*, est assurée par le CMS (Central Management Server).
- Magasin de données d'audit

Le magasin de données d'audit sert à stocker des informations sur des événements traçables qui se produisent sur la plateforme de BI. Ces informations peuvent être utilisées pour contrôler l'utilisation des composants système, l'activité des utilisateurs ou d'autres aspects des opérations quotidiennes.

- Base de données de surveillance
  La surveillance utilise la base de données du magasin de données d'audit pour stocker les informations de composants et de configuration système relatives aux modalités de prise en charge SAP.
- Base de données de commentaires
  L'application Commentaires BI a été introduite dans la CMC. Elle permet aux utilisateurs de collaborer en commentant toutes les données et statistiques disponibles dans un document donné.
  La base de données de commentaires est configurée dans la même base de données que la base de données d'audit. Elle est créée par défaut dans la base de données d'audit.

Si vous ne disposez pas déjà d'un serveur de base de données à utiliser avec les bases de données système du CMS et du magasin de données d'audit, le programme d'installation de la plateforme de BI peut en installer un et le configurer pour vous. Il est conseillé d'évaluer vos besoins par rapport aux informations du fournisseur de votre serveur de base de données Web pour déterminer quelle base de données prise en charge correspond le mieux aux besoins de votre entreprise.

> **Remarque**
>
> La base de données SQL Anywhere par défaut n'est pas recommandée sur les systèmes de production. Elle est incorporée dans les packages fournisseur de la plateforme de BI qui permet de déployer et de tester instantanément la plateforme de BI, mais inclut des fonctionnalités limitées pour la gestion d'une base de données. Il est conseillé d'utiliser SQL Anywhere dans sa forme complète ou une instance de base de données prise en charge existante pour le système de production, car votre base de données CMS doit impérativement résider dans votre centre de données. Il est géré par les administrateurs de base de données et les processus appropriés doivent avoir été établis pour la sécurité des données et la disponibilité des serveurs.

3.1.4 Serveurs, hôtes et clusters

La plateforme de BI comprend des ensembles de serveurs s'exécutant sur un ou plusieurs hôtes. Les petites installations (comme les systèmes de test ou de développement) peuvent utiliser un seul hôte pour un serveur d'applications Web, un serveur de base de données et tous les serveurs de la plateforme de BI.

Les installations moyennes et importantes peuvent utiliser des serveurs fonctionnant sur plusieurs hôtes. Par exemple, un hôte de serveur d'applications Web peut être utilisé en combinaison avec un hôte de serveur de la plateforme de BI. Cela libère des ressources sur l'hôte du serveur de la plateforme de BI, ce qui lui permet de traiter plus d'informations que s'il hébergeait également le serveur d'applications Web.

Les grandes installations peuvent disposer de plusieurs hôtes de serveurs de la plateforme de BI fonctionnant ensemble dans un cluster. Par exemple, si une entreprise compte un grand nombre d'utilisateurs SAP Crystal Reports, des serveurs de traitement Crystal Reports peuvent être créés sur plusieurs hôtes de serveurs de la plateforme de BI pour veiller à ce qu'il y ait suffisamment de ressources disponibles pour traiter les demandes des clients.

Les avantages d'avoir plusieurs serveurs sont les suivants :

- Amélioration des performances

Plusieurs hôtes de serveur de la plateforme de BI peuvent traiter une file d'attente d'informations de reporting plus rapidement qu'un seul hôte de serveur de la plateforme de BI.

- Equilibrage de charge
  Si un serveur rencontre une charge importante, le CMS envoie automatiquement le nouveau travail aux autres serveurs du cluster.
- Amélioration de la disponibilité
  Si un serveur rencontre une condition inattendue, le CMS réachemine automatiquement le travail vers d'autres serveurs jusqu'à ce que la condition soit corrigée.

3.1.5 Serveurs d'applications Web

Un serveur d'applications Web fait office de couche de traduction entre un navigateur Web ou une application riche et la plateforme de BI. Les serveurs d'applications Web exécutés sur les systèmes Windows, Unix et Linux sont pris en charge.

Pour obtenir une liste détaillée des serveurs d'applications Web pris en charge, consultez le document *Plateformes prises en charge/PAR*, disponible à l'adresse : https://support.sap.com/home.html.

Si vous ne disposez pas déjà d'un serveur d'applications Web à utiliser avec la plateforme de BI, le programme d'installation peut installer et configurer un serveur d'applications Web Tomcat. Il est conseillé d'évaluer vos besoins par rapport aux informations du fournisseur de votre serveur d'applications Web pour déterminer quel serveur d'applications Web pris en charge correspond le mieux aux besoins de votre entreprise.

> **Remarque**
>
> Lors de la configuration d'un environnement de production, il est conseillé d'héberger le serveur d'applications Web sur un système distinct. L'exécution de la plateforme de BI et d'un serveur d'applications Web sur le même hôte dans un environnement de production peut entraver les performances.

3.1.5.1 Activation de la mise en cluster dans l'application Web Zone de lancement BI pour prendre en charge le basculement de session et l'évolutivité

Cette section décrit comment activer la mise en cluster dans l'application Web Zone de lancement BI pour prendre en charge le basculement de session et l'évolutivité. Elle décrit aussi les étapes requises pour configurer les serveurs d'applications Apache Tomcat et WebSphere à cette fin.

Pour activer la mise en cluster pour un serveur d'applications comme Tomcat ou WebSphere, les composants suivants sont requis :

- Un serveur HTTP
- Un équilibreur de charge compatible
- Deux instances ou plus du serveur d'applications avec l'application Web requise déjà installée
- Une installation complète de BOE (référentiel)

> **Remarque**
>
> Les étapes décrites dans cette section sont génériques et peuvent être utilisées pour activer la mise en cluster pour toute autre application. Les seules différences sont les modifications apportées dans le descripteur de déploiement de l'application Web (web.xml). SAP vous recommande de contacter votre fournisseur de serveurs d'applications Web pour savoir comment configurer l'équilibrage de charge de niveau Web.

3.1.5.1.1 Installation d'Apache Tomcat

Pour installer le serveur Apache Tomcat, procédez comme suit :

1. Installez le serveur Apache HTTP.
2. Installez le serveur Apache Tomcat sur les ordinateurs exécutant l'instance.
3. Téléchargez mod_jk (équilibreur de charge) et enregistrez-le dans le répertoire "modules" sur le serveur Apache HTTPD à l'adresse http://tomcat.apache.org/download-connectors.cgi .
4. Exécutez l'agent SI sur un ordinateur exécutant une installation complète de BOE.

   > **Remarque**
   >
   > Pour vérifier la compatibilité de mod_jk, démarrez votre serveur HTTP. Un message d'erreur apparaît dans la console si la version téléchargée de mod_jk est incompatible avec votre version de serveur HTTP.

Configuration d'Apache Tomcat

Pour configurer Apache Tomcat, procédez comme suit :

1. Configurez le serveur Apache HTTP.
   a. Configurez httpd.conf (équilibreur de charge, chargement de l'application Web, surveillance, chemin d'accès au fichier workers.properties).
   b. Configurez le fichier workers.properties et enregistrez-le dans la bibliothèque Apache\Conf.

```
64  # If specified, ensure that no two invocations of Apache share the same
65  # scoreboard file. The scoreboard file MUST BE STORED ON A LOCAL DISK.
66  #
67  #ScoreBoardFile logs/apache_runtime_status
68
69  # Used for clustering
70
71  # Specify path to worker configuration file
72  #
73  JkWorkersFile C:\Server\Apache2\Apache2\conf\workers.properties
74  # Configure logging and memory
75  JkShmFile logs/mod_jk.shm
76  JkLogFile logs/mod_jk.log
77  JkLogLevel info
78
79  # Configure monitoring
80  JKMount /jkmanager jkstatus
81  JkMount /jkmanager/* jkstatus
82  <Location /jkmanager>
83  Order deny,allow
84  Deny from all
85  Allow from localhost
86  </Location>
87
88  # Configure applications
89  # JkMount /webapp-directory/* loadBalancer
90  JKMount /clusterjsp loadBalancer
91  JKMount /clusterjsp/* loadBalancer
92  JKMount /login loadBalancer
93  JKMount /login/* loadBalancer
94  JKMount /boe loadBalancer
95  JKMount /boe/* loadBalancer
96  #JKMount /BOE loadBalancer
97  #JKMount /BOE/* loadBalancer
98  JKMount /docs loadBalancer
99  JKMount /docs/* loadBalancer
100
```

```
182 LoadModule env_module modules/mod_env.so
183 #LoadModule expires_module modules/mod_expires.so
184 #LoadModule file_cache_module modules/mod_file_cache.so
185 #LoadModule headers_module modules/mod_headers.so
186 LoadModule imap_module modules/mod_imap.so
187 LoadModule include_module modules/mod_include.so
188 #LoadModule info_module modules/mod_info.so
189 LoadModule isapi_module modules/mod_isapi.so
190
191 # Used for clustering
192 #LoadModule for clustering
193
194 LoadModule jk_module modules/mod_jk.so
195
196 LoadModule log_config_module modules/mod_log_config.so
197 LoadModule mime_module modules/mod_mime.so
```

Load Tomcat Connector (mod_jk)

2. Configurez server.xml dans Tomcat (ajoutez des balises de mise en cluster).
   a. Dans server.xml, l'attribut jvmRoute doit correspondre au nom que vous avez utilisé dans le fichier workers.properties.
   b. Si vous utilisez Tomcat 8 ou une version ultérieure, supprimez JvmRouteSessionIDBinderListener (obsolète).
3. Ajoutez une balise distribuable au fichier web.xml (descripteur de déploiement) de l'application Web où la mise en cluster doit être prise en charge.

Le distributeur personnalisé, qui appelle le distributeur par défaut pour chaque requête, est spécifié ci-dessous. Si vous utilisez Tomcat 8, dans tout le fichier .xml du serveur Tomcat, remplacez :

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Inte
rceptor"/>
```

par

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatchInterc
eptor"/>
```

```
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>

  <Valve className="com.sap.customvalve.ForceReplicationValve"/>
   <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=".*\.gif;.*\.jpg;.*\.png;.*\.js;.*\.htm
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer" deployDir="/tmp/war-deploy/" tempDir="/tmp
```

4. Exportez le fichier jar pour le distributeur personnalisé (si des modifications sont requises) depuis le code. Copiez le fichier `forcereplicationvalve.jar` dans `<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` et collez-le dans `<TomcatInstallDir>/tomcat/lib` (dans tous les nœuds Tomcat).
5. Stockez ce fichier dans le dossier `tomcat/lib` pour chaque instance.
6. Redémarrez tous les serveurs.

> **Remarque**
>
> - Il est recommandé de démarrer les serveurs l'un après l'autre et de patienter le temps qu'un serveur ait complètement démarré avant d'en démarrer un autre.
> - N'utilisez pas localhost:6400 comme nom du système dans l'écran de connexion de la zone de lancement. Indiquez le nom (ou l'IP) de l'ordinateur exécutant l'installation de BOE. Vérifiez que l'agent SI est exécuté sur cette installation.
> - Explorez l'attribut channelSendOptions pour rechercher l'option la plus adéquate. Il permet de définir les options de réponse synchrone, réponse asynchrone, etc.
> - Lors de l'exportation du fichier jar pour le distributeur personnalisé depuis le code, pensez à créer une hiérarchie de packages adéquate pour le fichier jar et à l'inclure dans server.xml.

3.1.5.1.2 Installation de WebSphere

Configuration de WebSphere

Pour configurer WebSphere, procédez comme suit :

1. Ajoutez une balise distribuable au fichier web.xml de l'application Web BOE pour les deux instances du serveur d'applications WebSphere.
2. Dans la console IBM, allez à *Tous les serveurs* > *membre1* > *Gestion de la session*.
   a. Vérifiez et activez les cookies.
   b. Activez *Autoriser l'accès en série* et passez le délai d'expiration à 10 secondes.
3. Accédez à *Paramètres de l'environnement de distribution* > *Réplication de mémoire à mémoire*.
   a. Créez un domaine de réplication et sélectionnez-le.
   b. Sélectionnez le mode de réplication : à la fois client et serveur.
4. Dans chaque instance sous *Tous les serveurs*, sélectionnez le même domaine de réplication que celui sélectionné à l'étape précédente.
5. Accédez à *Paramètres de l'environnement de distribution* > *Paramètres d'ajustement personnalisés*.
   a. Pour le basculement, sélectionnez le niveau d'ajustement *Faible*.
6. Redémarrez tous les serveurs.

3.1.5.2 Serveur conteneur d'applications Web (WACS)

Un serveur d'applications Web est requis pour héberger les applications Web de la plateforme de BI.

Si vous êtes un administrateur expérimenté de serveurs d'applications Web Java avec des besoins avancés en administration, utilisez un serveur d'applications Web Java pris en charge pour héberger les applications Web de la plateforme de BI. Si vous utilisez un système d'exploitation Windows pris en charge pour héberger la plateforme de BI et préférez un processus d'installation de serveur d'applications Web simple ou si vous ne disposez pas des ressources pour gérer un serveur d'applications Web Java, vous pouvez installer le WACS (Web Application Container Service) lors de l'installation de la plateforme de BI.

Le WACS est un serveur de la plateforme de BI qui permet aux applications Web de la plateforme de BI telles que la CMC (Central Management Console), la zone de lancement BI et les services Web, de s'exécuter sans installation préalable d'un serveur d'applications Web Java.

L'utilisation d'un serveur WACS présente plusieurs avantages :

- Les serveurs WACS sont extrêmement simples à installer, maintenir et configurer. Ils sont installés et configurés par le programme d'installation de la plateforme de BI et ne requièrent aucune autre action pour en commencer l'utilisation.
- Le serveur WACS ne requiert aucune compétence en administration et maintenance de serveurs d'applications Java.
- Le serveur WACS fournit une interface d'administration compatible avec d'autres serveurs de la plateforme de BI.

- Comme les autres serveurs de la plateforme de BI, le WACS peut être installé sur un hôte dédié.

> **Remarque**
>
> Il existe certaines limites à l'utilisation du serveur WACS à la place d'un serveur d'applications Web Java dédié :
>
> - Les serveurs WACS sont uniquement disponibles sur les systèmes d'exploitation Windows pris en charge.
> - Les applications Web personnalisées ne peuvent être déployées sur des WACS car ils ne prennent en charge que les applications Web installées avec la plateforme de BI.
> - Les WACS ne peuvent pas être utilisés avec un équilibreur de charge Apache.

Il est possible d'utiliser un serveur d'applications Web dédié en plus du WACS. Cela permet à votre serveur d'applications Web dédié d'héberger des applications Web personnalisées tandis que la CMC et les autres applications Web de la plateforme de BI sont hébergées par le WACS.

3.1.6 Kits de développement logiciel

Le kit de développement logiciel (SDK) permet au développeur d'intégrer des aspects de la plateforme SAP BusinessObjects Business Intelligence aux applications et systèmes d'une organisation.

La plateforme de BI offre des SDK pour le développement logiciel sur les plateformes Java et .NET.

> **Remarque**
>
> Les SDK .NET de la plateforme de BI ne sont pas installés par défaut. Ils doivent être téléchargés depuis SAP Service Marketplace.

Les SDK ci-après sont pris en charge par la plateforme de BI :

- SDK Java et SDK .NET de la plateforme de Business Intelligence.
  Les SDK de la plateforme de BI permettent aux applications d'exécuter des tâches telles que l'authentification, la gestion des sessions, l'utilisation d'objets du référentiel, la planification et la publication de rapports et la gestion des serveurs.

  > **Remarque**
  >
  > Pour accéder à l'ensemble des fonctions de sécurité, gestion des serveurs et audit, utilisez le SDK Java.

- SDK de services Web RESTful de la plateforme de Business Intelligence
  Le SDK de services Web RESTful de la plateforme de BI permet d'accéder à la plateforme de BI à l'aide du protocole HTTP. Vous pouvez utiliser ce SDK pour vous connecter à la plateforme de BI, parcourir le référentiel de la plateforme de BI, accéder à des ressources et réaliser une planification des ressources de base. Vous pouvez accéder à ce SDK en écrivant des applications qui utilisent un langage de programmation prenant en charge le protocole HTTP ou en utilisant un outil prenant en charge la création de requêtes HTTP.
- SDK Java Consumer et SDK .NET Consumer de la plateforme de Business Intelligence
  Une implémentation de services Web SOAP permettant de gérer l'authentification et la sécurité des utilisateurs, l'accès aux documents et aux rapports, la planification, la publication et la gestion des serveurs.

Les services Web de la plateforme de BI utilisent des normes telles que XML, SOAP, AXIS 2.0 et WSDL. La plateforme suit la spécification de services Web WS-Interoperability Basic Profile 1.0.

> **Remarque**
>
> Les applications des services Web ne sont actuellement prises en charge qu'avec les configurations d'équilibrage de charge suivantes :
> 1. Persistance de l'adresse IP source.
> 2. Persistance des ports de destination et des ports IP sources (disponible uniquement sur le modèle Cisco Content Services Switch).
> 3. Persistance SSL.
> 4. Persistance de session basée sur des cookies

> **Remarque**
>
> La persistance SSL peut entraîner des problèmes de sécurité et de fiabilité sur certains navigateurs Web. Vérifiez auprès de votre administrateur réseau si la persistance SSL est adaptée à votre organisation.

- SDK Java de connexion et de pilote d'accès aux données
  Ces SDK permettent de créer des pilotes de base de données pour le Connection Server et de gérer les connexions à la base de données.
- SDK Java de couche sémantique
  Le SDK Java de couche sémantique permet de développer une application Java assurant les tâches d'administration et de sécurité sur les univers et connexions. Par exemple, vous pouvez implémenter des services pour la publication d'un univers dans un référentiel ou l'extraction d'une connexion sécurisée d'un référentiel à votre espace de travail. Cette application peut être intégrée à des solutions de la plateforme de BI intégrant la plateforme de BI en tant qu'OEM.
- SDK Java et .NET de Report Application Server
  Les SDK de Report Application Server permettent aux applications d'ouvrir, de créer et de modifier des rapports Crystal existants, y compris de définir des valeurs de paramètres, de modifier des sources de données et d'exporter les données vers d'autres formats tels que XML, PDF, Microsoft Word et Microsoft Excel.
- Visualiseurs Java et .NET Crystal Reports
  Les visualiseurs permettent aux applications d'afficher et d'exporter des rapports Crystal. Les visualiseurs suivants sont disponibles :
  - Visualiseur de pages de rapport DHTML : présente les données et permet l'exploration, la navigation, le zoom, les invites, la recherche, la mise en surbrillance, l'exportation et l'impression.
  - Visualiseur de parties de rapport : permet de visualiser des parties de rapport, notamment des diagrammes, du texte et des champs.
- SDK Java et .NET du moteur de rapport
  Les SDK du moteur de rapport permettent aux applications d'interagir avec des rapports créés avec SAP BusinessObjects Web Intelligence.
  Les SDK du moteur de rapport incluent des bibliothèques pouvant être utilisées pour générer un outil de conception de rapports Web. Les applications générées avec ces SDK permettent de visualiser, créer ou modifier différents documents Web Intelligence. Les utilisateurs peuvent modifier les documents en ajoutant, supprimant ou modifiant des objets tels que des tableaux, des diagrammes, des conditions et des filtres.

- SDK de recherche de plateformes : le kit de développement de recherche de plateformes est l'interface entre l'application client et le service de recherche de plateformes. La recherche de plateformes prend en charge le SDK public intégré au SDK de recherche de plateformes.
  Lorsqu'un paramètre de requête de recherche est envoyé via l'application client à la couche du SDK, cette dernière convertit le paramètre de requête au format codé XML et le transmet au service de recherche de plateformes.

Les SDK peuvent être utilisés ensemble pour offrir un vaste choix de fonctions BI pour vos applications. Pour en savoir plus sur ces SDK, notamment les guides du développeur et références d'API, consultez la page de produit de la plateforme SAP BusinessObjects Business Intelligence.

3.1.7 Sources de données

3.1.7.1 Univers

L'univers est une couche sémantique qui simplifie les opérations sur les données en utilisant un langage pratique plutôt qu'un langage de données pour permettre l'accès aux données, leur manipulation et leur organisation. Ce langage pratique est stocké sous forme d'objets dans un fichier d'univers. Web Intelligence, Crystal Reports et d'autres applications utilisent des univers pour simplifier le processus de création utilisateur requis pour les requêtes et les analyses simples et complexes des utilisateurs finaux.

Les univers sont un composant central de la plateforme de BI. Tous les objets et connexions d'univers sont stockés et sécurisés dans le référentiel central par le Connection Server. Les outils client de conception d'univers doivent être connectés à la plateforme de BI pour accéder au système et créer des univers. L'accès aux univers et la sécurité au niveau des lignes/colonnes peuvent également être gérés au niveau des groupes ou des utilisateurs individuels depuis l'environnement de conception.

La couche sémantique permet à Web Intelligence de fournir des documents en utilisant plusieurs fournisseurs de données synchronisées, y compris des sources de données OLAP (Online Analytical Processing) et CWM (Common Warehousing Metamodel).

3.1.7.2 Vues d'entreprise

Les vues d'entreprise simplifient la création des rapports et l'interaction entre les rapports en simplifiant la complexité des données pour les développeurs de rapports. Les vues d'entreprise permettent de séparer les connexions de données, l'accès aux données, les éléments d'entreprise et le contrôle d'accès.

Les vues d'entreprise peuvent uniquement être utilisées par Crystal Reports et sont conçues pour simplifier la sécurité au moment de la visualisation et l'accès aux données requis pour la création de rapports Crystal. Les vues d'entreprise prennent en charge la combinaison de plusieurs sources de données dans une vue unique. Les vues d'entreprise sont totalement prises en charge sur la plateforme de BI.

3.1.8 Authentification et connexion unique

La sécurité du système est gérée par le CMS (Central Management Server), des plug-ins de sécurité et des outils d'authentification tiers tels que SiteMinder ou Kerberos. Ces composants authentifient les utilisateurs et autorisent l'accès utilisateur à la plateforme de BI, à ses dossiers et à d'autres objets.

Les plug-ins de sécurité de connexion unique d'authentification utilisateur suivants sont disponibles :

- Enterprise (par défaut), y compris la prise en charge de l'authentification sécurisée à utiliser avec des méthodes d'authentification comme SAML, X.509, la connexion unique SAP NW et autres méthodes prises en charge par votre serveur d'applications.
- LDAP
- Windows AD (Active Directory)

Lors de l'utilisation d'un système ERP (Enterprise Resource Planning), la connexion unique est utilisée pour authentifier l'accès utilisateur au système ERP de sorte que les rapports puissent être comparés aux données ERP. Les systèmes de connexion unique d'authentification utilisateur pour ERP suivants sont pris en charge :

- SAP ERP et Business Warehouse (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

3.1.8.1 Plug-ins de sécurité

Ils automatisent la création et la gestion des comptes en permettant de mapper des comptes et des groupes d'utilisateurs de systèmes tiers vers la plateforme de BI. Vous pouvez mapper des comptes utilisateur tiers à des comptes utilisateur Enterprise existants, ou créer des comptes utilisateur Enterprise qui correspondent à chaque entrée mappée dans le système externe.

Les plug-ins de sécurité mettent dynamiquement à jour les listes d'utilisateurs et de groupes tiers. Ainsi, après mappage d'un groupe LDAP (Lightweight Directory Access Protocol) ou Windows AD (Active Directory) à la plateforme de BI, tous les utilisateurs appartenant à ce groupe peuvent se connecter à la plateforme de BI. Les modifications apportées ultérieurement à l'appartenance à des groupes tiers sont automatiquement propagées.

La plateforme de BI prend en charge les plug-ins de sécurité suivants :

- Plug-in de sécurité Enterprise
  Le CMS (Central Management Server) gère les informations de sécurité, telles que les comptes utilisateur, l'appartenance aux groupes et les droits des objets qui définissent les droits des utilisateurs et des groupes. On parle alors d'authentification Enterprise.
  L'authentification Enterprise est toujours activée, elle ne peut pas être désactivée. Utilisez l'authentification Enterprise système par défaut si vous préférez créer des comptes et des groupes distincts à utiliser avec la plateforme de BI ou si vous n'avez pas encore configuré de hiérarchie d'utilisateurs et de groupes sur un serveur LDAP ou Windows AD.
  L'authentification sécurisée est un composant de l'authentification Enterprise s'intégrant aux solutions de connexion unique tierces, y compris JAAS (Java Authentication and Authorization Service). Les applications qui possèdent une sécurité établie avec le Central Management Server peuvent utiliser

l'authentification sécurisée pour permettre aux utilisateurs de se connecter sans entrer leurs mots de passe.

- Plug-in de sécurité LDAP
- Windows AD

> **Remarque**
>
> Bien qu'un utilisateur puisse configurer une authentification Windows AD pour la plateforme de BI et des applications personnalisées via la CMC, la CMC et la zone de lancement BI ne prennent pas en charge l'authentification Windows AD avec NTLM. Les seules méthodes d'authentification prises en charge par la CMC et la zone de lancement BI sont Windows AD avec Kerberos, LDAP, Enterprise et l'authentification sécurisée.

3.1.8.2 Intégration de Enterprise Resource Planning (ERP)

Les applications ERP (Enterprise Resource Planning, Planification des ressources de l'entreprise) soutiennent les fonctions essentielles des processus d'une entreprise en rassemblant des informations en temps réel relatives aux opérations quotidiennes. La plateforme de BI prend en charge la connexion unique et le reporting depuis les systèmes ERP suivants :

- SAP ERP et Business Warehouse (BW)
- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

> **Remarque**
>
> - La prise en charge SAP ERP et BW est installée par défaut. Utilisez l'option d'installation *Personnalisée/Etendue* pour désélectionner la prise en charge de l'intégration SAP si vous ne souhaitez pas la prise en charge de SAP ERP ou BW.
> - Les prises en charge de Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne et PeopleSoft ne sont pas installées par défaut. Utilisez l'option d'installation *Personnalisée/Etendue* pour sélectionner et installer l'intégration des systèmes ERP non SAP.

Pour obtenir des informations détaillées sur les versions spécifiques prises en charge par la plateforme de BI, consultez le document *Plateformes prises en charge/PAR* disponible à l'adresse : https://support.sap.com/home.html.

Pour configurer l'intégration d'ERP, consultez le chapitre *Configurations supplémentaires pour les environnements Enterprise Resource Planning* de ce guide.

3.1.9 Intégration SAP

La plateforme de BI s'intègre à votre infrastructure SAP existante avec les outils SAP suivants :

- Répertoire du paysage système (SLD)
  Le System Landscape Directory de SAP NetWeaver est la source centrale des informations d'infrastructure système pertinentes pour la gestion du cycle de vie du logiciel. Par le biais d'un répertoire contenant des informations sur tous les logiciels SAP pouvant être installés et de données mises à jour automatiquement sur les systèmes déjà installés dans un paysage, vous disposez d'un support outil pour planifier les tâches de cycle de vie du logiciel dans votre paysage système.
  Le programme d'installation de la plateforme de BI enregistre le fournisseur de contenus et les noms et versions des produits auprès du SLD, ainsi que les noms, versions et l'emplacement des serveurs et des composants front-end.
- SAP Solution Manager
  SAP Solution Manager est une plateforme fournissant le contenu intégré, les outils et méthodologies pour implémenter, prendre en charge, opérer et contrôler les solutions SAP et non SAP d'une entreprise.
  Un logiciel non SAP avec une intégration certifiée SAP est entré dans le référentiel central et transféré automatiquement à votre répertoire du paysage système SAP. Les clients SAP peuvent alors identifier aisément quelle version d'intégration de produit tiers a été certifiée par SAP dans leur environnement système SAP. Ce service offre une connaissance supplémentaire des produits tiers outre nos catalogues en ligne pour les produits tiers.
  SAP Solution Manager est accessible aux clients SAP sans coûts additionnels et comprend l'accès direct au support SAP et aux informations de répertoire de mise à niveau des produits SAP. Pour en savoir plus sur le SLD, voir « Enregistrement de la plateforme de BI dans le paysage système »
- CTS+ (Change and Transport System)
  Le CTS permet d'organiser des projets de développement dans ABAP Workbench et dans le Customizing, puis de transporter les modifications entre les systèmes SAP dans votre paysage système. Tout comme les objets ABAP, vous pouvez transporter des objets Java (J2EE, JEE) et des technologies non ABAP spécifiques à SAP (comme Web Dynpro Java ou SAP NetWeaver Portal) dans votre paysage.
- Surveillance avec CA Wily Introscope
  CA Wily Introscope est un produit de gestion d'applications Web qui permet de surveiller et de diagnostiquer les problèmes de performance susceptibles de se produire dans les modules SAP Java en production, y compris la visibilité dans les applications Java personnalisées et les connexions aux systèmes dorsaux. Il permet d'isoler les goulets d'étranglement au niveau de la performance dans les modules NetWeaver, y compris les servlets, JSP, EJB, JCO, les classes, méthodes, etc. Il offre une surveillance en temps réel avec un temps système réduit, une visibilité des transactions de bout en bout, des données historiques pour l'analyse ou la planification de la capacité, des tableaux de bord personnalisables, des alertes automatiques de dépassement de seuil et une architecture ouverte pour étendre la surveillance au-delà des environnements NetWeaver.

3.1.10 Contrôle de version intégrée

Les fichiers qui composent la plateforme de BI sur un serveur système gardés sous contrôle de version.
Le programme d'installation installera et configurera le système de contrôle de version Subversion ou vous pouvez saisir les renseignements pour utiliser un système de contrôle de version Subversion ou ClearCase existant.

Un système de contrôle de version permet la conservation et la restauration de diverses révisions de configuration et d'autres fichiers, ce qui signifie qu'il est toujours possible de faire reprendre le système à un état connu d'un moment quelconque du passé.

3.2 Serveurs, services, nœuds et hôtes

La plateforme de BI utilise les termes serveur et service pour désigner les deux types de logiciels s'exécutant sur un ordinateur de la plateforme de BI.

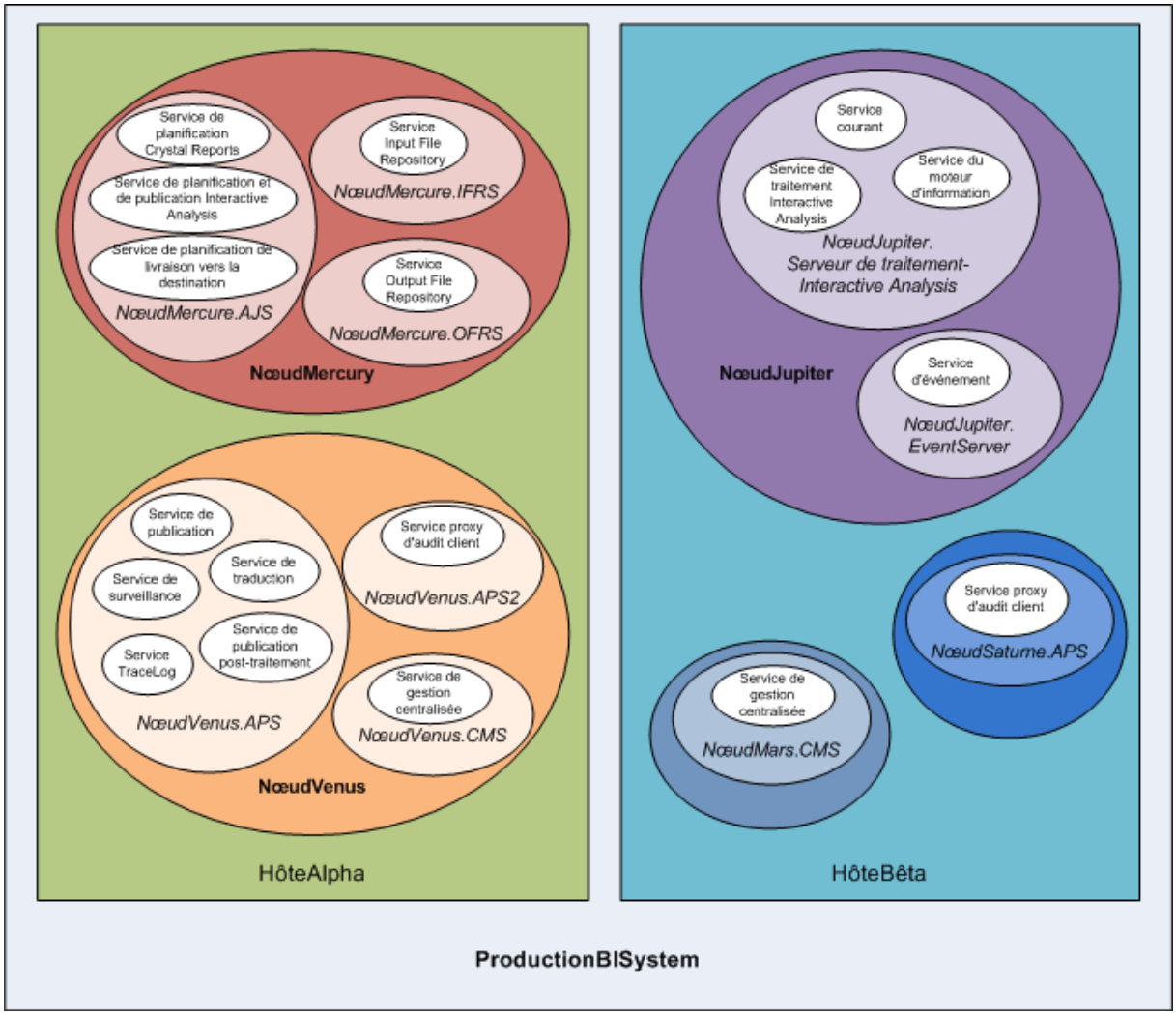
Le terme « serveur » sert à décrire un processus au niveau du système d'exploitation (appelé démon sur certains systèmes) qui héberge un ou plusieurs services. Par exemple, le CMS (Central Management Server) et le serveur de traitement adaptatif (Adaptive Processing Server) sont des serveurs. Un serveur s'exécute sous un compte système spécifique et possède son propre ID de processus (PID).

Un service est un sous-système de serveur qui exécute une fonction spécifique. Le service s'exécute dans l'espace mémoire de son serveur sous l'ID de processus du conteneur parent (serveur). Par exemple, le service de planification Web Intelligence est un sous-système qui s'exécute sur l'Adaptive Job Server.

Un nœud est un ensemble de serveurs de la plateforme de BI qui s'exécutent tous sur le même hôte et sont gérés par le même SIA (Server Intelligence Agent). Un même hôte peut contenir un ou plusieurs nœuds.

La plateforme de BI peut être installée sur un seul ordinateur, répartie sur plusieurs ordinateurs d'un intranet ou sur un réseau étendu (WAN).

Le diagramme suivant illustre une hypothèse d'installation de la plateforme de BI. Le nombre d'hôtes, nœuds, serveurs et services, ainsi que le type des serveurs et services, varient en dans les installations réelles.



Deux hôtes forment le cluster nommé ProductionBISystem :

- L'hôte nommé HostAlpha comporte l'installation de la plateforme de BI et est configuré de sorte à contenir deux nœuds :
  - NodeMercuy contient un Adaptive Job Server (`NodeMercury.AJS`) avec les services de planification et publication de rapports, un Input File Repository Server (`NodeMercury.IFRS`) avec un service de stockage des rapports d'entrée, ainsi qu'un Output File Repository Server (`NodeMercury.OFRS`) avec un service de stockage des rapports de sortie.
  - NodeVenus contient un serveur de traitement adaptatif (`NodeVenus.APS`) avec des services fournissant des fonctions de publication, de surveillance et de traduction, un serveur de traitement adaptatif (`NodeVenus.APS2`) avec un service d'audit client, ainsi qu'un Central Management Server (`NodeVenus.CMS`) avec un service fournissant les services du CMS.
- L'hôte nommé HostBeta comporte l'installation de la plateforme de BI et est configuré de sorte à contenir trois nœuds :
  - NodeMars contient un Central Management Server (`NodeMars.CMS`) avec un service fournissant les services du CMS. Le fait d'avoir le CMS sur deux ordinateurs permet d'avoir des fonctionnalités d'équilibrage des charges, d'atténuation et de basculement.

- NodeJupiter contient un serveur de traitement Web Intelligence (`NodeJupiter.Web Intelligence`) avec un service assurant le reporting Web Intelligence et un Event Server (`NodeJupiter.EventServer`) assurant la surveillance des rapports des fichiers.
- NodeSaturn contient un serveur de traitement adaptatif (`NodeSaturn.APS`) avec un service fournissant l'audit client.

3.2.1 Modifications des serveurs depuis la version XI 3.1

Le tableau suivant décrit les principales modifications de serveurs de la plateforme de BI depuis la version XI 3.1. Les types de modification comprennent :

- Les serveurs ayant changé de nom entre deux versions tout en offrant des fonctionnalités identiques ou similaires.
- Les serveurs qui ne sont plus proposés par les nouvelles versions.
- Les services communs ou associés ayant été consolidés sur les serveurs Adaptive.
  Par exemple, les services de planification fournis par des Job servers individuels dans la version XI 3.1 ont été déplacés vers l'Adaptive Job Server depuis la version 4.0.
- Les nouveaux serveurs ayant été introduits.

Modifications de serveur

XI 3.1	4,0	4.0 Feature Pack 3	4,1	4,2	4,3
Serveur de connexion [1]	Serveur de connexion Serveur de connexion 32	Serveur de connexion Serveur de connexion 32	Serveur de connexion Serveur de connexion 32	Serveur de connexion Serveur de connexion 32	Serveur de connexion Serveur de connexion 32
Crystal Reports Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server
Serveur de traitement Crystal Reports	Serveur de traitement Crystal Reports 2011 Serveur de traitement Crystal Reports (pour SAP Crystal Reports, pour les rapports Enterprise)	Serveur de traitement Crystal Reports 2011 Serveur de traitement Crystal Reports (pour SAP Crystal Reports, pour les rapports Enterprise)	Serveur de traitement Crystal Reports 2013 Serveur de traitement Crystal Reports (pour SAP Crystal Reports, pour les rapports Enterprise)	Serveur de traitement Crystal Reports 2016 Serveur de traitement Crystal Reports (pour SAP Crystal Reports, pour les rapports Enterprise)	Serveur de traitement Crystal Reports 2020 Serveur de traitement Crystal Reports (pour SAP Crystal Reports, pour les rapports Enterprise)
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (espaces de travail BI)	Non disponible depuis la version 4.0 Feature Pack 3	Non disponible dans la version 4.1	Non disponible dans la version 4.2	Non disponible dans la version 4.3

XI 3.1	4,0	4.0 Feature Pack 3	4,1	4,2	4,3
Serveur d'analyses de tableaux de bord (Dashboard Builder) [2]	Serveur d'analyses de tableaux de bord (espaces de travail BI)	Non disponible depuis la version 4.0 Feature Pack 3	Non disponible dans la version 4.1	Non disponible dans la version 4.2	Non disponible dans la version 4.3
Serveur de mise en cache Desktop Intelligence [3]	Non disponible depuis la version 4.0	Non disponible depuis la version 4.0	Non disponible dans la version 4.1 [3]	Non disponible dans la version 4.2 [3]	Non disponible dans la version 4.3 [3]
Desktop Intelligence Job Server [3]	Non disponible depuis la version 4.0	Non disponible depuis la version 4.0	Non disponible dans la version 4.1 [3]	Non disponible dans la version 4.2 [3]	Non disponible dans la version 4.3 [3]
Serveur de traitement Desktop Intelligence [3]	Non disponible depuis la version 4.0	Non disponible depuis la version 4.0	Non disponible dans la version 4.1 [3]	Non disponible dans la version 4.2 [3]	Non disponible dans la version 4.3 [3]
Destination Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server
Serveur Multi-Dimensional Analysis Services	Serveur de traitement adaptatif	Serveur de traitement adaptatif	Serveur de traitement adaptatif	Serveur de traitement adaptatif	Serveur de traitement adaptatif
Program Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server
Report Application Server (RAS)	Report Application Server (RAS) de Crystal Reports 2011	Report Application Server (RAS) de Crystal Reports 2011	Report Application Server (RAS) de Crystal Reports 2013	Report Application Server (RAS) de Crystal Reports 2016	Report Application Server (RAS) de Crystal Reports 2020
Web Intelligence Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server
Serveur de mise en cache Xcelsius [4]	Serveur de mise en cache Dashboard Design (Xcelsius) [5]	Serveur de mise en cache Dashboards (Xcelsius)	Serveur de mise en cache Dashboards (Xcelsius)	Serveur de mise en cache Dashboards (Xcelsius)	Non disponible dans la version 4.3 [7]
Serveur de traitement Xcelsius [4]	Serveur de traitement Dashboard Design (Xcelsius) [5]	Serveur de traitement Dashboards (Xcelsius)	Serveur de traitement Dashboards (Xcelsius)	Serveur de traitement Dashboards (Xcelsius)	Non disponible dans la version 4.3 [7]
Composants WebPart spécifiques au contenu [6]	Visualiseur Crystal Report, visualiseur Xcelsius et visualiseur de rapports analytiques	Visualiseur Crystal Report, visualiseur Xcelsius et visualiseur de rapports analytiques	Visualiseur Crystal Report, visualiseur Xcelsius et visualiseur de rapports analytiques	Visualiseur Crystal Report, visualiseur Xcelsius et visualiseur de rapports analytiques	Les composants WebPart spécifiques au contenu sont obsolètes dans la version 4.3.

- [1] Dans la version 4.0, Connection Server 32 est un serveur 32 bits qui exécute spécifiquement les connexions aux sources de données qui ne prennent pas en charge le middleware 64 bits. Connection

Server est un serveur 64 bits qui exécute les connexions vers toutes les autres sources de données. Pour en savoir plus, reportez-vous au *Guide d'accès aux données*.

- [2] Le serveur de tableaux de bord et le serveur d'analyses de tableaux de bord ont été supprimés dans la version 4.0 Feature Pack 3. La configuration de serveur n'est plus requise pour la fonctionnalité des espaces de travail BI (précédemment Dashboard Builder dans XI 3.1).
- [3] Desktop Intelligence n'était pas disponible dans la version 4.0 et les packages de maintenance 4.0. L'application client Desktop Intelligence est disponible dans la version 4.1, mais les serveurs Desktop Intelligence ne le sont pas. Les rapports Desktop Intelligence peuvent être convertis en documents Web Intelligence à l'aide de l'outil de conversion de rapport.
- [4] Les services de mise en cache et de traitement Xcelsius ont été introduits à partir de la version XI 3.1 Service Pack 3 pour optimiser les requêtes Query as a Web Service sur les sources de données relationnelles de Xcelsius. Des services de mise en cache et de traitement équivalents sont disponibles sur les serveurs de mise en cache et de traitement Dashboards introduits dans la version 4.0 Feature Pack 3.
- [5] Les serveurs Dashboard Design de la version 4.0 ont été renommés « Dashboards » dans la version 4.0 Feature Pack 3 pour s'aligner avec le changement de nom du produit en SAP BusinessObjects Dashboards.
- [6] Les composants WebPart spécifiques suivants sont obsolètes dans la version 4.3 :
  - Visualiseur Crystal Reports
  - Visualiseur Xcelsius
  - Visualiseur de rapports analytiques
- [7] Le serveur de traitement Dashboards (Xcelsius) et Dashboards Cache Server (Xcelsius) sont obsolètes.

3.2.2 Services

Lors de l'ajout de serveurs, vous devez inclure certains services sur l'Adaptive Job Server. Par exemple, le service de planification de livraison vers la destination.

> **Remarque**
>
> - Il se peut que de nouveaux types de services ou de serveurs soient ajoutés lors de futures versions de maintenance.
> - Un exemple de service de planification Java est utilisé uniquement à des fins de développement interne et ne peut être utilisé par des utilisateurs externes.

Service	Catégorie de service	Type de serveur	Description du service
Adaptive Connectivity Service	Services de connectivité	Serveur de traitement adaptatif	Fournit les services de connectivité aux pilotes Java
Service Analytics Hub	Services principaux	Serveur de traitement adaptatif	Ce service s'exécute sous le serveur de traitement adaptatif et communique avec le système SAP Analytics Cloud et SAP Analytics Hub.

Service	Catégorie de service	Type de serveur	Description du service
Service de planification de mise à jour de l'authentification	Services principaux	Adaptative Job Server	Fournit la synchronisation de mises à jour pour les plug-ins de sécurité tiers
Service d'applications Web BEx	Analysis Services	Serveur de traitement adaptatif	Fournit l'intégration des applications Web Business Explorer (BEx) de SAP Business Warehouse (BW) à la zone de lancement BI.
BIMobileService(OCA)	Services principaux	Serveur de traitement adaptatif	Active les notifications push sur les périphériques mobiles
Service conteneur d'applications Web	Services principaux	Serveur conteneur d'applications Web	Fournit des applications Web pour le WACS, y compris la CMC (Central Management Console), la zone de lancement BI et OpenDocument.
Service de gestion centralisée	Services principaux	Central Management Server	Fournit la gestion des serveurs, des utilisateurs, des sessions et de la sécurité (droits d'accès et authentification). Au moins un service de gestion centralisée doit être disponible dans un cluster pour que ce dernier fonctionne.
Service proxy d'audit client	Services principaux	Serveur de traitement adaptatif	Regroupe les événements d'audit envoyés par les clients et les transfère au serveur CMS.
Services de commentaires	Services principaux	Serveur de traitement adaptatif	Permet de réaliser des opérations sur les commentaires dans les documents
Service de traitement Crystal Reports 2020	Services Crystal Reports	Crystal Reports Processing Server	Accepte et traite les rapports Crystal Reports 2020 ; il peut partager des données entre les rapports pour réduire le nombre d'accès à la base de données.
Service de planification Crystal Reports 2020	Services Crystal Reports	Adaptative Job Server	Exécute les travaux Crystal Reports antérieurs planifiés et publie les résultats à un emplacement de sortie.
Service de modification et de visualisation Crystal Reports 2020	Services Crystal Reports	Report Application Server (RAS)	Traite les demandes d'affichage et de modification des rapports Crystal Reports 2020.

Service	Catégorie de service	Type de serveur	Description du service
Service de mémoire cache Crystal Reports	Services Crystal Reports	Crystal Reports Cache Server	Limite le nombre d'accès à la base de données générés depuis les rapports Crystal et accélère le reporting en gérant un cache des rapports.
Service de traitement Crystal Reports	Services Crystal Reports	Crystal Reports Processing Server	Accepte et traite les rapports Crystal ; il peut partager des données entre les rapports pour réduire le nombre d'accès à la base de données.
Service de planification Crystal Reports	Services Crystal Reports	Adaptative Job Server	Exécute les nouveaux travaux Crystal Reports planifiés et publie les résultats à un emplacement de sortie.
Service d'accès aux données personnalisé	Services Web Intelligence	Serveur de traitement adaptatif	Fournit des connexions dynamiques aux sources de données qui ne nécessitent pas un Connection Server. Ce service permet d'accéder aux rapports créés à l'aide de certains fournisseurs de données personnels comme les fichiers CSV et de les actualiser. Voir le *Guide de l'utilisateur SAP BusinessObjects Web Intelligence Rich Client* pour en savoir plus sur l'élaboration d'une requête ou l'actualisation d'un document basé sur un fichier texte.
Service de fédération de données	Services de fédération de données	Serveur de traitement adaptatif	Interroge et traite les sources de données sous-jacentes d'un univers à plusieurs sources

Service	Catégorie de service	Type de serveur	Description du service
Service de planification de livraison vers la destination	Services principaux	Adaptative Job Server	Exécute les travaux planifiés et publie les résultats à un emplacement de sortie comme un système de fichiers, un serveur FTP ou SFTP, le courrier électronique ou la boîte de réception d'un utilisateur. **Remarque** Lors de l'ajout de serveurs, vous devez inclure certains services d'Adaptive Job Server, y compris ce service.
Service de récupération de documents	Services Web Intelligence	Serveur de traitement adaptatif	Enregistrement automatique et récupération de documents Web Intelligence
Service du pont DSL	Services Web Intelligence	Serveur de traitement adaptatif	Prise en charge des sessions DSL (Dimensional Semantic Layer, couche sémantique dimensionnelle)
Service d'événement	Services principaux	Event Server	Surveille les événements de fichier d'un File Repository Server (FRS) et déclenche les rapports pour qu'ils s'exécutent lorsque c'est nécessaire
Service d'accès aux données Excel	Services Web Intelligence	Serveur de traitement adaptatif	Prend en charge les fichiers Excel téléchargés sur la plateforme de BI en tant que sources de données. Voir le *Guide de l'utilisateur SAP BusinessObjects Web Intelligence Rich Client* pour en savoir plus sur l'élaboration d'une requête ou l'actualisation d'un document basé sur un fichier Excel.
Service du moteur d'informations	Services Web Intelligence	Web Intelligence Processing Server	Service requis pour le traitement des documents Web Intelligence

Service	Catégorie de service	Type de serveur	Description du service
Service de stockage des fichiers d'entrée	Services principaux	Input File Repository Server	Gère les objets rapport publié et les objets programme pouvant être utilisés pour la génération de nouveaux rapports lors de la réception d'un fichier d'entrée.
Service Insight to Action	Services principaux	Serveur de traitement adaptatif	Permet l'appel d'actions et fournit une prise en charge du RRI.
Service ClearCase de la gestion des promotions	Services de gestion des promotions	Serveur de traitement adaptatif	Fournit une prise en charge ClearCase pour LCM
Service de planification de la gestion des promotions	Services de gestion des promotions	Adaptative Job Server	Exécute les travaux de gestion des promotions planifiés
Services de gestion des promotions	Services de gestion des promotions	Serveur de traitement adaptatif	Service principal de gestion des promotions
Service de surveillance	Services principaux	Serveur de traitement adaptatif	Fournit les fonctions de surveillance
Service MDAS (Multi-Dimensional Analysis Service)	Services Analysis	Serveur de traitement adaptatif	Fournit un accès aux données OLAP (Online Analytical Processing) multidimensionnelles, convertit au format XML les données brutes, qui peuvent être affichées dans des tableaux croisés et des diagrammes Excel, PDF ou Analysis (anciennement Voyager)
Service de connectivité natif	Services de connectivité	Serveur de connexion	Fournit des services de connectivité pour l'architecture 64 bits
Service de connectivité natif (32 bits)	Services de connectivité	Serveur de connexion	Fournit des services de connectivité pour l'architecture 32 bits
Service de stockage des fichiers de sortie	Services principaux	Output File Repository Server	Gère une collection de documents terminés
Service de planification de recherche de plateforme	Services principaux	Adaptative Job Server	Exécute des recherches planifiées pour indexer l'ensemble du contenu du référentiel du CMS (Central Management Server)
Service de recherche de plateformes	Services principaux	Serveur de traitement adaptatif	Fournit la fonctionnalité de recherche pour la plateforme de BI

Service	Catégorie de service	Type de serveur	Description du service
Service de planification de la métrique	Services principaux	Adaptative Job Server	Fournit les travaux de métrique planifiés et publie les résultats à un emplacement de sortie.
Service de planification du programme	Services principaux	Adaptative Job Server	Exécute les programmes qui ont été planifiés pour s'exécuter à un moment donné
Service de planification de la publication	Services principaux	Adaptative Job Server	Exécute les travaux de publication planifiés et publie les résultats à un emplacement de sortie.
Service de post-traitement de la publication	Services principaux	Serveur de traitement adaptatif	Réalise des actions sur les rapports lorsqu'ils sont terminés, comme l'envoi d'un rapport à un emplacement de sortie
Service de publication	Services principaux	Serveur de traitement adaptatif	Se coordonne avec le service de post-traitement de la publication et le service de travaux de destination pour publier les rapports à un emplacement de sortie comme un système de fichiers, un serveur FTP ou SFTP, le courrier électronique ou la boîte de réception d'un utilisateur.
Service Rebean	Services Web Intelligence	Serveur de traitement adaptatif	SDK utilisé par Web Intelligence et Explorer
Service de réplication	Services principaux	Adaptative Job Server	Exécute des travaux de fédération planifiés pour répliquer le contenu entre des sites fédérés
Service Web RESTful	Services principaux	Serveur conteneur d'applications Web (WACS)	Fournit la gestion des sessions pour les demandes de service Web RESTful.
Service de planification des requêtes de sécurité	Services principaux	Adaptative Job Server	Exécute les travaux de requêtes de sécurité planifiés
Service de jetons de sécurité	Services principaux	Serveur de traitement adaptatif	Prise en charge de la connexion unique SAP
Service de matérialisation des ensembles	Services principaux	Serveur de traitement adaptatif	Opère la matérialisation d'ensembles et de groupes d'ensembles
Service de planification de la matérialisation des ensembles	Services principaux	Adaptative Job Server	Permet de planifier des ensembles et des groupes d'ensembles pour la matérialisation.

Service	Catégorie de service	Type de serveur	Description du service
Service de traduction	Services principaux	Serveur de traitement adaptatif	Traduit les InfoObjects à l'aide d'informations du client Gestionnaire de traduction
Service de planification d'importation d'utilisateurs et de groupes	Services principaux	Adaptative Job Server	Permet la planification des importations de fichiers principaux
Service de planification de la différence visuelle	Services de gestion des promotions	Adaptative Job Server	Exécute les travaux de requête de différence visuelle (Gestion des promotions) et publie les résultats à un emplacement de sortie
Service de différence visuelle	Services de gestion des promotions	Serveur de traitement adaptatif	Détermine si les documents sont visuellement identiques pour la promotion de documents et la gestion des promotions
Service de visualisation	Services Web Intelligence	Serveur de traitement adaptatif	Service commun de visualisation des modèles d'objet, utilisé par Web Intelligence
Service commun Web Intelligence	Services Web Intelligence	Web Intelligence Processing Server	Prend en charge le traitement des documents Web Intelligence
Service principal Web Intelligence	Services Web Intelligence	Web Intelligence Processing Server	Prend en charge le traitement des documents Web Intelligence
Service de traitement Web Intelligence	Services Web Intelligence	Web Intelligence Processing Server	Accepte et traite les documents Web Intelligence
Service de planification Web Intelligence	Services Web Intelligence	Adaptative Job Server	Permet la prise en charge des travaux Web Intelligence planifiés
Service de gestion des versions	Services de gestion des promotions	Serveur de traitement adaptatif	Gère plusieurs versions des ressources BI à l'aide de IBM Rational ClearCase ou de Apache SubVersion

3.2.3 Catégories de service

> **Remarque**
>
> Il se peut que de nouveaux types de services ou de serveurs soient ajoutés lors de futures versions de maintenance.

Catégorie de service	Service	Type de serveur
Services Analysis	Service d'applications Web BEx	Adaptive Processing Server
Services Analysis	Service MDAS (Multi-Dimensional Analysis Service)	Serveur de traitement adaptatif
Services de connectivité	Adaptive Connectivity Service	Adaptive Processing Server
Services de connectivité	Service de connectivité natif	Serveur de connexion
Services de connectivité	Service de connectivité natif (32 bits)	Serveur de connexion
Services principaux	Service Analytics Hub	Serveur de traitement adaptatif
Services principaux	Service de planification de la mise à jour de l'authentification	Adaptative Job Server
Services principaux	BIMobileService(OCA)	Adaptive Processing Server
Services principaux	Service de gestion centralisée	Central Management Server
Services principaux	Service proxy d'audit client	Adaptive Processing Server
Services principaux	Service de commentaires	Adaptive Processing Server
Services principaux	Service de configuration de destination*	Adaptative Job Server
Services principaux	Service de planification de livraison vers la destination	Adaptative Job Server
Services principaux	Service d'événement	Event Server
Services principaux	Service Insight to Action	Adaptive Processing Server
Services principaux	Service de stockage des fichiers d'entrée	Input File Repository Server
Services principaux	Service de surveillance	Adaptive Processing Server
Services principaux	Service de stockage des fichiers de sortie	Output File Repository Server
Services principaux	Service de planification de recherche de plateformes	Adaptative Job Server
Services principaux	Service de recherche de plateformes	Adaptive Processing Server
Services principaux	Service de planification de la métrique	Adaptative Job Server
Services principaux	Service de planification du programme	Adaptative Job Server
Services principaux	Service de planification de la publication	Adaptative Job Server
Services principaux	Service de post-traitement de la publication	Serveur de traitement adaptatif
Services principaux	Service de publication	Adaptive Processing Server
Services principaux	Service Web RESTful	Serveur conteneur d'applications Web
Services principaux	Service de réplication	Adaptative Job Server
Services principaux	Service de planification des requêtes de sécurité	Adaptative Job Server

Catégorie de service	Service	Type de serveur
Services principaux	Service de jetons de sécurité	Adaptive Processing Server
Services principaux	Service de matérialisation des ensembles	Adaptive Processing Server
Services principaux	Service de planification de la matérialisation des ensembles	Serveur de traitement adaptatif
Services principaux	Service de connexion unique*	Central Management Server, Serveur de connexion, serveur de traitement Crystal Reports, RAS et serveur de traitement Web Intelligence
Services principaux	Service de journal de suivi	N'importe quel serveur
Services principaux	Service de traduction	Adaptive Processing Server
Services principaux	Service de planification d'importation d'utilisateurs et groupes*	Adaptative Job Server
Services principaux	Service conteneur d'applications Web*	Serveur conteneur d'applications Web
Services Crystal Reports	Service de traitement Crystal Reports 2020	Serveur de traitement Crystal Reports
Services Crystal Reports	Service de planification Crystal Reports 2020	Adaptative Job Server
Services Crystal Reports	Service de modification et de visualisation Crystal Reports 2020	RAS (Report Application Server)
Services Crystal Reports	Service de mise en cache Crystal Reports	Serveur de mise en cache Crystal Reports
Services Crystal Reports	Service de traitement Crystal Reports	Serveur de traitement Crystal Reports
Services Crystal Reports	Service de planification Crystal Reports	Adaptative Job Server
Services de fédération de données	Service de fédération de données	Adaptive Processing Server
Services de gestion du cycle de vie	Service ClearCase de la gestion des promotions	Adaptive Processing Server
Services de gestion du cycle de vie	Service de planification de la gestion des promotions	Adaptative Job Server
Services de gestion du cycle de vie	Service de gestion des promotions	Adaptive Processing Server
Services de gestion du cycle de vie	Service de planification de la différence visuelle	Adaptative Job Server
Services de gestion du cycle de vie	Service de différence visuelle	Adaptive Processing Server
Services Web Intelligence	Service d'accès aux données personnalisé	Adaptive Processing Server
Services Web Intelligence	Service de récupération de documents	Adaptive Processing Server
Services Web Intelligence	Service DSL Bridge	Adaptive Processing Server
Services Web Intelligence	Service d'accès aux données Excel	Adaptive Processing Server
Services Web Intelligence	Service de moteur d'informations	Serveur de traitement Web Intelligence
Services Web Intelligence	Service Rebean	Adaptive Processing Server

Catégorie de service	Service	Type de serveur
Services Web Intelligence	Service de visualisation	Adaptive Processing Server
Services Web Intelligence	Service commun Web Intelligence	Serveur de traitement Web Intelligence
Services Web Intelligence	Services principaux Web Intelligence	Serveur de traitement Web Intelligence
Services Web Intelligence	Service de surveillance Web Intelligence*	Adaptive Processing Server
Services Web Intelligence	Service de traitement Web Intelligence	Serveur de traitement Web Intelligence
Services Web Intelligence	Service de planification Web Intelligence	Adaptative Job Server
Services de gestion des promotions	Service de gestion des versions	Adaptive Processing Server

3.2.4 Types de serveurs

Un astérisque en regard d'un nom de service indique qu'il s'agit d'un service secondaire. Certains services secondaires sont créés automatiquement, mais vous pouvez choisir d'inclure d'autres services secondaires après sélection du service principal dont ils dépendent.

> **Remarque**
>
> Il se peut que de nouveaux types de services ou de serveurs soient ajoutés lors de futures versions de maintenance.

Type de serveur	Service	Catégorie de service
N'importe quel serveur	Service de journal de suivi	Services principaux
Adaptative Job Server	Service de planification de la mise à jour de l'authentification	Services principaux
Adaptative Job Server	Service de planification Crystal Reports 2020	Services Crystal Reports
Adaptative Job Server	Service de planification Crystal Reports	Services Crystal Reports
Adaptative Job Server	Service de configuration de destination*	Services principaux
Adaptative Job Server	Service de planification de livraison vers la destination	Services principaux
Adaptative Job Server	Service de planification de la gestion des promotions	Services de gestion des promotions
Adaptative Job Server	Service de planification de recherche de plateforme	Services principaux
Adaptative Job Server	Service de planification de la métrique	Services principaux
Adaptative Job Server	Service de planification du programme	Services principaux

Type de serveur	Service	Catégorie de service
Adaptative Job Server	Service de planification de la publication	Services principaux
Adaptative Job Server	Service de réplication	Services principaux
Adaptative Job Server	Service de planification des requêtes de sécurité	Services principaux
Adaptative Job Server	Services de planification de la matérialisation des ensembles	Services principaux
Adaptative Job Server	Service de planification d'importation d'utilisateurs et groupes*	Services principaux
Adaptative Job Server	Service de planification de la différence visuelle	Services de gestion des promotions
Adaptative Job Server	Service de planification Web Intelligence	Services Web Intelligence
Serveur de traitement adaptatif	Adaptive Connectivity Service	Services de connectivité
Serveur de traitement adaptatif	Services Analytics Hub	Services principaux
Serveur de traitement adaptatif	Service d'applications Web BEx	Analysis Services
Serveur de traitement adaptatif	Service proxy d'audit client	Services principaux
Serveur de traitement adaptatif	Service d'accès aux données personnalisé	Services Web Intelligence
Serveur de traitement adaptatif	Service de fédération de données	Services de fédération de données
Serveur de traitement adaptatif	Service de récupération de documents	Services Web Intelligence
Serveur de traitement adaptatif	Service DSL Bridge	Services Web Intelligence
Serveur de traitement adaptatif	Service d'accès aux données Excel	Services Web Intelligence
Serveur de traitement adaptatif	Service Insight to Action	Services principaux
Serveur de traitement adaptatif	Service ClearCase de la gestion des promotions	Services de gestion des promotions
Serveur de traitement adaptatif	Service de gestion des promotions	Services de gestion des promotions
Serveur de traitement adaptatif	Service de surveillance	Services principaux
Serveur de traitement adaptatif	Service MDAS (Multi-Dimensional Analysis Service)	Services Analysis
Serveur de traitement adaptatif	Service de recherche de plateformes	Services principaux
Serveur de traitement adaptatif	Service de post-traitement de la publication	Services principaux
Serveur de traitement adaptatif	Service de publication	Services principaux
Serveur de traitement adaptatif	Service Rebean	Services Web Intelligence
Serveur de traitement adaptatif	Service de jetons de sécurité	Services principaux
Serveur de traitement adaptatif	Service de matérialisation des ensembles	Services principaux

Type de serveur	Service	Catégorie de service
Serveur de traitement adaptatif	Service de traduction	Services principaux
Serveur de traitement adaptatif	Service de différence visuelle	Services de gestion des promotions
Serveur de traitement adaptatif	Service de visualisation	Services Web Intelligence
Serveur de traitement adaptatif	Service de surveillance Web Intelligence*	Services Web Intelligence
Central Management Server	Service de gestion centralisée	Services principaux
Central Management Server	Service de connexion unique*	Services principaux
Serveur de connexion	Service de connectivité natif	Services de connectivité
Serveur de connexion	Service de connectivité natif (32 bits)	Services de connectivité
Serveur de connexion	Service de connexion unique*	Services principaux
Crystal Reports Cache Server	Service de mémoire cache Crystal Reports	Services Crystal Reports
Crystal Reports Processing Server	Service de traitement Crystal Reports 2020	Services Crystal Reports
Crystal Reports Processing Server	Service de traitement Crystal Reports	Services Crystal Reports
Crystal Reports Processing Server	Service de connexion unique*	Services principaux
Event Server	Service d'événement	Services principaux
Input File Repository Server	Service de stockage des fichiers d'entrée	Services principaux
Output File Repository Server	Service de stockage des fichiers de sortie	Services principaux
Report Application Server (RAS)	Service de modification et de visualisation Crystal Reports 2020	Services Crystal Reports
RAS	Service de connexion unique*	Services principaux
Serveur conteneur d'applications Web	Service Web RESTful	Services principaux
Serveur conteneur d'applications Web	Service conteneur d'applications Web*	Services principaux
Web Intelligence Processing Server	Service du moteur d'informations	Services Web Intelligence
Web Intelligence Processing Server	Service de connexion unique*	Services principaux
Web Intelligence Processing Server	Service commun Web Intelligence	Services Web Intelligence
Web Intelligence Processing Server	Service principal Web Intelligence	Services Web Intelligence
Web Intelligence Processing Server	Service de traitement Web Intelligence	Services Web Intelligence

Type de serveur	Service	Catégorie de service
Adaptative Job Server	Service de planification de la mise à jour de l'authentification	Services principaux
Adaptative Job Server	Service de planification Crystal Reports 2020	Services Crystal Reports
Adaptative Job Server	Service de planification Crystal Reports	Services Crystal Reports

Type de serveur	Service	Catégorie de service
Adaptative Job Server	Service de planification de livraison vers la destination	Services principaux
Adaptative Job Server	Service de planification de la gestion des promotions	Services de gestion des promotions
Adaptative Job Server	Service de planification de recherche de plateforme	Services principaux
Adaptative Job Server	Service de planification de la métrique	Services principaux
Adaptative Job Server	Service de planification du programme	Services principaux
Adaptative Job Server	Service de planification de la publication	Services principaux
Adaptative Job Server	Service de réplication	Services principaux
Adaptative Job Server	Service de planification des requêtes de sécurité	Services principaux
Adaptative Job Server	Service de planification de la différence visuelle	Services de gestion des promotions
Adaptative Job Server	Service de planification Web Intelligence	Services Web Intelligence
Serveur de traitement adaptatif	Adaptive Connectivity Service	Services de connectivité
Serveur de traitement adaptatif	Service d'applications Web BEx	Analysis Services
Serveur de traitement adaptatif	Service proxy d'audit client	Services principaux
Serveur de traitement adaptatif	Service d'accès aux données personnalisé	Services Web Intelligence
Serveur de traitement adaptatif	Service de fédération de données	Services de fédération de données
Serveur de traitement adaptatif	Service de récupération de documents	Services Web Intelligence
Serveur de traitement adaptatif	Service DSL Bridge	Services Web Intelligence
Serveur de traitement adaptatif	Service d'accès aux données Excel	Services Web Intelligence
Serveur de traitement adaptatif	Service Insight to Action	Services principaux
Serveur de traitement adaptatif	Service ClearCase de la gestion des promotions	Services de gestion des promotions
Serveur de traitement adaptatif	Service de gestion des promotions	Services de gestion des promotions
Serveur de traitement adaptatif	Service de surveillance	Services principaux
Serveur de traitement adaptatif	Service MDAS (Multi-Dimensional Analysis Service)	Services Analysis
Serveur de traitement adaptatif	Service de recherche de plateformes	Services principaux
Serveur de traitement adaptatif	Service de post-traitement de la publication	Services principaux
Serveur de traitement adaptatif	Service de publication	Services principaux
Serveur de traitement adaptatif	Service Rebean	Services Web Intelligence

Type de serveur	Service	Catégorie de service
Serveur de traitement adaptatif	Service de jetons de sécurité	Services principaux
Serveur de traitement adaptatif	Service de traduction	Services principaux
Serveur de traitement adaptatif	Service de différence visuelle	Services de gestion des promotions
Serveur de traitement adaptatif	Service de visualisation	Services Web Intelligence
Central Management Server	Service de gestion centralisée	Services principaux
Serveur de connexion	Service de connectivité natif	Services de connectivité
Serveur de connexion	Service de connectivité natif (32 bits)	Services de connectivité
Crystal Reports Cache Server	Service de mémoire cache Crystal Reports	Services Crystal Reports
Crystal Reports Processing Server	Service de traitement Crystal Reports 2020	Services Crystal Reports
Crystal Reports Processing Server	Service de traitement Crystal Reports	Services Crystal Reports
Event Server	Service d'événement	Services principaux
Input File Repository Server	Service de stockage des fichiers d'entrée	Services principaux
Output File Repository Server	Service de stockage des fichiers de sortie	Services principaux
Report Application Server (RAS)	Service de modification et de visualisation Crystal Reports 2020	Services Crystal Reports
Serveur conteneur d'applications Web	Service Web RESTful	Services principaux
Web Intelligence Processing Server	Service du moteur d'informations	Services Web Intelligence
Web Intelligence Processing Server	Service commun Web Intelligence	Services Web Intelligence
Web Intelligence Processing Server	Service principal Web Intelligence	Services Web Intelligence
Web Intelligence Processing Server	Service de traitement Web Intelligence	Services Web Intelligence

3.2.5 Serveurs

Les serveurs sont un regroupement de services exécutés sous un SIA (Server Intelligence Agent) sur un hôte. Le type de serveur est signalé par les services qui y sont exécutés. Les serveurs peuvent être créés dans la CMC (Central Management Console). Le tableau suivant répertorie les différents types de serveurs pouvant être créés dans la CMC.

Serveur	Description
Adaptative Job Server	Serveur générique traitant les travaux planifiés. Lorsque vous ajoutez un Job Server au système de la plateforme de BI, vous pouvez configurer le Job Server pour traiter les rapports, documents, programmes ou publications et envoyer les résultats vers différentes destinations.

Serveur	Description
Serveur de traitement adaptatif	Serveur générique qui héberge les services responsables du traitement des demandes provenant de diverses sources. Le programme d'installation installe un serveur de traitement adaptatif (APS) par système hôte. Selon les fonctionnalités que vous avez installées, cet APS peut héberger un grand nombre de services, tels que le service de surveillance, le service de gestion du cycle de vie, le service d'analyse multidimensionnelle (MDAS), le service de publication et d'autres. Pour les systèmes de production ou de test, la meilleure méthode consiste à créer des APS supplémentaires, puis de les configurer pour répondre à vos exigences de gestion. Pour en savoir plus, voir Introduction à l'Assistant de configuration du système [page 90] et Configuration des serveurs de traitement adaptif (APS, Adaptive Processing Servers) pour les systèmes de production [page 464].
Central Management Server (CMS)	Gère une base de données d'informations concernant votre système de la plateforme de BI (dans la base de données système du CMS) et les actions utilisateur auditées (dans le magasin de données d'audit). Tous les services de plateforme sont gérés par le CMS. Le CMS contrôle également l'accès aux fichiers système où sont stockés les documents, les informations relatives aux utilisateurs, groupes d'utilisateurs, niveaux de sécurité (y compris l'authentification et l'autorisation) et le contenu.
Serveur de connexion	Permet l'accès de la base de données aux données source. Les bases de données relationnelles sont prises en charge, de même que OLAP et autres formats. Le Connection Server gère les connexions et l'interaction avec les diverses sources de données et fournit un ensemble de fonctions communes aux clients.
Crystal Reports Cache Server	Intercepte les demandes de rapport envoyées par les clients au Page Server. Si le Cache Server ne peut pas répondre à la demande avec une page de rapport mise en cache, il transmet la demande au serveur de traitement Crystal Reports, qui exécute le rapport et renvoie les résultats. Le Cache Server met alors la page de rapport en mémoire cache en vue d'une potentielle utilisation ultérieure.
Crystal Reports Processing Server	Répond aux demandes de page en traitant les rapports et en générant des pages au format de page encapsulée (EPF). L'avantage clé du format EPF est qu'il prend en charge l'accès aux pages à la demande, si bien que seule la page demandée est renvoyée et non le rapport complet. Cela améliore les performances système et réduit le trafic réseau inutile dans le cas de grands rapports.
Event Server	Surveille les événements du système qui peuvent déclencher l'exécution d'un rapport. Lorsque vous configurez un déclenchement d'événement, l'Event Server

Serveur	Description
	surveille la condition et notifie au CMS l'exécution d'un événement. Le CMS peut ensuite démarrer tous les travaux configurés pour s'exécuter lors de l'événement. L'Event Server gère les événements basés sur des fichiers qui se produisent dans le niveau de stockage.
File Repository Server	En charge de la création des objets système de fichiers, tels que les rapports exportés, et des fichiers importés dans des formats non natifs. Un Input FRS stocke les objets de rapport et de programme qui ont été publiés sur le système par les administrateurs et les utilisateurs finaux. Un Output FRS stocke toutes les instances de rapport générées par le Job Server.
Web Intelligence Processing Server	Traite les documents SAP BusinessObjects Web Intelligence.
Report Application Server	Fournit des fonctionnalités de reporting ad hoc permettant aux utilisateurs de créer et de modifier des rapports Crystal via le SDK (Software Development Kit) de SAP Crystal Reports Server Embedded.

3.3 Applications client

Vous pouvez interagir avec la plateforme de BI en utilisant deux types principaux d'applications client :

- Applications de bureau
  Ces applications doivent être installées sur un système d'exploitation Microsoft Windows pris en charge. Elles peuvent traiter des données et créer des rapports localement.

  > **Remarque**
  >
  > Le programme d'installation de la plateforme de BI n'installe plus les applications de bureau. Pour installer des applications de bureau sur un serveur, utilisez le programme d'installation autonome des outils client de la plateforme SAP BusinessObjects Business Intelligence.

  Les applications client de bureau permettent de décharger une partie du traitement des rapports BI sur des ordinateurs client individuels. La plupart des applications de bureau accèdent directement aux données de votre organisation via des pilotes installés sur le bureau et communiquent avec votre déploiement de la plateforme de BI via CORBA ou CORBA SSL crypté.
  Crystal Reports et Live Office sont des exemples de ce type d'application.

  > **Remarque**
  >
  > Bien que Live Office soit une application à fonctionnalité riche, elle forme une interface avec les services Web de la plateforme de BI via HTTP.

- Applications Web
  Ces applications sont hébergées par un serveur d'applications Web et sont accessibles via un navigateur Web pris en charge sur les systèmes d'exploitation Windows, Macintosh, Unix et Linux.

Cela permet de fournir un accès Business Intelligence (BI) à de grands groupes d'utilisateurs, sans avoir à déployer de logiciels de bureau. La communication est assurée via HTTP avec ou sans cryptage SSL (HTTPS).
La zone de lancement BI, SAP BusinessObjects Web Intelligence, la CMC (Central Management Console) et les visualiseurs de rapport sont des exemples de ce type d'application.

3.3.1 Installées avec les outils client de la plateforme SAP BusinessObjects Business Intelligence

3.3.1.1 Web Intelligence Rich Client

Web Intelligence Rich Client est un outil d'analyse et de reporting ad-hoc conçu pour les utilisateurs professionnels avec ou sans accès à la plateforme de BI.

Il permet aux utilisateurs d'accéder aux données via des univers (.unv et .unx), des requêtes ou d'autres sources, en utilisant des termes de gestions familiers dans une interface avec fonctionnalité glisser-déposer. Les workflows permettent d'analyser les questions très larges ou très ciblées et de poser d'autres questions au cours du workflow d'analyse.

Les utilisateurs de Web Intelligence Rich Client peuvent continuer à utiliser des fichiers de document Web Intelligence (.wid), même s'ils ne peuvent pas se connecter à un CMS (Central Management Server).

> ⓘ Remarque
>
> - Il est déconseillé d'installer Web Intelligence Rich Client sur le même ordinateur que les serveurs de la plateforme de BI. Web Intelligence Rich Client et les serveurs de la plateforme de BI ont des fichiers binaires en commun, ce qui peut poser des problèmes lors de votre déploiement si vous effectuez une montée de version de l'installation (client ou serveur). Si vous installez Web Intelligence Rich Client, installez-le sur un ordinateur distinct.
> - Si vous effectuez une mise à niveau depuis 4.2, assurez-vous d'arrêter et de fermer la version précédente avant d'installer la version 4.3. Vérifiez la barre d'état du système Windows, Rich Client peut être réduit et est toujours en cours d'exécution.

3.3.1.2 Gestionnaire de vues d'entreprise

Le Gestionnaire de vues d'entreprise permet aux utilisateurs de créer des objets de couche sémantique qui simplifient la complexité des bases de données sous-jacentes.

Le Gestionnaire de vues d'entreprise permet de créer des connexions de données, des connexions de données dynamiques, des fondations de données, des éléments d'entreprise, des vues d'entreprise et des vues relationnelles. Il permet aussi de définir une sécurité détaillée au niveau des colonnes et des lignes pour les objets d'un rapport.

Les concepteurs peuvent créer des connexions à plusieurs sources de données, joindre des tables, créer des alias pour des noms de champs, des champs calculés, puis utiliser cette structure simplifiée sous forme de vue

d'entreprise. Les concepteurs et les utilisateurs de rapports peuvent ensuite utiliser la vue d'entreprise comme base de leurs rapports, plutôt qu'accéder directement aux données et créer leurs propres requêtes.

3.3.1.3 Outil de conversion de rapport

RCT est obsolète dans la version BI 4.3. Pour en savoir plus, voir la note SAP 2801797

3.3.1.4 Outil de conception d'univers

L'Outil de conception d'univers (anciennement Universe Designer) permet aux concepteurs de données de combiner les données de plusieurs sources dans une couche sémantique qui masque la complexité des bases de données aux utilisateurs finaux. Il simplifie la complexité des données en utilisant un langage métier plutôt qu'un langage technique pour les parcourir, les manipuler et les organiser.

L'outil de conception d'univers fournit une interface graphique pour sélectionner et visualiser les tables d'une base de données. Les tables de bases de données sont représentées par des symboles de tables dans un diagramme de schéma. Les concepteurs peuvent utiliser cette interface pour manipuler des tables, créer des jointures entre les tables, des tables d'alias et des contextes et résoudre des boucles dans un schéma.

Vous pouvez également créer des univers à partir de sources de métadonnées. L'outil de conception d'univers est utilisé pour générer des univers à la fin du processus de création.

3.3.1.5 Outil de conception d'information

L'outil de conception d'information (anciennement Information Designer) est un environnement de conception de métadonnées qui permet au concepteur d'extraire, de définir et de manipuler les métadonnées de sources relationnelles et OLAP pour créer et déployer des univers SAP BusinessObjects.

3.3.1.6 Outil de gestion de la traduction

La plateforme de BI prend en charge les documents et univers multilingues. Un document multilingue contient des versions localisées des métadonnées d'univers et des invites de document. Par exemple, un utilisateur peut créer des rapports à partir du même univers dans les langues de son choix.

L'outil de gestion de la traduction (anciennement Gestionnaire de traduction) définit les univers multilingues et gère la traduction des univers, ainsi que d'autres ressources de rapport et d'analyse du référentiel du CMS.

Outil de gestion de la traduction :

- Traduit l'univers ou les documents pour un public multilingue.
- Définit les parties métadonnées du document et la traduction appropriée. Génère un format XLIFF externe et importe les fichiers XLIFF pour obtenir des informations traduites.

- Indique la structure de l'univers ou des documents à traduire.
- Permet de traduire les métadonnées via l'interface utilisateur ou par le biais d'un outil de traduction externe en important et en exportant des fichiers XLIFF.
- Crée des documents multilingues.

3.3.1.7 Outil d'administration de fédération de données

L'Outil d'administration de fédération de données (anciennement Data Federator) est une application Rich Client qui offre des fonctionnalités faciles à utiliser pour gérer votre service de fédération de données.

Etroitement intégré à la plateforme de BI, le service de fédération de données active les univers à plusieurs sources en diffusant les requêtes dans plusieurs sources de données et vous permet ainsi de fédérer les données par le biais d'une fondation de données unique.

L'outil d'administration de fédération de données vous permet d'optimiser les requêtes de fédération de données et d'ajuster le moteur de recherche de fédération de données en vue d'obtenir les meilleures performances possibles.

Il permet d'effectuer les opérations suivantes :

- Tester les requêtes SQL.
- Visualiser les plans d'optimisation qui détaillent la façon dont les requêtes sont transmises à chaque source.
- Calculer des statistiques et définir des paramètres système pour ajuster les services de fédération de données et obtenir les meilleures performances possibles.
- Gérer les propriétés afin de contrôler la façon dont les requêtes sont exécutées dans chaque source de données au niveau du connecteur.
- Surveiller les requêtes SQL en cours.
- Parcourir l'historique des requêtes exécutées.

3.3.2 Installées avec la plateforme SAP BusinessObjects Business Intelligence

3.3.2.1 Central Configuration Manager (CCM)

Le CCM (Central Configuration Manager) est un outil de gestion de nœuds et de dépannage de serveurs proposé sous deux formes. Dans un environnement Microsoft Windows, le CCM permet de gérer des serveurs locaux et distants via son interface utilisateur graphique ou depuis une ligne de commande. Dans un environnement Unix, le script shell du CCM (`ccm.sh`) permet de gérer les serveurs à partir de la ligne de commande.

Le CCM vous permet de créer et de configurer des nœuds et de démarrer ou arrêter votre serveur d'applications Web, s'il s'agit du serveur d'applications Web Tomcat fourni par défaut. Sous Windows, il permet également de configurer des paramètres réseau, tels que le cryptage SSL (Secure Socket Layer). Ces paramètres s'appliquent à tous les serveurs d'un même nœud.

> **Remarque**
>
> La plupart des tâches de gestion des serveurs sont à présent gérées via la CMC, et non via le CCM. Désormais, le CCM est utilisé pour le dépannage et la configuration des nœuds.

3.3.2.2 Outil de gestion de mise à niveau

UMT est obsolète dans la version BI 4.3. Pour en savoir plus, voir la note SAP 2801797

3.3.2.3 Outil de diagnostic de référentiel

L'outil de diagnostic de référentiel permet d'analyser, de diagnostiquer et de réparer les incohérences qui peuvent se produire entre la base de données système du CMS (Central Management Server) et le stockage des fichiers FRS (File Repository Servers).

Il permet également de créer un rapport sur le statut de réparation et les actions exécutées. Pour déterminer la synchronisation entre le système de fichiers et la base de données, le RDT doit être utilisé après la première exécution d'une sauvegarde à chaud par l'utilisateur. Il peut également être utilisé après une restauration et avant le démarrage des services de la plateforme de BI. L'utilisateur peut définir une limite pour le nombre d'erreurs trouvées et réparées par le RDT avant l'arrêt.

3.3.3 Disponibles séparément

3.3.3.1 SAP BusinessObjects Analysis, édition pour Microsoft Office

SAP BusinessObjects Advanced Analysis, édition pour Microsoft Office constitue une alternative de premier choix à Business Explorer (BEx) en permettant aux analystes professionnels d'explorer des données OLAP (Online Analytical Processing) multidimensionnelles.

Les analystes peuvent ainsi répondre rapidement aux questions de gestion et partager avec d'autres utilisateurs leurs analyses et leur espace de travail sous forme d'*analyses*.

SAP BusinessObjects Analysis, édition pour Microsoft Office, fournit aux analystes la possibilité :

- D'identifier les tendances, les extrêmes et les détails stockés dans les systèmes financiers sans l'aide d'un administrateur de base de données.
- D'obtenir des réponses à leurs questions de gestion efficacement en consultant des jeux de données multidimensionnels de petite ou grande taille.
- D'accéder à l'ensemble des sources de données OLAP disponibles au sein de l'entreprise et de partager les résultats à l'aide d'une interface intuitive simple.
- D'accéder aux différentes sources de données OLAP des mêmes analyses pour obtenir un aperçu complet de l'activité et de l'impact croisé des tendances.

- D'interroger, d'analyser, de comparer et de prévoir les facteurs d'activité.
- D'utiliser une gamme complète de calculs de gestion et temporels.

3.3.3.2 SAP Crystal Reports

Le logiciel SAP Crystal Reports permet aux utilisateurs de concevoir des rapports interactifs à partir d'une source de données.

3.3.3.3 SAP Lumira

L'application SAP Lumira aide à visualiser les données et à créer des récits portant sur celles-ci. SAP Lumira permet de manipuler, modifier, mettre en forme et affiner vos données, créer des visualisations pour représenter les données sous forme de graphique et partager vos visualisations à l'aide de récits.

SAP Lumira est à présent répertorié comme une application de la CMC, ce qui permet de gérer les droits relatifs à la fonctionnalité d'acquisition de données et de partage de contenu de SAP Lumira pour chaque utilisateur ou groupe d'utilisateurs.

> ⓘ Remarque
>
> Tous les événements associés à l'application SAP Lumira sont enregistrés sans ID client dans la base de données d'audit.

3.3.4 Clients d'applications Web

Les clients d'applications Web résident sur un serveur d'applications Web et sont accessibles sur un navigateur Web client. Les applications Web sont déployées automatiquement lors de l'installation de la plateforme de BI.

Les applications Web sont facilement accessibles depuis un navigateur Web et la communication peut être sécurisée par cryptage SSL si vous planifiez d'autoriser un accès utilisateur externe au réseau de votre organisation.

De plus, les applications Web Java peuvent être reconfigurées ou déployées après l'installation initiale en utilisant l'outil de ligne de commande WDeploy fourni, qui permet de déployer des applications Web sur un serveur d'applications Web comme suit :

1. Mode autonome
   Toutes les ressources d'applications Web sont déployées sur un serveur d'applications Web qui sert à la fois le contenu statique et dynamique. Ce mode est adapté aux petites installations.
2. Mode divisé
   Le contenu statique de l'application Web (HTML, images, CSS) est déployé sur un serveur Web dédié alors que le contenu dynamique (JSP) est déployé sur un serveur d'applications Web. Ce mode est adapté aux installations plus importantes qui bénéficient du fait que le serveur d'applications Web n'a pas à servir le contenu Web statique.

Pour en savoir plus sur WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

3.3.4.1 Central Management Console (CMC)

La CMC (Central Management Console) est un outil Web à utiliser pour effectuer les tâches administratives (dont la gestion des utilisateurs, du contenu et des serveurs) et pour configurer les paramètres de sécurité. La CMC étant une application Web, vous pouvez effectuer toutes les tâches d'administration dans un navigateur Web, sur tout ordinateur pouvant se connecter au serveur d'applications Web.

Seuls les membres du groupe Administrateurs peuvent modifier les paramètres de gestion, à moins que les droits pour le faire ne soient explicitement accordés à un utilisateur. Des rôles peuvent être affectés dans la CMC afin d'accorder des droits d'utilisateurs pour effectuer des tâches administratives mineures comme la gestion des utilisateurs d'un groupe ou des rapports dans les dossiers appartenant à une équipe.

3.3.4.2 Zone de lancement BI façon Fiori

La zone de lancement BI façon Fiori (précédemment connue sous le nom d'InfoView) est une interface Web à laquelle les utilisateurs finaux accèdent pour afficher, planifier et suivre les rapports Business Intelligence (BI) publiés. La zone de lancement BI façon Fiori permet d'accéder à n'importe quel type de document de Business Intelligence, dont les rapports, les analyses et les tableaux de bord, et aussi d'interagir avec eux et de les exporter.

La zone de lancement BI façon Fiori permet aux utilisateurs de gérer :

- la navigation et la recherche dans le contenu BI,
- l'accès au contenu BI (création, édition et visualisation),
- la planification et la publication du contenu BI.

3.3.4.3 Espaces de travail BI

Les espaces de travail BI aident à suivre les activités commerciales et les performances à l'aide de modules (modèles de données) et des espaces de travail Business Intelligence (BI) (visualisation de données dans un ou plusieurs modules). Les modules et les espaces de travail BI fournissent les informations nécessaires à l'ajustement des règles de gestion lorsque les conditions changent. Cela vous aide à suivre et à analyser les données de gestion clés via les modules et les espaces de travail BI de gestion. L'analyse et la prise de décision en groupe sont également prises en charge via les fonctionnalités de collaboration et de workflow intégrées. Les espaces de travail BI offrent les fonctions suivantes :

- La navigation par onglet
- Création de pages : gestion des espaces de travail BI et des modules
- Un générateur d'application interactif
- La liaison de contenu entre modules pour une analyse approfondie des données

> **Remarque**
>
> La liaison de contenu n'est pas prise en charge pour les documents Design Studio.

3.3.4.4 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence désigne un outil Web qui fournit des fonctionnalités de requête, de reporting et d'analyse pour les sources de données relationnelles dans un produit Web unique.

Il permet aux utilisateurs de créer des rapports, d'effectuer des requêtes ad hoc, d'analyser des données et de mettre en forme des rapports dans une interface autorisant le glisser-déposer. Web Intelligence masque la complexité des sources de données sous-jacentes.

Les rapports peuvent être publiés sur un portail Web pris en charge ou dans des applications Microsoft Office à l'aide de SAP BusinessObjects Live Office.

3.3.4.5 SAP BusinessObjects Analysis, édition pour OLAP

SAP BusinessObjects Analysis, édition pour OLAP (anciennement Voyager) désigne un outil OLAP (Online Analytical Processing) figurant sur le portail de la zone de lancement BI, qui permet d'utiliser des données multidimensionnelles. Il permet aussi de combiner des informations issues de différentes sources de données OLAP dans un espace de travail unique. Les fournisseurs OLAP pris en charge incluent SAP BW et Microsoft Analysis Services.

L'ensemble de fonctions d'Analysis, édition pour OLAP combine les éléments de SAP Crystal Reports (accès direct aux données des cubes OLAP à des fins de reporting de production) et de la solution SAP BusinessObjects Web Intelligence (reporting analytique ad hoc avec les univers des sources de données OLAP). Il offre une gamme de calculs d'activité et de temps et inclut des fonctions telles que les curseurs de temps pour rendre l'analyse des données OLAP aussi simple que possible.

> **Remarque**
>
> L'application Web Analysis, édition pour OLAP est uniquement disponible sous forme d'application Web Java. Il n'existe pas d'application correspondante pour .NET.

3.3.4.6 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile permet aux utilisateurs d'accéder à distance aux mêmes rapports, métriques et données en temps réel Business Intelligence (BI) disponibles dans les applications client de bureau depuis un appareil sans fil. Le contenu est optimisé pour les périphériques mobiles de sorte que les utilisateurs peuvent facilement accéder aux rapports courants, naviguer dans ces rapports et les analyser sans aucune formation supplémentaire.

Avec SAP BusinessObjects Mobile, les responsables et les techniciens de l'information disposent en permanence de données à jour sur la base desquelles ils peuvent prendre des décisions avisées. Les équipes

de vente et service après-vente peuvent fournir à tout moment des informations pertinentes relatives au client, au produit et à l'ordre de travail.

SAP BusinessObjects Mobile prend en charge une large gamme de périphériques mobiles, y compris BlackBerry, Windows Mobile et Symbian.

Pour en savoir plus sur l'installation, la configuration et le déploiement Mobile, reportez-vous au *Guide d'installation et de déploiement de SAP BusinessObjects Mobile*. Pour en savoir plus sur l'utilisation de SAP BusinessObjects Mobile, reportez-vous au guide *Utilisation de SAP BusinessObjects Mobile*.

3.4 Workflows de traitement

Lors de l'exécution de tâches telles que la connexion, la planification ou la visualisation d'un rapport, des flux d'informations qui transitent sur le système et les serveurs communiquent entre eux. La section suivante décrit certains des flux de traitement tels qu'ils se produisent dans la plateforme de BI.

Pour visualiser d'autres workflows de processus avec des supports visuels voir les tutoriels produit officiels de la plateforme SAP BusinessObjects Business Intelligence 4.x à l'adresse : http://scn.sap.com/docs/DOC-8292

3.4.1 Démarrage et authentification

3.4.1.1 Connexion à la plateforme de BI

Ce workflow décrit une connexion utilisateur à une application Web de la plateforme de BI partir d'un navigateur Web. Ce workflow s'applique aux applications Web telles que la zone de lancement BI et la CMC (Central Management Console).

1. Le navigateur (client Web) envoie la demande de connexion via le serveur Web au serveur d'applications Web où s'exécute l'application Web.
2. Le serveur d'applications Web détermine qu'il s'agit d'une requête de connexion. Le serveur d'applications Web envoie le nom d'utilisateur, le mot de passe et le type d'authentification au CMS pour authentification.
3. Le CMS valide le nom d'utilisateur et le mot de passe par rapport à la base de données appropriée. Dans ce cas, l'authentification Enterprise est utilisée et les références de l'utilisateur sont authentifiées par rapport à la base de données système du CMS.
4. Une fois la validation réussie, le CMS crée une session pour l'utilisateur dans la mémoire.
5. Le CMS envoie une réponse au serveur d'applications Web pour l'aviser que la validation a réussi.
6. Le serveur d'applications Web génère un jeton de connexion pour la session utilisateur dans la mémoire. Durant la reste de la session, le serveur d'applications Web utilise le jeton de connexion pour valider l'utilisateur auprès du CMS. Le serveur d'applications Web génère la page Web suivante pour l'envoyer au client Web.
7. Le serveur d'applications Web envoie la page Web suivante au serveur Web.
8. Le serveur Web envoie la page Web au client Web, où elle s'affiche dans le navigateur de l'utilisateur.

3.4.1.2 Démarrage du SIA

Un SIA (Server Intelligence Agent) peut être configuré pour démarrer automatiquement avec le système d'exploitation hôte ou manuellement avec le CCM (Central Configuration Manager).

Un SIA extrait des informations sur les serveurs qu'il gère depuis un CMS (Central Management Server). Si le SIA utilise un CMS local et que celui-ci n'est pas en cours d'exécution, le SIA le démarre. Si un SIA utilise un CMS distant, il tente de s'y connecter.

Une fois le SIA lancé, la séquence d'événements ci-après est exécutée.

1. Le SIA recherche un SMS dans son cache.
   a. Si le SIA est configuré pour démarrer un CMS local et que le CMS n'est pas en cours d'exécution, le SIA le démarre et se connecte.
   b. Si le SIA est configuré pour utiliser un CMS en cours d'exécution (local ou distant), il tente de se connecter au premier CMS dans son cache. Si ce CMS n'est pas disponible, il tente de se connecter au CMS suivant dans son cache. Si aucun des CMS mis en cache n'est disponible, le SIA attend qu'un CMS soit disponible.
2. Le CMS confirme l'identité du SIA pour s'assurer qu'il est valide.
3. Une fois le SIA connecté à un CMS, il demande une liste de serveurs à gérer.

   > **Remarque**
   >
   > Le SIA ne stocke pas d'informations sur les serveurs qu'il gère. Les informations de configuration qui déterminent quel serveur est géré par un SIA sont stockées dans la base de données système du CMS et sont extraites du CMS par le SIA à son démarrage.

4. Le CMS demande à la base de données système du CMS la liste des serveurs gérés par le SIA. La configuration de chaque serveur est également extraite.
5. Le CMS renvoie au SIA la liste des serveurs et leur configuration.
6. Le SIA lance chaque serveur configuré pour démarrer automatiquement avec la configuration correspondante et surveille son statut. Chaque serveur lancé par le SIA est configuré pour utiliser le même CMS que le SIA.

   Les serveurs non configurés pour démarrer automatiquement avec le SIA ne sont pas lancés.

3.4.1.3 Fermeture du SIA

Le SIA (Server Intelligence Agent) s'arrête automatiquement quand vous arrêtez le système d'exploitation de l'hôte. Sinon, vous pouvez arrêter manuellement le SIA dans le CCM (Central Configuration Manager).

A la fermeture du SIA, les étapes suivantes sont exécutées :

Le SIA informe le CMS qu'il est en cours de fermeture.

a. Si le SIA est en cours d'arrêt car le système d'exploitation hôte se referme, il demande à ses serveurs de s'arrêter. Les serveurs qui ne s'arrêtent pas au bout de 25 secondes sont forcés de s'arrêter.
b. Si le SIA est arrêté manuellement, il attend que le serveur géré ait terminé de traiter les travaux existants. Dans ce cas, les serveurs gérés n'acceptent pas de nouveaux travaux. Une fois les travaux terminés, les serveurs s'arrêtent. Lorsque tous les serveurs sont arrêtés, le SIA s'arrête également.

Lors d'un arrêt forcé, le SIA ordonne à tous les serveurs gérés de s'arrêter immédiatement.

3.4.2 Objets de programme

3.4.2.1 Définition de la planification d'un objet programme

Ce workflow décrit la manière dont un utilisateur planifie l'exécution d'un objet programme à une heure future à partir d'une application Web comme la CMC (Central Management Console) ou la zone de lancement BI.

1. L'utilisateur envoie la demande de planification au serveur d'applications Web à partir du client Web, via le serveur Web.
2. Le serveur d'applications Web interprète la demande et détermine qu'il s'agit d'une demande de planification. Le serveur d'applications Web envoie l'heure de planification, les valeurs de connexion à la base de données, les valeurs des paramètres, la destination et le format au CMS (Central Management Server) spécifié.
3. Le CMS vérifie si l'utilisateur dispose des droits appropriés pour planifier l'objet. Si l'utilisateur dispose de droits suffisants, le CMS ajoute un nouvel enregistrement à la base de données système du CMS et ajoute l'instance à sa liste de planifications en attente.
4. Le CMS envoie une réponse confirmant la réussite de l'opération de planification au serveur d'applications Web.
5. Le serveur d'applications Web génère la page HTML suivante et l'envoie au client Web via le serveur Web.

3.4.2.2 Exécution d'un objet programme planifié

Ce workflow décrit le processus d'un objet programme planifié s'exécutant à une heure planifiée. L'Adaptive Job Server et l'Input File Repository Server doivent également être en cours d'exécution.

> **Remarque**
>
> Ce workflow requiert que le CMS, l'Adaptive Job Server et l'Input File Repository Server soient en cours d'exécution.

1. Le CMS (Central Management Server) vérifie la base de données système du CMS pour déterminer si une planification de rapport SAP Crystal doit être exécutée à ce moment.
2. A l'heure du travail planifié, le CMS recherche un service de planification du programme en cours d'exécution sur un Adaptive Job Server. Le CMS envoie les informations sur le travail au service de planification du programme.
3. Le service de planification du programme communique avec l'Input File Repository Server (FRS) pour obtenir l'objet programme.

   > **Remarque**
   >
   > Cette étape requiert également la communication avec le CMS pour rechercher le serveur et les objets requis.

4. Le service de planification du programme lance le programme.
5. Le service de planification du programme met régulièrement à jour le statut des travaux sur le CMS. Le statut actuel est Traitement en cours.

6. Le service de planification du programme envoie un fichier journal à l'Output File Repository Server. L'Output File Repository Server notifie le service de planification du programme que l'objet a été planifié en lui envoyant un fichier journal de l'objet.

> **Remarque**
>
> Cette étape requiert également la communication avec le CMS pour rechercher le serveur et les objets requis.

7. Le service de planification du programme met à jour le statut des travaux sur le CMS. Le statut actuel est Réussite.
8. Le CMS met à jour le statut des travaux dans sa mémoire, puis il écrit les informations sur l'instance dans la base de données système du CMS.

3.4.3 Crystal Reports

3.4.3.1 Visualisation d'une page de rapport SAP Crystal mise en cache

Ce workflow décrit le processus d'un utilisateur demandant une page d'un rapport SAP Crystal (par exemple depuis le visualiseur de rapport de la zone de lancement BI), lorsque la page du rapport existe déjà sur un serveur de mise en cache. Ce workflow s'applique à SAP Crystal Reports 2020 et SAP Crystal Reports pour Enterprise.

> **Remarque**
>
> Ce workflow requiert que le CMS et le Crystal Reports Cache Server soient en cours d'exécution.

1. Le client Web envoie une demande de visualisation dans une URL au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la demande et détermine qu'il s'agit d'une demande de visualisation d'une page de rapport sélectionnée. Le serveur d'applications Web envoie une demande au CMS (Central Management Server) pour vérifier que l'utilisateur a les droits appropriés pour visualiser le rapport.
3. Le CMS contrôle la base de données système du CMS pour vérifier que l'utilisateur dispose des droits suffisants pour visualiser le rapport.
4. Le CMS envoie une réponse au serveur d'applications Web pour confirmer que l'utilisateur a les droits suffisants pour visualiser le rapport.
5. Le serveur d'applications Web envoie une requête au serveur de mise en cache Crystal Reports pour lui demander la page du rapport (fichier `.epf`).
6. Le serveur de mise en cache Crystal Reports détermine si le fichier `.epf` demandé existe dans le répertoire de la mémoire cache. Dans cet exemple, le fichier `.epf` s'y trouve.
7. Le serveur de mise en cache Crystal Reports renvoie la page demandée au serveur d'applications Web.
8. Le serveur d'applications Web envoie via le serveur Web la page au client Web, où elle s'affiche.

3.4.3.2 Visualisation d'une page SAP Crystal Reports 2020 non mise en cache

Ce workflow décrit le processus d'un utilisateur demandant une page d'un rapport SAP Crystal Reports 2020 (par exemple depuis le visualiseur de rapport de la zone de lancement BI), lorsque la page du rapport n'existe pas encore sur un Cache Server.

> **Remarque**
>
> Ce workflow requiert que le CMS, le Crystal Reports Cache Server, le serveur de traitement Crystal Reports 2020 et l'Output File Repository Server soient en cours d'exécution.

1. L'utilisateur envoie la requête de visualisation au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la demande, détermine si c'est une demande de visualisation d'une page de rapport sélectionnée et envoie une demande au CMS (Central Management Server) pour vérifier que l'utilisateur dispose des droits suffisants pour visualiser le rapport.
3. Le CMS contrôle la base de données système du CMS pour vérifier que l'utilisateur dispose des droits suffisants pour visualiser le rapport.
4. Le CMS envoie une réponse au serveur d'applications Web pour confirmer que l'utilisateur a les droits suffisants pour visualiser le rapport.
5. Le serveur d'applications Web envoie une requête au serveur de mise en cache Crystal Reports pour lui demander la page du rapport (fichier `.epf`).
6. Le Crystal Reports Cache Server détermine si le fichier demandé existe dans le répertoire cache. Dans cet exemple, le fichier `.epf` demandé ne se trouve pas dans le répertoire de la mémoire cache.
7. Le serveur de mise en cache Crystal Reports envoie la requête au serveur de traitement Crystal Reports 2020.
8. Le serveur de traitement Crystal Reports 2020 interroge l'Output File Repository Server (FRS) au sujet de l'instance de rapport demandée et l'Output FRS envoie celle-ci au serveur de traitement Crystal Reports 2020.

   > **Remarque**
   >
   > Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

9. Le serveur de traitement Crystal Reports 2020 ouvre l'instance de rapport et vérifie si le rapport contient des données.

   Le serveur de traitement Crystal Reports 2020 détermine que le rapport contient des données, puis il crée le fichier `.epf` pour la page de rapport demandée sans se connecter à la base de données de production.
10. Le serveur de traitement Crystal Reports 2020 envoie le fichier `.epf` au serveur de mise en cache Crystal Reports.
11. Le serveur de traitement Crystal Reports 2011 écrit le fichier `.epf` dans le répertoire de la mémoire cache.
12. Le Crystal Reports Cache Server envoie la page demandée au serveur d'applications Web.
13. Le serveur d'applications Web envoie via le serveur Web la page au client Web, où elle s'affiche.

3.4.3.3 Visualisation d'un rapport SAP Crystal Reports 2020 à la demande

Ce workflow décrit le processus d'un utilisateur demandant une page de rapport SAP Crystal Reports 2020 à la demande pour voir les dernières données, par exemple depuis le visualiseur de rapport de la zone de lancement BI.

> **Remarque**
>
> Ce workflow requiert que le CMS, le Crystal Reports Cache Server, le serveur de traitement Crystal Reports 2020 et l'Input File Repository Server soient en cours d'exécution.

1. L'utilisateur envoie la requête de visualisation au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la demande et détermine qu'il s'agit d'une demande de visualisation d'une page de rapport sélectionnée. Le serveur d'applications Web envoie une demande au CMS (Central Management Server) pour vérifier que l'utilisateur a les droits appropriés pour visualiser le rapport.
3. Le CMS contrôle la base de données système du CMS pour vérifier que l'utilisateur dispose des droits suffisants pour visualiser le rapport.
4. Le CMS envoie une réponse au serveur d'applications Web pour confirmer que l'utilisateur a les droits suffisants pour visualiser le rapport.
5. Le serveur d'applications Web envoie une requête au serveur de mise en cache Crystal Reports pour lui demander la page du rapport (fichier `.epf`).
6. Le Crystal Reports Cache Server vérifie si la page existe déjà. Sauf si le rapport répond aux exigences du partage de rapport à la demande (dans un délai défini par rapport à une autre requête à la demande, connexion à la base de données, paramètres), le serveur de mise en cache Crystal Reports envoie une requête au serveur de traitement Crystal Reports 2020 pour générer la page.
7. Le serveur de traitement Crystal Reports 2020 demande l'objet de rapport à l'Input File Repository Server (FRS). L'Input FRS transmet une copie de l'objet au serveur de traitement Crystal Reports 2020.

   > **Remarque**
   >
   > Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

8. Le serveur de traitement Crystal Reports 2020 ouvre le rapport dans sa mémoire et vérifie s'il contient des données. Dans cet exemple, il n'y a pas de données dans l'objet de rapport, le serveur de traitement Crystal Reports 2020 se connecte donc à la source de données pour récupérer les données et générer le rapport.
9. Le serveur de traitement Crystal Reports 2020 envoie la page (fichier `.epf`) au serveur de mise en cache Crystal Reports. Le serveur de mise en cache Crystal Reports stocke une copie du fichier `.epf` dans son répertoire de mémoire cache dans l'attente de nouvelles demandes de visualisation.
10. Le Crystal Reports Cache Server envoie la page au serveur d'applications Web.
11. Le serveur d'applications Web envoie via le serveur Web la page au client Web, où elle s'affiche.

3.4.3.4 Définition de la planification d'un rapport SAP Crystal

Ce workflow décrit le processus d'un utilisateur planifiant l'exécution d'un rapport SAP Crystal à une heure future à partir d'une application Web comme la CMC (Central Management Console) ou la zone de lancement BI. Ce workflow s'applique à SAP Crystal Reports 2020 et SAP Crystal Reports pour Enterprise.

1. Le client Web envoie une demande de planification dans une URL au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la requête URL et détermine qu'il s'agit d'une requête de planification. Le serveur d'applications Web envoie l'heure de planification, les valeurs de connexion à la base de données, les valeurs des paramètres, la destination et le format au CMS (Central Management Server) spécifié.
3. Le CMS vérifie si l'utilisateur dispose des droits appropriés pour planifier l'objet. Si tel est le cas, le CMS ajoute un nouvel enregistrement à la base de données système du CMS. Le CMS ajoute également l'instance à sa liste de planifications en attente.
4. Le CMS envoie une réponse au serveur d'applications Web pour l'aviser que l'opération de planification a réussi.
5. Le serveur d'applications Web génère la page HTML suivante et l'envoie au client Web via le serveur Web.

3.4.3.5 Un rapport SAP Crystal Reports 2020 s'exécute

Ce workflow décrit le processus d'un rapport SAP Crystal Reports 2020 planifié exécuté à une heure planifiée.

1. Le CMS (Central Management Server) vérifie la base de données système du CMS pour déterminer si une planification de rapport SAP Crystal doit être exécutée à ce moment.
2. À l'heure du travail planifié, le CMS recherche un service de planification Crystal Reports 2020 disponible s'exécutant sur un Adaptive Job Server (en fonction de la valeur *Nombre maximal de travaux autorisés* configurée sur chaque Adaptive Job Server). Le CMS envoie les informations sur le travail (ID rapport, format, destination, informations de connexion, paramètres et formules de sélection) au service de planification Crystal Reports 2020.
3. Le service de planification Crystal Reports 2020 communique avec l'Input File Repository Server (FRS) pour obtenir un exemple de rapport conforme à l'ID du rapport demandé.

   > **Remarque**
   >
   > Cette étape requiert également la communication avec le CMS pour rechercher le serveur et les objets requis.

4. Le service de planification Crystal Reports 2020 lance le processus JobChildserver.
5. Le processus enfant (JobChildserver) lance `ProcReport.dll` lorsqu'il reçoit le modèle de l'Input File Repository Server. `ProcReport.dll` contient tous les paramètres que le CMS a transmis au service de planification Crystal Reports 2020.
6. `ProcReport.dll` démarre `crpe32.dll`, qui traite le rapport d'après les paramètres transmis.
7. Pendant que `crpe32.dll` continue à traiter le rapport, des enregistrements sont récupérés dans la source de données selon les définitions du rapport.

8. Le service de planification Crystal Reports 2020 met périodiquement à jour le statut des travaux sur le CMS. Le statut actuel est Traitement en cours.
9. Une fois que le rapport est compilé dans la mémoire du service de planification Crystal Reports 2020, il peut être exporté dans un autre format, par exemple PDF (Portable Document Format). `crxfpdf.dll` est utilisé lors de l'exportation en PDF.
10. Le rapport contenant les données enregistrées est envoyé à l'emplacement planifié (courrier électronique par exemple), puis à l'Output FRS.

> **Remarque**
>
> Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

11. Le service de planification Crystal Reports 2020 met à jour le statut du travail sur le CMS. Le statut actuel est Réussite.
12. Le CMS met à jour le statut des travaux dans sa mémoire, puis il écrit les informations sur l'instance dans la base de données système du CMS.

3.4.4 Web Intelligence

3.4.4.1 Visualisation d'un document SAP BusinessObjects Web Intelligence sur demande

Ce workflow décrit le processus d'un utilisateur visualisant une page de document SAP BusinessObjects Web Intelligence à la demande pour voir les dernières données, par exemple depuis le visualiseur Web Intelligence de la zone de lancement BI.

1. Un navigateur Web envoie la demande de visualisation au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la demande et détermine qu'il s'agit d'une demande de visualisation d'un document Web Intelligence. Le serveur d'applications Web envoie une demande au CMS (Central Management Server) pour vérifier que l'utilisateur a les droits appropriés pour visualiser le document.
3. Le CMS contrôle la base de données système du CMS pour vérifier que l'utilisateur dispose des droits suffisants pour visualiser le document.
4. Le CMS envoie une réponse au serveur d'applications Web pour confirmer que l'utilisateur a les droits suffisants pour visualiser le document.
5. Le serveur d'applications Web envoie une requête au Web Intelligence Processing Server pour obtenir le document.
6. Le Web Intelligence Processing Server demande à l'Input File Repository Server le document, ainsi que le fichier d'univers sur lequel le document demandé est basé. Le fichier d'univers contient des informations sur la métacouche, notamment les droits au niveau des lignes et des colonnes.
7. L'Input File Repository Server transmet au serveur de traitement de Web Intelligence une copie du document, ainsi que le fichier d'univers sur lequel le document demandé est basé.

> **Remarque**
>
> Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

8. Le moteur de rapport Web Intelligence (sur le serveur de traitement Web Intelligence) ouvre le document en mémoire et lance `QT.dll` ainsi qu'un serveur de connexion en cours de traitement.
9. `QT.dll` génère, valide et régénère le code SQL, puis se connecte à la base de données pour exécuter la requête. Le serveur de connexion utilise le code SQL pour extraire les données de la base de données et les envoyer au moteur de rapport, où a lieu le traitement du document.
10. Le Web Intelligence Processing Server envoie la page de document à visualiser demandée au serveur d'applications Web.
11. Le serveur d'applications Web envoie via le serveur Web la page de document au client Web, où elle s'affiche.

3.4.4.2 Définition de la planification d'un document SAP BusinessObjects Web Intelligence

Ce workflow décrit le processus d'un utilisateur planifiant l'exécution d'un document SAP BusinessObjects Web Intelligence à une heure future à partir d'une application Web comme la CMC (Central Management Console) ou la zone de lancement BI.

1. Le client Web envoie une demande de planification dans une URL au serveur d'applications Web, via le serveur Web.
2. Le serveur d'applications Web interprète la requête URL et détermine qu'il s'agit d'une requête de planification. Le serveur d'applications Web envoie l'heure de planification, les valeurs de connexion à la base de données, les valeurs des paramètres, la destination et le format au CMS (Central Management Server) spécifié.
3. Le CMS vérifie si l'utilisateur dispose des droits appropriés pour planifier l'objet. Si tel est le cas, le CMS ajoute un nouvel enregistrement à la base de données système du CMS. Le CMS ajoute également l'instance à sa liste de planifications en attente.
4. Le CMS envoie une réponse au serveur d'applications Web pour l'aviser que l'opération de planification a réussi.
5. Le serveur d'applications Web génère la page HTML suivante et l'envoie au client Web via le serveur Web.

3.4.4.3 Un document SAP BusinessObjects Web Intelligence planifié s'exécute

Ce workflow décrit le processus d'un document SAP BusinessObjects Web Intelligence planifié exécuté à une heure planifiée.

1. Le CMS (Central Management Server) contrôle la base de données système du CMS pour déterminer si l'exécution d'un document Web Intelligence est planifiée.

2. A l'heure planifiée, le CMS recherche un service de planification Web Intelligence s'exécutant sur un Adaptative Job Server. Le CMS envoie la demande de planification et toutes les informations la concernant au service de planification Web Intelligence.
3. Le service de planification Web Intelligence recherche un serveur de traitement Web Intelligence disponible d'après la valeur *Nombre maximal de connexions* configurée sur chaque serveur de traitement Web Intelligence
4. Le serveur de traitement Web Intelligence détermine l'emplacement de l'Input File Repository Server (FRS) qui héberge le document et le fichier métacouche d'univers sur lequel ce document est basé. Le serveur de traitement Web Intelligence demande ensuite le document à l'Input File Repository Server. L'Input File Repository Server recherche le document Web Intelligence ainsi que le fichier d'univers sur lequel ce document est basé, et les transmet au serveur de traitement Web Intelligence.

   > **Remarque**
   >
   > Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

5. Le document Web Intelligence est stocké dans un répertoire temporaire sur le Web Intelligence Processing Server. Le serveur de traitement Web Intelligence ouvre le document dans la mémoire et `QT.dll` génère le SQL depuis l'univers sur lequel est basé le document. Les bibliothèques du serveur de connexion incluses dans le serveur de traitement Web Intelligence se connectent à la source de données. Les données de la requête retournent via `QT.dll` au moteur de rapport du serveur de traitement Web Intelligence, où le document est traité. Une nouvelle instance réussie est créée.
6. Le serveur de traitement Web Intelligence charge l'instance du document sur l'Output File Repository Server.

   > **Remarque**
   >
   > Cette étape nécessite également une communication avec le CMS pour localiser le serveur et les objets requis.

7. Le serveur de traitement Web Intelligence notifie au service de planification Web Intelligence (sur l'Adaptive Job Server) que la création du document est terminée. Si le document est planifié pour une destination spécifique (système de fichiers, FTP, SFTP, SMTP ou boîte de réception), l'Adaptive Job Server extrait le document traité de l'Output File Repository Server et l'envoie à chaque destination spécifiée. Cela n'est pas le cas dans cet exemple.
8. Le service de planification Web Intelligence met à jour le statut du travail sur le CMS.
9. Le CMS met à jour le statut des travaux dans sa mémoire, puis il écrit les informations sur l'instance dans la base de données système du CMS.

3.4.5 Analysis

3.4.5.1 Visualisation d'un espace de travail SAP BusinessObjects Analysis, édition pour OLAP

Ce workflow décrit le processus d'un utilisateur demandant à visualiser depuis la zone de lancement BI un espace de travail SAP BusinessObjects Analysis, édition pour OLAP.

> **Remarque**
>
> Ce workflow requiert que le CMS, le serveur de traitement adaptatif (contenant MDAS (Multi-Dimensional Analysis Service)) et l'Input File Repository Server soient en cours d'exécution.

1. Le client Web envoie une requête de visualisation d'un nouvel espace de travail au serveur d'applications Web, via le serveur Web. Le client Web communique avec le serveur d'applications Web en utilisant la technologie DHTML AJAX (Asynchronous JavaScript and XML). La technologie AJAX permet la mise à jour partielle d'une page, ce qui évite l'affichage d'une nouvelle page à chaque nouvelle requête.
2. Le serveur d'applications Web traduit la requête et l'envoie ensuite au CMS (Central Management Server) pour déterminer si un utilisateur a les droits requis pour visualiser ou créer un espace de travail.
3. Le CMS extrait les références de connexion de l'utilisateur de la base de données système du CMS.
4. Si l'utilisateur est autorisé à visualiser ou créer un espace de travail, le CMS le confirme au serveur d'applications Web. En même temps, il envoie aussi une liste de tous les MDAS (Multi-Dimensional Analysis Services) disponibles.
5. Le serveur d'applications Web choisit un MDAS dans la liste des services disponibles, puis envoie à ce service une requête CORBA pour trouver le(s) serveur(s) OLAP approprié(s) pour créer un espace de travail ou actualiser un espace de travail existant.
6. Le MDAS doit communiquer avec l'Input File Repository Server (FRS) pour extraire le document de l'espace de travail approprié qui contient les informations relatives à la base de données OLAP sous-jacente, ainsi qu'une requête OLAP initiale ayant été enregistrée avec lui. L'Input File Repository Server extrait l'espace de travail Analysis approprié du répertoire sous-jacent et le transmet au MDAS.
7. Le MDAS ouvre l'espace de travail, formule une requête et envoie cette requête au serveur de base de données OLAP. Le MDAS doit utiliser un client de base de données OLAP approprié et configuré pour la source de données OLAP. La requête du client Web doit être traduite en requête OLAP appropriée. Le serveur de base de données OLAP renvoie le résultat de la requête au MDAS.
8. Le MDAS, en fonction du type de la requête (requête de création, de visualisation, d'impression ou d'exportation), affiche un aperçu du résultat afin de permettre au serveur Java WAS de terminer l'affichage plus rapidement. Le MDAS renvoie les packages XML du résultat affiché au serveur d'applications Web.
9. Le serveur d'applications Web affiche l'espace de travail et envoie la page mise en forme ou une partie de celle-ci au client Web, via le serveur Web. Le client Web affiche la page mise à jour ou la nouvelle page demandée. Cette solution sans client ne nécessite aucun téléchargement de composants Java ou ActiveX.

3.5 Intégration à la barre de lancement SAP Fiori sur le SAP Enterprise Portal

Présentation

L'intégration de SAP BusinessObjects BI aux plateformes de la barre de lancement SAP Fiori permet aux utilisateurs finaux du SAP Enterprise Portal d'afficher les rapports de BI sur le CMS SAP BusinessObjects. Sur l'onglet Menu utilisateur, les utilisateurs finaux ont accès aux rapports de BI, dont la hiérarchie de dossiers correspond à celle du CMS SAP BusinessObjects.

Conditions préalables

- Business Intelligence 4.2 SP4
- Web Dispatcher 7.49 pour la connectivité
- NetWeaver 7.5 SP7
- Authentification Active Directory et configuration de connexion unique basée sur Kerberos, comme indiqué dans la note SAP 1631734

Procédure

L'administrateur de contenu de la zone de lancement SAP Fiori et l'administrateur du SAP Enterprise Portal peuvent intégrer SAP BusinessObjects Enterprise à la zone de lancement SAP Fiori.

Pour obtenir les informations de configuration complète, voir Intégration de SAP BusinessObjects Enterprise dans la documentation du portail SAP NetWeaver 7.5.

> **Remarque**
>
> - La plateforme de BI prend en charge les services OData pour l'intégration entre la barre de lancement SAP Fiori et SAP Enterprise Portal.
> - La plateforme de BI prend en charge les services OData dans le serveur d'applications NetWeaver.
> - Une fois l'intégration réussie, vous pouvez accéder aux dossiers publics, aux dossiers personnels et à la boîte de réception BI à partir de SAP Enterprise Portal.

4 Assistant de configuration du système

4.1 Introduction à l'Assistant de configuration du système

Après avoir installé la plateforme SAP BusinessObjects Business Intelligence, il est probable que vous souhaitiez effectuer la configuration essentielle post-installation , comme choisir le modèle de déploiement ou sélectionner les produits SAP BusinessObjects utilisés par votre entreprise. Pour réaliser cette configuration et faire fonctionner la plateforme de BI le plus rapidement possible, exécutez l'*Assistant de configuration du système*.

Avantages importants de l'assistant :

- L'assistant vous explique et vous guide dans les étapes de configurations que vous devez effectuer.
- L'utilisation de l'assistant réduit la probabilité d'une mauvaise configuration du système.
- L'Assistant configure les paramètres à votre place, ce qui accélère la configuration du système.

Par défaut, l'assistant est configuré pour s'exécuter automatiquement lorsque vous vous connectez à la Central Management Console (CMC), mais vous pouvez également lancer l'assistant dans la zone *Gérer* de la CMC. Vous pouvez réexécuter l'assistant à tout moment pour ajuster votre configuration, et vous pouvez utiliser la page de gestion *Serveurs* dans la CMC pour ajuster tous les paramètres, y compris ceux effectués à l'aide de l'assistant.

> ⓘ Remarque
>
> Pour plus de sécurité, seuls les membres du groupe Administrateurs peuvent accéder à l'assistant.

> ⓘ Remarque
>
> Pour empêcher l'exécution automatique de l'Assistant, l'utilisateur « Administrateur » peut cocher la case *Ne plus afficher cet assistant lorsque la CMC est démarrée* sur la première page de l'Assistant.

> ⓘ Remarque
>
> Si vous prévoyez d'installer des modules complémentaires ou d'ajouter des nœuds au déploiement de votre plateforme de BI, il est conseillé de suivre cette procédure avant d'exécuter l'Assistant de configuration du système.

4.2 Indication des produits utilisés

Vous pouvez simplifier la configuration des serveurs de la plateforme de BI en indiquant les produits utilisés par votre entreprise. Vous pouvez également optimiser la distribution des ressources en interrompant les serveurs pour les produits non utilisés par votre entreprise. Pour ce faire, sélectionnez les produits sur la page *Produits*. Lorsque vous indiquez les produits utilisés par votre entreprise, l'assistant lance tous les serveurs

et les dépendances requis pour que ces produits s'exécutent, et configure ces serveurs et dépendances pour qu'ils démarrent automatiquement lorsque la plateforme de BI démarre. De plus, en décochant les produits non utilisés, vous pouvez améliorer la durée de démarrage et l'utilisation des ressources de la plateforme de BI.

Par exemple, si vous sélectionnez le produit Crystal Reports, la plateforme de BI démarre automatiquement tous les serveurs Crystal Reports et les dépendances appropriées.

Pour afficher une liste des serveurs automatiquement lancés pour un produit, cliquez sur l'icône *?* à côté du nom du produit.

L'assistant configure les serveurs de produit de la manière suivante :

- La sélection d'un produit déclenche le démarrage de tous les serveurs qui relèvent de ce produit, ainsi que tous les autres serveurs requis pour que ce produit fonctionne (dépendances), dès la fin de l'assistant. La sélection d'un produit configure également le démarrage automatique avec la plateforme de BI des serveurs du produit. Si un serveur héberge des services de plusieurs produits, le serveur est lancé si l'un de ces produits est sélectionné. Notez que certains services des produits qui ne sont pas sélectionnés peuvent s'exécuter s'ils sont hébergés par un serveur qui héberge également des services de produits sélectionnés.
- Le fait de désélectionner un produit déclenche l'arrêt des serveurs utilisés par ce produit, à condition que ces serveurs n'hébergent pas en plus des services d'un produit toujours sélectionné, ou des services appartenant à la catégorie Services principaux. Les serveurs de produits arrêtés sont configurés pour ne pas démarrer automatiquement avec la plateforme de BI. Si un serveur héberge des services de produits sélectionnés et non sélectionnés, le serveur continue à s'exécuter.
- Le fait de désélectionner un produit peut également provoquer l'arrêt des serveurs qui n'appartiennent pas au produit désélectionné, s'ils contiennent des services dépendants utilisés uniquement par le produit désélectionné. Cet arrêt libère des ressources puisque ces serveurs dépendants ne sont plus nécessaires.
- Lorsqu'un produit est sélectionné ou désélectionné, tous les serveurs qui hébergent les services appartenant à la catégorie Services principaux sur la plateforme de BI (sauf les services hébergés par WACS) sont automatiquement lancés. Le WACS reste dans son état actuel.
- Le fait de désélectionner des produits ne désinstalle ni ne supprime les fichiers de ces produits.

Lorsque vous ouvrez la page *Produits*, les états des produits représentent l'état actuel du système.

Si tous les serveurs pour un produit sont en cours d'exécution, alors la case pour ce produit est cochée. Si tous les serveurs pour un produit sont arrêtés, alors la case est décochée. Si seulement certains serveurs pour un produit sont en cours d'exécution, et que d'autres serveurs se trouvent dans d'autres états, par exemple arrêtés, alors la page *Produits* affiche la case à cocher *Conserver la configuration existante* pour indiquer que le système a été configuré en dehors de l'assistant. Vous pouvez décocher la case si vous souhaitez utiliser l'assistant pour modifier votre configuration.

> **ⓘ Remarque**
>
> La page *Produits* affiche tous les produits installés sur le cluster. Par exemple, si les produits P1 et P2 sont installés sur la machine A, et que les produits P2 et P3 sont installés sur la machine B, alors la page *Produits* affiche les produits P1, P2 et P3. Les produits qui ne sont pas installés n'apparaissent pas sur la page *Produits*.

> **ⓘ Remarque**
>
> Pour simplifier le déploiement, la configuration de cette page n'a pas besoin d'être répétée pour chaque nœud ; elle s'applique à l'ensemble du cluster.

> **Remarque**
>
> Si un paramètre a été précédemment modifié dans la CMC, l'assistant affiche un message indiquant que les paramètres ont été modifiés en dehors de l'assistant. Vous pouvez choisir de conserver la configuration existante ou de remplacer les paramètres actuels.

> **Remarque**
>
> Les modifications que vous apportez dans l'assistant s'appliquent dès lors que vous cliquez sur *Appliquer* sur la page *Réviser*.

Lorsque vous avez fini d'apporter des modifications, cliquez sur *Suivant* pour accéder à la page suivante de l'assistant. Vous pouvez également utiliser le panneau de navigation à gauche pour passer directement aux pages que vous avez déjà consultées.

4.3 Sélection d'un modèle de déploiement

L'installation par défaut de la plateforme de BI configure un petit déploiement adapté à un environnement de démonstration sur un matériel système limité. Pour mieux correspondre à votre matériel et vos cas d'utilisation (par exemple, préparation d'un système de test ou un système de production), sélectionnez l'un des modèles de déploiement prédéfinis dans la page *Capacité*. Le but de ces modèles est de vous aider à faire fonctionner rapidement votre système de plateforme de BI et diminuer votre durée de déploiement initiale.

Bien que la sélection d'un modèle de déploiement approprié vous aide dans la configuration initiale et offre un bon point de départ, elle ne remplace pas le dimensionnement et à l'ajustement du système qui doivent quand même être effectués. Pour obtenir les meilleures performances, vous devez dimensionner le système en faisant référence à un guide de dimensionnement : http://www.sap.com/bisizing.

La sélection d'un modèle de déploiement approprié est importante pour plusieurs raisons :

- La capacité de gestion des requêtes de votre système dépend du modèle de déploiement que vous sélectionnez. Un grand déploiement offre une plus grande capacité pour gérer plus de requêtes, ou des requêtes plus complexes. Cependant, un grand déploiement nécessite plus de ressources système.
- La sélection d'un grand déploiement ne garantit pas de meilleures performances, notamment si vous ne disposez pas d'assez de ressources matérielles disponibles.
- Le modèle de déploiement que vous sélectionnez doit correspondre aux besoins de votre entreprise et à vos ressources matérielles. Il est possible que les capacités et performances du système soient réduites si vous sélectionnez un modèle de déploiement trop petit pour vos besoins d'entreprise, ou trop grand pour les ressources matérielles disponibles.
- Les grands modèles de déploiement fournissent un meilleur cloisonnement : les erreurs d'un produit sont moins susceptibles de toucher les autres produits. Sélectionnez un modèle qui équilibre les performances et l'utilisation des ressources (RAM). Par exemple, si une grande quantité de mémoire RAM est disponible, sélectionnez le plus grand modèle de déploiement autorisé par votre mémoire RAM ; cela vous permet d'obtenir un meilleur cloisonnement du système.

Vous pouvez utiliser le curseur pour sélectionner un modèle de déploiement, ou sélectionner une quantité de mémoire RAM dans la liste déroulante. Lorsque vous modifiez le paramètre, notez que l'indicateur *Nombre de serveurs de traitement adaptatif* change pour vous montrer la manière dont le système sera configuré si vous sélectionnez ce paramètre.

ⓘ Remarque

Le modèle de déploiement que vous sélectionnez affecte également les serveurs de traitement adaptatif (APS). Les autres serveurs, comme le CMS ou Adaptive Job Server, ne sont pas affectés.

ⓘ Remarque

La Mémoire RAM requise correspond à la quantité minimale de mémoire RAM requise pour les serveurs de la plateforme de BI. Par exemple, sur une machine qui dispose de 16 Go de mémoire RAM, dont 1 Go est utilisé par le système d'exploitation, un autre par le serveur de base de données et 10 Go par les serveurs de la plateforme de BI, la mémoire RAM requise est égale à 10 Go, et non pas 12 ou 16. Le nombre indiqué dans Mémoire RAM requise représente uniquement une valeur générale ; votre système peut avoir besoin de plus de mémoire RAM lors d'un chargement important. Pour des performances système optimales, vous devez toujours effectuer un dimensionnement du système.

ⓘ Remarque

Lorsque vous ouvrez la page *Capacité*, le modèle de déploiement affiché représente l'état du système actuel, si l'état du système actuel correspond à l'un des modèles de déploiement prédéfinis. Par exemple, si vous avez créé manuellement un serveur de traitement adaptatif supplémentaire à l'aide de la CMC, l'état actuel de votre système ne correspond pas aux modèles de déploiement. Par conséquent, la page *Capacité* affiche la case à cocher *Conserver la configuration existante* pour indiquer que le système a été configuré sans l'assistant. Dans un déploiement à plusieurs nœuds, la case à cocher*Conserver la configuration existante* est également affichée si le nombre d'APS d'un nœud ne correspond pas à un modèle de déploiement, ou que le nombre d'APS est différent sur plusieurs nœuds. Vous pouvez décocher la case si vous souhaitez utiliser l'assistant pour modifier votre configuration.

ⓘ Remarque

Pour simplifier le déploiement, la configuration de l'APS que vous sélectionnez s'applique à chaque nœud (à condition que ces nœuds comportent un APS installé) ; plus vous avez de nœuds, plus votre cluster aura des capacités.

ⓘ Remarque

Les modules complémentaires (par exemple, SAP BusinessObjects Data Services ou AADS (Service de conception d'application d'analyse)) ne sont pas gérés par l'assistant. Les services créés par les modules complémentaires ne seront pas déplacés vers des APS différents par l'assistant.

Exemples :

- Si l'AADS est hébergé par un APS qui héberge d'autres services à partir de l'installation principale de la plateforme de BI, puis si vous exécutez l'assistant et que vous remplacez la taille du modèle de déploiement XS par M, l'assistant crée sept nouveaux APS, puis y déplace tous les services, à l'exception du service AADS qui demeure dans l'APS initial.
- Les modules complémentaires SAP BusinessObjects Data Services créent un APS dédié. L'assistant n'altère pas cet APS dédié et ne le prend pas en compte lorsqu'il indique le nombre d'APS dans le système.

Fichier DeploymentTemplates.pdf

Pour une description détaillée des paramétrages réalisés par l'assistant pour chaque modèle de déploiement disponible, cliquez sur le lien *Modèle de déploiement* dans la page *Capacité* pour ouvrir le fichier `DeploymentTemplates.pdf`.

Le fichier `DeploymentTemplates.pdf` décrit en détail les modèles de déploiement. Notez que les modèles n'indiquent pas le nombre d'utilisateurs qui peuvent être pris en charge, car cela dépend du chargement. Vous devez réaliser un dimensionnement du système pour déterminer le nombre d'utilisateurs que vous devez prendre en charge; et par conséquent la quantité de mémoire RAM requise, les besoins en unités centrales, etc.

4.4 Indication des emplacements des dossiers de données

Utilisez la page *Dossiers* pour indiquer l'emplacement où vous souhaitez que la plateforme de BI enregistre ses fichiers journaux et de données. Vous pouvez indiquer des emplacements de dossier, ou accepter les emplacements actuels.

Si votre déploiement de la plateforme de BI comporte plusieurs nœuds, vous disposez de deux options pour définir les emplacements de dossier :

- Si vous souhaitez configurer les mêmes emplacements de dossier pour tous les nœuds, sélectionnez l'option *Tous les nœuds ont les mêmes emplacements de dossier*.
- Si les serveurs de votre cluster ne sont pas configurés de la même façon, les chemins d'installation ou les structures des répertoires de fichiers peuvent être différents. Vous pouvez sélectionner l'option *Les nœuds ont des emplacements de dossier différents* pour configurer des emplacements de dossier spécifiques pour chaque nœud.

Lorsque l'assistant ouvre la page *Dossiers*, il affiche les noms de dossier de la manière suivante :

- Si tous les nœuds ont des dossiers avec les mêmes valeurs (c'est-à-dire que les dossiers Journal sur tous les serveurs du cluster sont identiques, ainsi que les dossiers Données, etc.), l'option *Tous les nœuds ont les mêmes emplacements de dossier* est sélectionnée et les noms de dossier actuels sont affichés.
- Si tous les dossiers d'un type particulier (Journal, Données, Audit, Stockage du fichier d'entrée ou Stockage du fichier de sortie) sont identiques dans chaque nœud, mais différents selon les nœuds, alors l'option *Les nœuds ont des emplacements de dossier différents* est sélectionnée et les noms de dossier actuels sont affichés.
- Si tous les dossiers d'un type particulier ne sont pas identiques dans chaque nœud et différents selon les nœuds, alors l'option *Les nœuds ont des emplacements de dossier différents* est sélectionnée, mais les noms de dossier sont vides.

Si vous modifiez les emplacements des dossiers, l'assistant configure le système afin qu'il utilise les nouveaux dossiers. L'assistant ne copie ni ne déplace les contenus des dossiers d'origine vers les nouveaux dossiers, à l'exception du dossier des données d'audit. Si les nouveaux dossiers ne contiennent pas le bon contenu, ou si vous souhaitez migrer des données des dossiers d'origine, vous devez déplacer ou copier ces données vers les nouveaux dossiers.

Pour les dossiers Stockage du fichier d'entrée, Stockage du fichier de sortie et Données, si l'emplacement du nouveau dossier est vide, vous devez copier manuellement les fichiers à partir de l'ancien emplacement de dossier, ou restaurer les fichiers à partir d'une sauvegarde. Pour le dossier Journal, copiez les fichiers

de l'ancien dossier uniquement si vous souhaitez que le nouveau dossier contienne les fichiers journaux de l'ancien emplacement de dossier.

> → Conseil
>
> Si vous prévoyez de copier ou de restaurer des fichiers dans les nouveaux dossiers, faites-le avant de relancer les nœuds.

Exemple de scénarios :

- Si vous modifiez un emplacement de dossier et que le dossier d'origine contient des rapports, ces derniers ne seront pas disponibles dans la plateforme de BI tant que vous ne les copiez pas dans le nouveau dossier et que vous relanciez les nœuds.
- Si votre dossier d'origine contenait des rapports corrompus ou modifiés et que vous souhaitez revenir à une sauvegarde saine, vous devez extraire les rapports de la sauvegarde et les placer dans le nouveau dossier, au lieu de copier les contenus du dossier d'origine.
- Si vos fichiers de données se trouvaient à l'origine sur un disque ayant la lettre de lecteur X, et que vous modifiez la lettre de lecteur par Y dans le système d'exploitation, vous n'avez pas besoin de copier ou de déplacer les fichiers de données ; il vous suffit de modifier l'emplacement de dossier dans la plateforme de BI.

Si vous avez modifié manuellement certains emplacements de dossier de telle sorte que certains serveurs sur un nœud utilisent un ensemble de dossiers tandis que d'autres serveurs sur le même nœud utilisent des dossiers différents, la page *Dossiers* affiche la case à cocher *Conserver la configuration existante* pour indiquer que le système a été configuré en dehors de l'assistant. Par exemple, il est possible que deux File Repository Servers du même nœud soient configurés pour utiliser des chemins du dossier Journal différents. Vous pouvez décocher la case si vous souhaitez utiliser l'assistant pour modifier la configuration actuelle.

Pour plus d'informations sur les types de fichiers stockés dans chaque dossier, cliquez sur les icônes *?*.

> ⓘ Remarque
>
> Si vous modifiez l'un des emplacements de dossier suivants, vous devrez relancer manuellement tous les nœuds à la fin de l'assistant pour que les changements prennent effet :
>
> - Stockage du fichier d'entrée
> - Stockage du fichier de sortie
> - Dossier de journaux
> - Dossier de données

4.5 Révision des modifications

Une fois que vous avez sélectionné vos paramètres de configuration, ils s'affichent sur la page *Réviser* pour que vous les révisiez avant que les modifications s'appliquent à votre système de la plateforme de BI. Pour chaque catégorie de paramètres, vous pouvez cliquer sur *Détails* pour voir une description détaillée ou une liste de tous les paramètres et de toutes les modifications qui vont s'appliquer.

Si vous souhaitez modifier un paramètre, vous pouvez accéder aux pages individuelles directement à partir du menu de navigation dans la partie gauche de l'assistant.

Vos sélections sont enregistrées dans un fichier journal que vous pouvez télécharger à partir de la page Terminé.

Un fichier de réponse est également généré et enregistré. Le fichier de réponse vous aide à automatiser la configuration du système. Vous pouvez cliquer sur le bouton *Télécharger* pour visualiser le fichier de réponse ou le télécharger vers le disque local.

Lorsque vous cliquez sur *Appliquer*, vos paramètres de configuration s'appliquent à votre déploiement de la plateforme de BI. Lorsque l'assistant se termine, une page *Terminé* s'affiche, indiquant les étapes suivantes que vous devez effectuer manuellement.

Informations associées

Fichiers journaux et fichiers de réponse [page 96]

4.6 Fichiers journaux et fichiers de réponse

La page *Terminé* vous indique le statut des modifications, et vous permet de télécharger et d'afficher les fichiers journaux et de réponse pour votre session.

Les fichiers journaux et de réponse sont automatiquement enregistrés dans le dossier Assistant de configuration du système accessible à partir de la CMC. Les noms de fichier sont horodatés dans le format suivant : `année_mois_jour_heure_minute_seconde`. Les fichiers journaux utilisent l'extension `.log` tandis que les fichiers de réponse utilisent l'extension `.ini`.

Vous pouvez également cliquer sur le bouton *Télécharger* pour afficher les fichiers journaux et de réponse, ou les télécharger vers un disque local.

Le fichier journal contient les éléments suivants :

- Un enregistrement de toutes les modifications apportées dans cette session de configuration.
- L'emplacement de l'enregistrement du fichier de réponse.
- Une liste décrivant les étapes suivantes à suivre.

Informations associées

Utilisation d'un fichier de réponse [page 96]

4.6.1 Utilisation d'un fichier de réponse

A chaque fois que l'assistant se termine, il enregistre un fichier de réponse qui contient vos sélections ou les réponses à toutes vos questions sur les pages de l'assistant. Le fichier de réponse peut être utilisé pour

configurer les autres clusters lors du déploiement de la plateforme de BI sans devoir passer par l'assistant. Il peut également être utilisé ultérieurement si vous souhaitez définir le système sur le même état de configuration. Le fichier de réponse vous permet d'automatiser votre déploiement et d'éviter des erreurs d'opérateur.

Pour utiliser un fichier de réponse, vous devez exécuter un script qui utilise le fichier de réponse comme paramètre. Premièrement, cherchez le fichier de réponse que vous souhaitez utiliser et enregistrez-le sur le disque. Les fichiers de réponse sont automatiquement enregistrés dans le dossier Assistant de configuration du système, auquel les administrateurs peuvent accéder depuis la CMC. Les noms de fichier sont horodatés dans le format suivant :`année_mois_jour_heure_minute_seconde` et ont l'extension `.ini`. Depuis la CMC, vous pouvez visualiser le fichier de réponse et l'enregistrer sur le disque, ou utiliser les commandes de menu *Organiser* > *Envoyer* > *Emplacement de dossier* >.

Vous pouvez également télécharger le fichier de réponse pour la session d'assistant en cours depuis la page *Réviser* ou *Terminé*, et l'enregistrer sur le disque.

Si vous le souhaitez, vous pouvez modifier les paramètres du fichier de réponse avant de l'utiliser dans un éditeur de texte. Observez les exemples de fichier de réponse ci-dessous pour plus de détails.

Exécution du script

Une fois que vous avez le fichier de réponse approprié, utilisez le fichier comme un paramètre de ligne de commande pour les scripts qui exécutent l'assistant :

- Sous Windows, exécutez le fichier batch `SCW.bat`
- Sous Unix, exécutez le fichier script `scw.sh`.

Les fichiers batch et script se trouvent dans le même dossier que les scripts de gestion de serveur :

- Sous Windows : `<installdir>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- Sous Unix : `<installdir>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

Les fichiers batch et script utilisent ces paramètres de ligne de commande :

- `-help` : affiche l'aide pour la ligne de commande.
- `-r` : indique le chemin et le nom du fichier de réponse.
- `-cms` : indique le Central Management Server (CMS) auquel vous souhaitez vous connecter. Si ce paramètre est omis, le CMS sera par défaut la machine locale et le port par défaut (6400). Exemple : `nom_machine:6500`
- `-username` : indique un compte qui octroie des droits administratifs à la plateforme de BI. Si ce paramètre est omis, le compte Administrateur par défaut est utilisé.
- `-password` : indique le mot de passe pour le compte. Si aucun mot de passe n'est spécifié, un mot de passe vide est utilisé. Pour utiliser le paramètre `-password`, vous devez également utiliser le paramètre `-username`.

Exemples

Sous Windows :`SCW.bat –r c:\dossier\nomfichier.ini –cms nomcms:6400 –username "administrateur" –password exemplemotdepasse`

Sous Unix :`/scw.sh –r /accueil/dossier/nomfichier.ini –cms nomcms:6400 –username "administrateur" –password exemplemotdepasse`

Exemple de fichier de réponse

```
# *********************************************
# ***************** Products *****************
# *********************************************
# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the
“Products.” settings below.
Products.KeepExistingConfiguration = true
# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.
# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.
# Crystal Reports
Products.crystalreports = true
# Analysis edition for OLAP
Products.olap = true
# Web Intelligence
Products.webintelligence = false
# Dashboards (Xcelsius)
Products.dashboards = false
# Data Federator
Products.datafederator = true
# Lifecycle Manager
Products.LCM = true
# *******************************************************
# ***************** Deployment Template *****************
# *******************************************************
# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and
the Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to
the Capacity.DeploymentTemplate setting below.
Capacity.KeepExistingConfiguration = true
# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.
Capacity.DeploymentTemplate = xs
# *********************************************
# ***************** Folders *****************
# *********************************************
# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.
Folders.KeepExistingConfiguration = true
```

```
# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.
# ------ All nodes use the same folders ------
# Use this section when you have one node, or when all nodes have the same
folder locations. Otherwise, comment it out.
Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>
# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise,
comment it out.
# ------ NodeOne ------
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>
# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

Tous les paramètres du fichier de réponse doivent être indiqués, et aucun paramètre ne doit être vide, à l'exception des cas suivants :

- Si vous avez un déploiement à plusieurs nœuds, vous pouvez choisir d'omettre les paramètres de dossier pour un ou plusieurs nœuds, ce qui laissera les dossiers de ces nœuds inchangés. Toutefois, pour les nœuds que vous spécifiez dans le fichier de réponse, tous les emplacements de dossier doivent être spécifiés.
- Si le paramètre`KeepExistingConfiguration` est défini sur `vrai`, vous pouvez omettre les paramètres restants pour cette page. Par exemple, si `Products.KeepExistingConfiguration = true`, vous pouvez omettre les paramètres *Products* restants du fichier de réponse.

Dans certains cas, le fichier de réponse inclut des produits différents de ceux installés sur votre cluster cible. Dans ces cas, les comportements suivants s'appliquent :

- Si le fichier de réponse ne contient pas de définition pour les produits qui sont installés sur le cluster cible, l'opération échoue.
- Si le fichier de réponse contient des définitions pour des produits qui ne sont pas présents sur le cluster cible, un message d'avertissement s'ajoute au fichier journal, et les produits restants sont correctement configurés.

> **Remarque**
>
> Après avoir utilisé un fichier de réponse pour configurer un cluster, vous devez effectuer manuellement les étapes supplémentaires décrites dans la section « Etapes suivantes » du fichier journal.

> **Remarque**
>
> Pour plus de sécurité, seule la prise en charge de l'authentification Enterprise est requise (et non Windows AD, LDAP ni SAP).

> **Remarque**
>
> Si vous préférez repousser le redémarrage de l'un des nœuds au prochain redémarrage prévu, exécutez le script juste avant un temps d'arrêt planifié du système.

5 Gestion des licences

5.1 Gestion des clés de licence

Cette section explique comment gérer les clés de licence pour votre déploiement de la plateforme de BI.

Informations associées

Pour afficher les informations de licence [page 101]
Pour ajouter une clé de licence [page 101]
Pour visualiser l'activité du compte actuel [page 102]

5.1.1 Pour afficher les informations de licence

La zone de gestion *Clés de licence* de la CMC identifie le nombre de licences d'accès simultanés, d'utilisateurs nommés et de processeurs associées à chaque clé.

1. Accédez à la zone de gestion *Clés de licence* de la CMC.
2. Sélectionnez une clé de licence.

   Les détails associés à la clé figurent dans la zone *Informations sur la clé de licence*. Pour acquérir des clés de licence supplémentaires, contactez votre représentant commercial SAP.

Informations associées

Pour ajouter une clé de licence [page 101]
Pour visualiser l'activité du compte actuel [page 102]

5.1.2 Pour ajouter une clé de licence

Si vous effectuez une mise à niveau à partir d'une version d'essai du produit, vérifiez que vous supprimez la clé Evaluation avant de procéder à l'ajout de nouvelles clés de licence ou de codes clé d'activation de produit. Après avoir ajouté les nouvelles clés de licence, vous devrez réactiver tous vos serveurs.

> **Remarque**
>
> Si vous avez reçu de nouvelles clés de licence suite à une modification de la manière dont votre entreprise implémente les licences de la plateforme de BI, vous devez supprimer toutes les clés de licence précédentes du système pour rester en conformité.

> **Remarque**
>
> Lorsque vous mettez à jour vers la plateforme SAP BusinessObjects Business Intelligence 4.2 Support Package 2 ou version ultérieure depuis les versions antérieures, les licences existantes se comportent comme si elles avaient expiré. Vous devez générer et utiliser une nouvelle clé de licence pour la plateforme SAP BusinessObjects Business Intelligence 4.2.

1. Accédez à la zone de gestion *Clés de licence* de la CMC.
2. Saisissez la clé dans le champ *Ajouter une clé*.
3. Cliquez sur *Ajouter*.

La clé est ajoutée à la liste.

Informations associées

Pour afficher les informations de licence [page 101]
Pour visualiser l'activité du compte actuel [page 102]

5.1.3 Pour visualiser l'activité du compte actuel

1. Accédez à la zone de gestion *Paramètres* de la CMC.
2. Cliquez sur *Afficher les métriques système globales*.

   Cette section affiche l'utilisation de la licence actuelle ainsi que des performances supplémentaires.

Informations associées

Pour ajouter une clé de licence [page 101]
Pour afficher les informations de licence [page 101]

6 Gestion des utilisateurs et des groupes

6.1 Présentation de la gestion des comptes

La gestion des comptes concerne toutes les tâches relatives à la création, au mappage, à la modification et à l'organisation des informations concernant les utilisateurs et les groupes. La zone de gestion *Utilisateurs et groupes* de la CMC (Central Management Console) fournit un emplacement central pour exécuter ces tâches.

Une fois les comptes d'utilisateur et les groupes créés, vous pouvez ajouter des objets et définir les droits correspondants. Lorsque les utilisateurs se connectent, ils peuvent visualiser les objets à l'aide de la zone de lancement BI ou de leur application Web personnalisée.

6.1.1 Gestion des utilisateurs

Dans la zone de gestion *Utilisateurs et groupes*, vous pouvez saisir toutes les informations requises pour accéder à la plateforme de BI. Vous pouvez également visualiser les deux comptes d'utilisateur par défaut résumés dans le tableau « Comptes d'utilisateur par défaut ».

Comptes d'utilisateur par défaut

Nom du compte	Description
Administrateur	Cet utilisateur appartient aux groupes *Administrateurs* et *Tout le monde*. Un administrateur peut exécuter toutes les tâches dans toutes les applications de la plateforme de BI (telles que la CMC, le CCM, l'Assistant de publication et la Zone de lancement BI).
Guest	Cet utilisateur appartient au groupe *Tout le monde*. Ce compte est activé par défaut et aucun mot de passe ne lui est affecté par le système. Si vous lui en affectez un, la connexion unique à la zone de lancement BI est rompue.
SMAdmin	Il s'agit d'un compte en lecture seule utilisé par SAP Solution Manager pour accéder aux composants de la plateforme de BI.

> **Remarque**
>
> Les migrations d'objet sont mieux exécutées par des membres du groupe d'administrateurs, en particulier du groupe d'utilisateurs Administrateur. Pour migrer un objet, il se peut qu'un grand nombre d'objets liés doivent également être migrés. Dans le cas d'un compte administrateur délégué, il ne sera peut-être pas possible d'obtenir les droits de sécurité requis pour l'ensemble des objets.

6.1.2 Gestion des groupes

Les groupes sont des rassemblements d'utilisateurs qui partagent les mêmes droits de compte. Vous pouvez par conséquent créer des groupes par service, rôle ou emplacement. Les groupes vous permettent de modifier les droits des utilisateurs dans un seul endroit (un groupe), au lieu de modifier individuellement les droits de chaque compte d'utilisateur. Vous pouvez également affecter des droits d'accès aux objets à un ou plusieurs groupes.

Dans la zone *Utilisateurs et groupes*, vous pouvez créer des groupes donnant à plusieurs personnes le droit d'accéder au rapport ou au dossier approprié. Cela vous permet ainsi de modifier un seul compte d'utilisateur au lieu de la totalité. Vous pouvez également visualiser les divers comptes de groupe par défaut résumés dans le tableau « Comptes de groupe par défaut ».

Pour visualiser les groupes disponibles dans la CMC, cliquez sur *Liste des groupes* dans le panneau *Arborescence*. Vous pouvez également cliquer sur *Hiérarchie de groupe* pour afficher une liste hiérarchique de tous les groupes disponibles.

Comptes de groupe par défaut

Nom du compte	Description
Administrateurs	Les membres de ce groupe peuvent effectuer toutes les tâches dans toutes les applications de la plateforme de BI (CMC, CCM, Assistant de publication et Zone de lancement BI). Par défaut, le groupe *Administrateurs* contient uniquement l'utilisateur Administrator.
Tout le monde	Chaque utilisateur appartient au groupe *Tout le monde*.
Concepteur de groupe QaaWS	Les membres de ce groupe ont accès à Query as a Web Service.
Utilisateurs de l'outil de conversion de rapports	Les membres de ce groupe ont accès à l'application Outil de conversion de rapports.
Traducteurs	Les membres de ce groupe ont accès à l'application Gestionnaire de traduction.
Utilisateurs de Universe Designer	Les utilisateurs qui appartiennent à ce groupe disposent des droits d'accès aux dossiers *Universe Designer* et *Connexions*. Ils peuvent contrôler les droits d'accès à l'application Designer. Vous devez ajouter des utilisateurs à ce groupe selon vos besoins. Aucun utilisateur n'appartient à ce groupe par défaut.

Informations associées

Fonctionnement des droits sur la plateforme de BI [page 128]
Octroi d'un droit d'accès à des utilisateurs et à des groupes [page 116]

6.1.3 Types d'authentification disponibles

Avant de configurer des comptes et des groupes d'utilisateurs sur la plateforme de BI, choisissez le type d'authentification que vous souhaitez utiliser. Le tableau « Types d'authentification » résume les options d'authentification qui peuvent être disponibles, en fonction des outils de sécurité utilisés par votre organisation.

Types d'authentification

Type d'authentification	Description
Enterprise	Utilisez l'authentification système par défaut Enterprise si vous préférez créer des comptes et des groupes distincts à utiliser sur la plateforme de BI ou si vous n'avez pas encore défini de hiérarchie d'utilisateurs et de groupes sur un serveur de répertoires LDAP ou un serveur Windows AD.
LDAP	Si vous configurez un serveur de répertoires LDAP, vous pouvez utiliser les comptes d'utilisateur et les groupes LDAP existants sur la plateforme de BI. En mappant les comptes LDAP à la plateforme de BI, les utilisateurs peuvent accéder aux applications de la plateforme de BI avec leur nom d'utilisateur et leur mot de passe LDAP. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.
Windows AD	Vous pouvez utiliser des comptes et des groupes d'utilisateurs Windows AD existants sur la plateforme de BI. Le mappage de comptes AD à la plateforme de BI permet aux utilisateurs de se connecter aux applications de la plateforme de BI au moyen de leur nom d'utilisateur et de leur mot de passe AD. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.
SAP	Vous pouvez mapper des rôles SAP existants dans les comptes de la plateforme de BI. Le mappage de rôles SAP permet aux utilisateurs de se connecter aux applications de la plateforme de BI avec leurs références SAP. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.
Oracle EBS	Vous pouvez mapper des rôles Oracle EBS existants dans les comptes de la plateforme de BI. Le mappage de rôles Oracle EBS permet aux utilisateurs de se connecter aux applications de la plateforme de BI avec leurs références Oracle EBS. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.
Siebel	Vous pouvez mapper des rôles Siebel existants dans les comptes de la plateforme de BI. Le mappage de rôles Siebel permet aux utilisateurs de se connecter aux applications de la plateforme de BI avec leurs références Siebel. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.

Type d'authentification	Description
PeopleSoft Enterprise	Vous pouvez mapper des rôles PeopleSoft existants dans les comptes de la plateforme de BI. Le mappage de rôles PeopleSoft permet aux utilisateurs de se connecter aux applications de la plateforme de BI avec leurs références PeopleSoft. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.
JD Edwards EnterpriseOne	Vous pouvez mapper des rôles JD Edwards existants dans les comptes de la plateforme de BI. Le mappage de rôles JD Edwards permet aux utilisateurs de se connecter aux applications de la plateforme de BI avec leurs références JD Edwards. Ainsi, il est inutile de recréer des comptes d'utilisateur et des groupes individuels sur la plateforme de BI.

6.2 Gestion des comptes Enterprise et des comptes généraux

L'authentification Enterprise étant l'authentification par défaut pour la plateforme de BI, elle est automatiquement activée lorsque vous installez le système pour la première fois. Lorsque vous ajoutez et gérez des utilisateurs et des groupes, la plateforme de BI conserve des informations relatives à l'utilisateur et au groupe au sein de sa base de données.

> **Remarque**
>
> Lorsqu'un utilisateur se déconnecte d'une session Web dans la plateforme de BI en naviguant vers une page hors plateforme ou en fermant le navigateur Web, la session Enterprise n'est pas déconnectée et l'utilisateur possède toujours une licence. La session Enterprise expirera au bout de 24 heures environ. Pour terminer la session Enterprise de l'utilisateur et libérer la licence pour d'autres utilisateurs, l'utilisateur doit se déconnecter de la plateforme.

6.2.1 Pour créer un compte d'utilisateur

Lorsque vous créez un nouvel utilisateur, spécifiez ses propriétés et sélectionnez le ou les groupes auxquels il doit appartenir.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Cliquez sur *Gérer* > *Nouveau* > *Nouvel utilisateur*.
   La boîte de dialogue *Nouvel utilisateur* s'affiche.
3. Pour créer un utilisateur Enterprise :
   a. Dans la liste *Type d'authentification*, sélectionnez *Enterprise*.
   b. Saisissez le nom de compte, le nom complet, l'adresse électronique et une description.

> → Conseil
>
> Utilisez la zone de description pour inclure des informations supplémentaires sur l'utilisateur ou le compte.

c. Indiquez les informations et paramètres de mot de passe conformes aux critères de mot de passe définis pour l'authentification Enterprise.

4. Pour créer un utilisateur qui se connectera à l'aide d'un autre type d'authentification, sélectionnez l'option appropriée dans la liste *Type d'authentification* et entrez le nom du compte.
5. Effectuez l'une des actions suivantes pour désigner le compte utilisateur (en fonction de votre contrat de licence de la plateforme de BI) :
   - Sélectionnez l'option *Utilisateur simultané* si cet utilisateur relève d'un contrat de licence qui indique le nombre d'utilisateurs autorisés à se connecter en même temps.
   - Sélectionnez l'option *Utilisateur nommé* si cet utilisateur relève d'un contrat de licence qui associe un utilisateur spécifique à une licence. Les licences Utilisateur nommé sont utiles pour les personnes qui doivent accéder à la plateforme de BI, quel que soit le nombre d'utilisateurs connectés.

   > ⓘ Remarque
   >
   > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
   >
   > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

6. Cliquez sur *Créer et fermer*.

   L'utilisateur est ajouté au système, ainsi qu'au groupe Tout le monde automatiquement. Une boîte de réception est automatiquement créée pour l'utilisateur, avec un alias Enterprise.

Vous pouvez maintenant ajouter l'utilisateur à un groupe ou spécifier les droits de cet utilisateur.

6.2.2 Pour modifier un compte d'utilisateur

Suivez cette procédure pour modifier les propriétés ou l'appartenance d'un utilisateur à un groupe.

> ⓘ Remarque
>
> L'utilisateur sera affecté s'il est connecté lorsque vous apportez la modification.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur dont vous souhaitez modifier les propriétés.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* correspondant à cet utilisateur s'affiche.
4. Modifiez les propriétés de l'utilisateur.

   Outre les options disponibles au moment de la création du compte, vous pouvez maintenant désactiver le compte en cochant la case *Le compte est désactivé*.

> **Remarque**
>
> Les modifications apportées au compte d'utilisateur n'apparaissent qu'à la prochaine connexion de l'utilisateur.

5. Cliquez sur *Enregistrer et fermer*.

Informations associées

Pour créer un alias pour un utilisateur existant [page 124]

6.2.3 Pour supprimer un compte d'utilisateur

Suivez cette procédure pour supprimer un compte d'utilisateur. L'utilisateur peut recevoir un message d'erreur s'il est connecté lors de la suppression de son compte. Lorsque vous supprimez un compte d'utilisateur, le dossier Favoris, les catégories personnelles et la boîte de réception de cet utilisateur sont également supprimés.

Si vous pensez que l'utilisateur peut avoir besoin d'accéder à son compte ultérieurement, cochez la case *Le compte est désactivé* dans la page *Propriétés* de l'utilisateur sélectionné, plutôt que de supprimer le compte.

> **Remarque**
>
> La suppression d'un compte utilisateur n'empêche pas nécessairement l'utilisateur de se reconnecter à la plateforme de BI. Si le compte utilisateur existe également sur un système tiers et si le compte appartient à un groupe tiers mappé à la plateforme de BI, il se peut que l'utilisateur puisse encore se connecter.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur à supprimer.
3. Cliquez sur *Gérer* > *Supprimer*.

   La boîte de dialogue de confirmation de la suppression s'affiche et indique si l'utilisateur sélectionné est le propriétaire d'un ou de plusieurs objets.
4. Sélectionnez *OK*.
   Le compte d'utilisateur est supprimé.

Informations associées

Pour modifier un compte d'utilisateur [page 107]
Pour désactiver un alias [page 126]

6.2.4 Pour créer un groupe

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Cliquez sur *Gérer* > *Nouveau* > *Nouveau groupe*.
   La boîte de dialogue *Créer un groupe d'utilisateurs* s'affiche.
3. Saisissez le nom et la description du groupe.
4. Cliquez sur *OK*.

Après avoir créé un nouveau groupe, vous pouvez ajouter des utilisateurs, des sous-groupes ou spécifier une appartenance à un groupe de sorte que le nouveau groupe soit réellement un sous-groupe. Etant donné qu'ils apportent des niveaux d'organisation supplémentaires, les sous-groupes sont utiles lorsque vous définissez des droits d'accès aux objets en vue de contrôler l'accès des utilisateurs au contenu de la plateforme de BI.

6.2.5 Pour modifier les propriétés d'un groupe

Vous pouvez modifier les propriétés d'un groupe en changeant des paramètres.

> **Remarque**
>
> Les utilisateurs appartenant à ce groupe seront affectés par la modification à leur prochaine connexion.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, sélectionnez le groupe.
2. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
3. Modifiez les propriétés du groupe.

   Cliquez sur les liens dans la liste de navigation pour accéder à différentes boîtes de dialogue et modifier les propriétés correspondantes.

   - Si vous souhaitez modifier le titre ou la description du groupe, cliquez sur *Propriétés*.
   - Si vous souhaitez modifier les droits que les utilisateurs ou groupes principaux possèdent sur le groupe, cliquez sur *Sécurité de l'utilisateur*.
   - Si vous souhaitez modifier les valeurs de profil des membres de groupes, cliquez sur *Valeurs du profil*.
   - Si vous souhaitez ajouter le groupe en tant que sous-groupe à un autre groupe, cliquez sur *Membre de*.
4. Cliquez sur *Enregistrer*.

6.2.6 Pour afficher les membres d'un groupe

Suivez cette procédure si vous voulez afficher les utilisateurs qui appartiennent à un groupe spécifique.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Développez *Hiérarchie de groupe* dans le panneau *Arborescence*.
3. Sélectionnez le groupe dans le panneau *Arborescence*.

> **Remarque**
>
> L'affichage de la liste peut prendre quelques minutes si le groupe contient un grand nombre d'utilisateurs ou s'il est mappé à un répertoire tiers.

La liste des utilisateurs appartenant au groupe s'affiche.

6.2.7 Pour ajouter des sous-groupes

Vous pouvez ajouter un groupe à un autre groupe. Dans ce cas, le groupe ajouté devient un sous-groupe.

> **Remarque**
>
> L'ajout d'un sous-groupe est similaire à la spécification d'une appartenance à un groupe.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, sélectionnez le groupe à ajouter en tant que sous-groupe à un autre groupe.
2. Cliquez sur *Actions* > *Joindre au groupe*.
   La boîte de dialogue *Joindre au groupe* apparaît.
3. Déplacez le groupe auquel vous souhaitez ajouter le premier groupe de la liste *Groupes disponibles* vers la liste *Groupe(s) de destination*.
4. Cliquez sur *OK*.

Informations associées

Pour définir l'appartenance à un groupe [page 110]

6.2.8 Pour définir l'appartenance à un groupe

Un groupe peut devenir membre d'un autre groupe. Le groupe qui devient membre est appelé sous-groupe. Le groupe auquel vous ajoutez le sous-groupe est le groupe parent. Les sous-groupes héritent des droits du groupe parent.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, cliquez sur le groupe à ajouter à un autre groupe.
2. Cliquez sur *Actions* > *Membre de*.
   La boîte de dialogue *Membre de* s'affiche.
3. Cliquez sur *Joindre au groupe*.
   La boîte de dialogue *Joindre au groupe* apparaît.
4. Déplacez le groupe auquel vous souhaitez ajouter le premier groupe de la liste *Groupes disponibles* vers la liste *Groupe(s) de destination*.

   Tout droit associé au groupe parent sera hérité par le nouveau groupe que vous avez créé.

5. Cliquez sur *OK*.
   Vous revenez à la boîte de dialogue *Membre de* et le groupe parent apparaît dans la liste des groupes parent.

6.2.9 Pour supprimer un groupe

Vous pouvez supprimer un groupe lorsque celui-ci ne vous est plus nécessaire. Vous ne pouvez pas supprimer les groupes par défaut Administrateurs et Tout le monde.

> **Remarque**
>
> Les utilisateurs appartenant au groupe supprimé seront affectés par la modification à leur prochaine connexion.

> **Remarque**
>
> Ils perdront tous les droits qu'ils ont hérités de ce groupe.

Pour supprimer un groupe d'authentification tiers, tel que le groupe Utilisateurs Windows AD, utilisez la zone de gestion *Authentification* de la CMC.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez le groupe à supprimer.
3. Cliquez sur *Gérer* > *Supprimer*.
   La boîte de dialogue de confirmation de la suppression apparaît.
4. Cliquez sur *OK*.
   Le groupe est supprimé.

6.2.10 Pour ajouter des utilisateurs ou groupes d'utilisateurs en bloc

Vous pouvez utiliser un fichier CSV pour ajouter en bloc des utilisateurs ou des groupes d'utilisateurs à la CMC. Dans un fichier CSV correctement mis en forme, les virgules séparent les données sur une ligne, comme le montre l'exemple ci-dessous :

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

Les conditions suivantes s'appliquent au processus d'addition en bloc :

- Toute ligne du fichier CSV contenant une erreur sera ignorée par le processus d'importation.
- Les comptes utilisateur sont initialement désactivés après avoir été importés.
- Vous pouvez utiliser des mots de passe vierges lors de la création d'utilisateurs. Toutefois, vous devez utiliser un mot de passe d'authentification Enterprise valide pour toute mise à jour ultérieure vers des utilisateurs existants.
- Lorsqu'une référence de BD est ajoutée à un compte, les références de base de données sont activées dans le profil de l'utilisateur.

> **Remarque**
>
> Seuls les utilisateurs appartenant au groupe Administrateurs par défaut peuvent ajouter des utilisateurs en bloc. Cette fonctionnalité n'est pas prise en charge pour les administrateurs délégués.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, sélectionnez *Gérer* > *Importer* > *Utilisateur/Groupe/Référence de BD*.
   La boîte de dialogue *Importer un(e) Utilisateur/Groupe/Référence de BD* s'affiche.
2. Cliquez sur *Parcourir*, sélectionnez un fichier CSV et cliquez sur *Vérifier*.

   Le fichier est traité. Si les données sont correctement mises en forme dans le fichier, le bouton *Importer* devient actif. Si les données ne sont pas correctement mises en forme, des informations concernant l'erreur apparaissent, et vous devez résoudre l'erreur avant que la CMC puisse vérifier le fichier à importer.
3. Cliquez sur *Importer*.

Les utilisateurs ou les groupes d'utilisateurs sont importés dans la CMC.

Pour vérifier les utilisateurs ou les groupes d'utilisateurs que vous avez ajoutés, sélectionnez *Gérer* > *Importer* > *Historique* dans la zone de gestion *Utilisateurs et groupes*.

6.2.11 Pour activer le compte Guest

Le compte Guest est désactivé par défaut pour garantir que personne ne puisse se connecter à la plateforme de BI à l'aide de ce compte. Ce paramètre par défaut désactive également la fonction de connexion unique anonyme de la plateforme de BI, ce qui empêche les utilisateurs d'accéder à la zone de lancement BI sans fournir un nom d'utilisateur et un mot de passe valides.

Effectuez cette tâche si vous voulez activer le compte Guest afin que les utilisateurs n'aient pas besoin de leur propre compte pour accéder à la zone de lancement BI.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Cliquez sur *Liste des utilisateurs* dans le panneau de navigation.
3. Sélectionnez *Guest*.
4. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
5. Désactivez la case *Le compte est désactivé*.
6. Cliquez sur *Enregistrer & Fermer*.

6.2.12 Ajout d'utilisateurs à des groupes

Les groupes d'utilisateurs permettent aux administrateurs d'effectuer des tâches sur la zone de lancement BI pour des lots d'utilisateurs (par exemple, vous pouvez personnaliser les préférences ou la planification des publications pour des groupes d'utilisateurs spécifiques).

Vous pouvez ajouter des utilisateurs à des groupes de la façon suivante :

- Sélectionnez le groupe, puis cliquez sur *Actions* > *Ajouter des membres au groupe*.
- Sélectionnez l'utilisateur, puis cliquez sur *Actions* > *Membre de*.
- Sélectionnez l'utilisateur, puis cliquez sur *Actions* > *Joindre au groupe*.

Il est possible d'ajouter un utilisateur à plusieurs groupes. Toutefois, si un utilisateur appartient à deux ou plusieurs groupes d'utilisateurs, la zone de lancement de BI affiche les préférences pour un seul groupe.

Informations associées

Pour définir l'appartenance à un groupe [page 110]

6.2.12.1 Ajout d'un utilisateur à un ou plusieurs groupes d'utilisateurs

Il est possible d'ajouter un utilisateur à plusieurs groupes. La zone de lancement BI affichera cependant les préférences pour un seul groupe.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, sélectionnez l'utilisateur à ajouter au groupe.
2. Cliquez sur *Actions* > *Joindre au groupe*.

   > **Remarque**
   >
   > Tous les utilisateurs de la plateforme de BI qui figurent dans le système appartiennent au groupe Tout le monde.

3. Dans la boîte de dialogue *Joindre au groupe*, déplacez le groupe auquel ajouter l'utilisateur de la liste *Groupes disponibles* à la liste *Groupe(s) de destination*.

   > **→ Conseil**
   >
   > Utilisez la combinaison de touches `MAJ`+`clic` ou `CTRL`+`clic` pour sélectionner plusieurs groupes.

4. Cliquez sur *OK*.

6.2.12.2 Ajout d'un ou plusieurs utilisateurs à un groupe d'utilisateurs

Il est possible d'ajouter plusieurs utilisateurs à un groupe d'utilisateurs.

Les préférences définies pour un groupe s'appliquent à tous les utilisateurs du groupe. La zone de lancement BI affiiche les préférences pour un groupe d'utilisateurs à la fois.

1. Dans la zone de gestion *Utilisateurs et groupes* de la CMC, sélectionnez le groupe d'utilisateurs.

2. Cliquez sur *Actions* > *Ajouter des membres au groupe*.
3. Dans la boîte de dialogue *Ajouter*, cliquez sur *Liste des utilisateurs*.
   La liste *Utilisateurs/Groupes disponibles* est actualisée et affiche tous les comptes utilisateur du système.
4. Déplacez un ou plusieurs utilisateurs du groupe de la liste *Utilisateurs/Groupes disponibles* vers la liste *Utilisateurs/Groupes sélectionnés*.

   > → Conseil
   >
   > Utilisez la combinaison de touches `MAJ`+`clic` ou `CTRL`+`clic` pour sélectionner plusieurs utilisateurs. Pour rechercher un utilisateur spécifique, entrez le nom d'utilisateur dans la zone de *recherche*.

   > → Conseil
   >
   > Si votre système contient de nombreux utilisateurs, cliquez sur les boutons *Précédent* et *Suivant* pour parcourir la liste des utilisateurs.

5. Cliquez sur *OK*.

6.2.13 Modification des paramètres de mot de passe

Dans la CMC, vous pouvez modifier les paramètres de mot de passe d'un utilisateur donné ou de tous les utilisateurs du système. Les différentes restrictions énumérées ci-dessous s'appliquent uniquement aux comptes Enterprise ; elles ne s'appliquent pas aux comptes que vous avez mappés à une base de données d'utilisateurs externe (LDAP ou Windows AD). Toutefois, et de manière générale, votre système externe vous permettra de placer des restrictions similaires sur les comptes externes.

6.2.13.1 Pour modifier les paramètres de mot de passe d'utilisateur

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur dont vous voulez modifier les paramètres de mot de passe.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Cochez ou décochez la case associée au paramètre de mot de passe que vous voulez modifier.

   Les options disponibles sont les suivantes :

   - *Le mot de passe n'expire jamais*
   - *L'utilisateur doit modifier le mot de passe à la prochaine session*
   - *L'utilisateur ne peut pas changer de mot de passe*
5. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Lorsque vous modifiez le mot de passe d'un utilisateur, l'utilisateur est déconnecté de toutes les sessions existantes et redirigé vers la page d'accueil afin de se reconnecter

6.2.13.2 Modification des paramètres généraux de mot de passe

> **Remarque**
>
> Les comptes utilisateur inactifs ne seront pas désactivés automatiquement.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Enterprise*.
   La boîte de dialogue *Enterprise* s'affiche.
3. Activez la case à cocher pour chaque paramètre de mot de passe à utiliser et renseignez-la si nécessaire.

   Le tableau suivant identifie les valeurs minimales et maximales pour chacun des paramètres que vous pouvez configurer.

   Paramètres de mot de passe

Paramètre de mot de passe	Par défaut	Valeur minimale	Valeur maximale recommandée
Doit comprendre N caractères au minimum	8 caractère	6 caractères	255 caractères
Ne doit pas dépasser N caractères	255 caractères	13 caractères	255 caractères
Doit changer de mot de passe tous les N jours	30 jours	2 jours	100 jours
Les N derniers mots de passe ne peuvent être réutilisés	3 mots de passe	1 mot de passe	100 mots de passe
Le mot de passe peut être modifié après N minute(s)	0 minutes	0 minutes	100 minutes
Désactiver le compte après N échecs de connexion	10 échec	1 échec	100 échecs
Réinitialiser le nombre d'échecs de connexion après N minute(s)	5 minutes	1 minute	100 minutes

Paramètre de mot de passe	Par défaut	Valeur minimale	Valeur maximale recommandée
Réactiver le compte après N minute(s)	5 minute	0 minutes	100 minutes

> **Remarque**
>
> Lorsque vous mettez à niveau la plateforme SAP BusinessObjects Business Intelligence d'une version antérieure vers une version supérieure ou que vous essayez d'effectuer une installation étendue, vous devez définir *Désactiver le compte après N échecs de connexion* sur la valeur par défaut.

> **Remarque**
>
> Les règles mentionnées ci-dessus sont applicables uniquement aux utilisateurs Enterprise et à aucun autre type d'authentification tiers.

4. Cliquez sur *Mettre à jour*.

6.2.14 Octroi d'un droit d'accès à des utilisateurs et à des groupes

Vous pouvez accorder à des utilisateurs et à des groupes un accès administratif à d'autres utilisateurs et groupes. Les droits d'administration incluent : affichage, modification et suppression d'objets ; affichage et suppression d'instances d'objet ; suspension d'instances d'objet. Par exemple, pour le dépannage et la maintenance du système, vous pouvez accorder au département informatique un accès permettant de modifier et de supprimer des objets.

Informations associées

Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet [page 138]

6.2.15 Contrôle de l'accès aux boîtes de réception des utilisateurs

Lorsque vous ajoutez un utilisateur, le système crée automatiquement une boîte de réception pour cet utilisateur. Cette boîte de réception porte le même nom que l'utilisateur. Par défaut, seuls l'utilisateur et l'administrateur disposent des droits nécessaires pour y accéder.

Informations associées

Gestion des paramètres de sécurité des objets dans la CMC [page 137]

6.2.16 Configuration des options de la zone de lancement BI façon Fiori

Dans la CMC, les administrateurs peuvent configurer les préférences de la zone de lancement BI façon Fiori pour des groupes d'utilisateurs.

> **Remarque**
>
> Si un utilisateur appartient à deux ou plusieurs groupes d'utilisateurs, la zone de lancement BI façon Fiori affiche les préférences configurées pour un seul groupe.

6.2.16.1 Configuration de l'écran de connexion à la zone de lancement BI façon Fiori

Par défaut, l'écran de connexion à la zone de lancement BI façon Fiori invite les utilisateurs à saisir leur nom d'utilisateur et leur mot de passe. Vous pouvez faire en sorte que les utilisateurs soient également invités à saisir le nom du CMS et le type d'authentification. Pour modifier ce paramètre, vous devez modifier les propriétés de la zone de lancement BI façon Fiori pour le fichier BOE.war.

6.2.16.1.1 Configurer l'écran de connexion à la zone de lancement BI

Pour modifier les paramètres par défaut de la zone de lancement BI façon Fiori, vous devez définir des propriétés personnalisées pour le fichier BOE.war. Ce fichier est déployé sur l'ordinateur hébergeant le serveur d'applications Web.

1. Accédez au répertoire suivant de votre installation de la plateforme de BI :

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Créez un fichier dans un éditeur de texte.
3. Enregistrez le fichier sous le nom suivant .

   `FioriBI.properties`
4. Pour inclure les options d'authentification à l'écran de connexion de la zone de lancement BI façon Fiori, ajoutez la ligne suivante :

   ```
   authentication.visible=true
   ```

5. Pour modifier l'authentification par défaut, ajoutez la ligne suivante :

```
authentication.default=<authentication>
```

Remplacez `<authentification>` par l'une des options suivantes :

Type d'authentification	valeur d'<authentification>
Enterprise	`secEnterprise`
LDAP	`secLDAP`
Windows AD	`secWinAD`
SAP	`secSAPR3`

6. Pour demander aux utilisateurs de fournir le nom du CMS dans l'écran de connexion à la zone de lancement BI façon Fiori, ajoutez la ligne suivante :

```
cms.visible=true
```

7. Enregistrez le fichier et fermez-le.
8. Redémarrez le serveur d'applications Web.

Utilisez WDeploy pour redéployer le fichier `BOE.war` sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects de Business Intelligence*.

6.2.16.2 Paramétrage des préférences de la zone de lancement BI façon Fiori pour les groupes d'utilisateurs dans la CMC

Les administrateurs configurent les préférences par défaut de la zone de lancement BI façon Fiori pour les groupes d'utilisateurs dans la CMC.

Les préférences configurées par l'administrateur pour un groupe s'appliquent à tous les utilisateurs du groupe. Si un utilisateur appartient à deux ou plusieurs groupes d'utilisateurs, la zone de lancement BI façon Fiori affiche les préférences configurées pour un seul groupe.

Les utilisateurs peuvent configurer leurs propres préférences de la zone de lancement BI façon Fiori, et leurs préférences ont la priorité sur les valeurs par défaut. Ils peuvent également revenir aux préférences par défaut à tout moment. Consultez la section *Paramétrage des préférences de la page* pour le *Guide de l'utilisateur de la zone de lancement BI façon Fiori*.

Toutefois, si l'administrateur modifie les préférences par défaut de la zone de lancement BI façon Fiori dans la CMC, les valeurs par défaut ont la priorité sur les valeurs définies par l'utilisateur.

6.2.16.2.1 Paramétrage des préférences de la zone de lancement BI façon Fiori pour un groupe d'utilisateurs

1. Accédez à la zone de gestion des *Utilisateurs et groupes* de la CMC.
2. Sous *Liste des groupes*, sélectionnez le groupe d'utilisateurs pour lequel définir les préférences de la zone de lancement BI façon Fiori.
3. Faites un clic droit et sélectionnez *Préférences de la zone de lancement BI façon Fiori*.
4. Décochez la case *Aucune préférence définie*.
5. Pour personnaliser l'onglet *Accueil*, effectuez l'une des actions suivantes pour choisir la page d'accueil que vous voulez dans l'onglet :

Option de l'onglet de page d'accueil	Action
Afficher l'onglet d'accueil par défaut de la zone de lancement BI	Sélectionnez *Onglet Accueil par défaut*.
Afficher un onglet d'accueil spécifique	Sélectionnez *Sélectionnez l'onglet Accueil*, puis : 1. Dans le champ *Page d'accueil*, sélectionnez une page d'accueil : • *Mon accueil* • *Planification* • *Boîte de réception* • *Dossiers* • *Corbeille* 2. Dans le champ *Répertorier les documents comme*, sélectionnez la *Vue Vignette (par défaut)* ou la *Vue Liste*. 3. Dans le champ *Filtre d'accueil*, sélectionnez un filtre d'accueil : • *Afficher tout* • *Mes documents* • *Toutes les catégories* • *Mes favoris* • *Mes documents affichés récemment* • *Mes documents exécutés récemment* Vous pouvez sélectionner un objet dans *Mes dossiers*, *Dossiers publics*, *Catégories personnelles* et *Catégories d'entreprise* pour l'afficher en tant que page d'accueil par défaut.
Afficher un rapport spécifique en tant que page d'accueil	Sélectionnez *Sélectionner le rapport*, puis cliquez sur *Parcourir les documents* pour sélectionner un document dans *Mes dossiers* ou dans *Dossiers publics*.

Option de l'onglet de page d'accueil	Action
Afficher une catégorie en tant que page d'accueil	Sélectionnez *Sélectionner la catégorie*, puis cliquez sur *Parcourir les catégories* pour sélectionner une catégorie dans *Catégories personnelles* ou dans *Catégories d'entreprise*.

6. Dans le champ *Choisir la colonne à afficher dans l'onglet Documents*, sélectionnez les préférences de colonnes :
   - *Type*
   - *Dernière exécution*
   - *Instances*
   - *Description*
   - *Créé par*
   - *Dernière mise à jour*
   - *Créé le*
   - *Emplacement (catégories)*
   - *Mes favoris (Page d'accueil)*
   - *Statut (Planification)*
   - *Heure de l'instance (Planification)*
   - *Chemin d'accès au dossier*

   > **Remarque**
   >
   > Les colonnes *Type*, *Description*, *Dernière exécution*, *Mes favoris (Page d'accueil)*, *Statut (Planification)* et *Heure de l'instance (Planification)* sont sélectionnées par défaut. Vous pouvez modifier la sélection des colonnes que vous voulez afficher.

7. Sélectionnez *Enregistrer et fermer*.

Si les préférences ont été définies par un administrateur et doivent se refléter sur l'interface, les utilisateurs doivent se connecter à la zone de lancement BI façon Fiori et sélectionner *Paramètres* > *Préférences du compte* > *Préférences de la page*, puis activer *Utiliser les paramètres fournis par l'administrateur*.

6.2.17 Gestion des attributs des utilisateurs système

Les administrateurs de la plateforme de BI définissent et ajoutent les attributs utilisateur aux utilisateurs système à partir de la zone *Gestion des attributs utilisateur* de la CMC (Central Management Console). Vous pouvez gérer et étendre les attributs pour les répertoires utilisateur suivants :

- Enterprise
- SAP
- LDAP
- Windows AD

Lorsque les utilisateurs sont importés à partir de répertoires externes tels que SAP, LDAP et Windows AD, les attributs suivants sont généralement disponibles pour les comptes utilisateur :

- Nom complet
- Adresse électronique

Noms d'attribut

Tous les attributs utilisateur ajoutés au système doivent comporter les propriétés suivantes :

- *Nom*
- *Nom interne*

La propriété « Nom » est l'identifiant convivial de l'attribut, elle est utilisée pour les filtres des requêtes lors de l'utilisation de la couche sémantique d'univers. Pour plus d'informations, voir la documentation de l'outil de conception d'univers. Le « Nom interne » est utilisé par les développeurs lors de l'utilisation du SDK de la plateforme de BI. Cette propriété est un nom généré automatiquement.

Les noms d'attribut ne doivent pas dépasser 256 caractères et ne doivent contenir que des caractères alphanumériques et des traits de soulignement.

> → Conseil
>
> Si vous indiquez des caractères non valides pour le nom de l'attribut, la plateforme de BI ne génère pas de nom interne. Les noms internes ne peuvent pas être modifiés après leur ajout au système. Il est conseillé de sélectionner soigneusement des noms d'attributs appropriés contenant des caractères alphanumériques et des traits de soulignement.

Prérequis pour le développement des attributs utilisateur mappés

Avant d'ajouter des attributs utilisateur au système, tous les plug-ins d'authentification pertinents des répertoires utilisateur externes doivent être configurés pour mapper et importer les utilisateurs. En outre, vous devez bien connaître le schéma des répertoires externes, en particulier les noms utilisés pour les attributs cibles.

> ⓘ Remarque
>
> Pour le plug-in d'authentification SAP, seuls les attributs contenus dans la structure BAPIADDR3 peuvent être spécifiés.

Une fois la plateforme de BI configurée pour mapper les nouveaux attributs utilisateur, les valeurs sont renseignées lors de la prochaine mise à jour planifiée. Tous les attributs utilisateur sont affichés dans la zone de gestion *Utilisateurs et groupes* de la CMC.

6.2.18 Classement des attributs utilisateur entre plusieurs options d'authentification

Lors de la configuration des plug-ins d'authentification de SAP, LDAP, et AD, il est possible de spécifier les niveaux de priorité de chaque plug-in par rapport aux deux autres. Par exemple, dans la zone d'authentification

LDAP, utilisez l'option *Définir la liaison d'attribut LDAP par rapport aux autres liaisons d'attribut* pour spécifier la priorité LDAP par rapport à SAP et AD. La valeur d'attribut Enterprise a par défaut la priorité sur toute valeur de répertoire externe. Les priorités de liaison d'attributs sont définies au niveau du plug-in d'authentification et non pas pour un attribut spécifique.

Informations associées

Pour configurer l'hôte LDAP [page 280]
Pour importer des rôles SAP [page 351]

6.2.19 Pour ajouter un nouvel attribut utilisateur

Avant d'ajouter un nouvel attribut utilisateur à la plateforme de BI, vous devez configurer le plug-in d'authentification du répertoire externe à partir duquel vous mappez les comptes utilisateur. Ceci s'applique à SAP, LDAP et Windows AD. En particulier, vous devez cocher l'option *Importer le nom complet, l'adresse électronique et les autres attributs* de tous les plugins requis.

> **Remarque**
>
> Vous n'avez aucune tâche préliminaire à exécuter avant de procéder à l'extension des attributs des comptes utilisateur Enterprise.

> **→ Conseil**
>
> Si vous prévoyez d'étendre les mêmes attributs pour plusieurs plug-ins, il est recommandé de définir le niveau de priorité de liaison approprié pour les attributs conformément aux exigences de votre entreprise.

1. Accédez à la zone de gestion *Gestion des attributs utilisateur* de la CMC.
2. Cliquez sur l'icône *Ajouter un nouvel attribut de mappage personnalisé*.
   La boîte de dialogue *Ajouter un attribut* s'affiche.
3. Spécifiez un nom pour le nouvel attribut dans le champ *Nom*.

   La plateforme de BI utilise le nom fourni comme nom convivial du nouvel attribut.

   Lorsque vous saisissez le nom convivial, le champ *Nom interne* est automatiquement rempli selon le schéma suivant : `SI_[Nomconvivival]`. Lorsque l'administrateur système spécifie un nom d'attribut "convivial", la plateforme de BI génère automatiquement le nom "interne".
4. Si nécessaire, modifiez le champ *Nom Interne* à l'aide de lettres, chiffres ou caractères de soulignement.

   > **→ Conseil**
   >
   > La valeur du champ *Nom Interne* ne peut être modifiée qu'à cette étape. Vous ne pouvez pas modifier cette valeur après avoir enregistré le nouvel attribut.

   Si le nouvel attribut concerne des comptes Enterprise, passez à l'étape 8.
5. Sélectionnez l'option appropriée pour *Ajouter une nouvelle source pour* dans la liste et cliquez sur l'icône *Ajouter*. Les options suivantes sont disponibles :

- *SAP*
- *LDAP*
- *AD*

Une ligne de table est créée pour la source de l'attribut spécifié.

6. Sous la colonne *Nom de la source de l'attribut*, spécifiez le nom de l'attribut dans le répertoire source.

   La plateforme de BI ne fournit pas de mécanisme permettant de vérifier automatiquement que le nom d'attribut fourni existe dans le répertoire externe. Assurez-vous que le nom fourni est correct et valide.
7. Répétez les étapes 5 et 6 si d'autres sources sont requises pour le nouvel attribut.
8. Cliquez sur *OK* pour enregistrer et soumettre le nouvel attribut à la plateforme de BI.
   Le nom du nouvel attribut, le nom interne, la source et le nom de la source de l'attribut s'affichent dans la zone de gestion *Gestion des attributs utilisateur* de la CMC.

Le nouvel attribut et sa valeur correspondante pour chaque compte utilisateur affecté s'afficheront lors de la prochaine actualisation planifiée dans la zone de gestion *Utilisateurs et groupes*.

Si vous utilisez plusieurs sources pour le nouvel attribut, assurez-vous que les bonnes priorités de liaison d'attributs sont spécifiées pour chaque plug-in d'authentification.

6.2.20 Modifications des attributs utilisateur personnalisés

Utilisez la procédure suivante pour modifier les attributs utilisateur ayant été créés dans la plateforme de BI. Il est possible de modifier :

- Le nom de l'attribut dans la plateforme de BI.

  > **Remarque**
  >
  > Il ne s'agit pas du nom interne utilisé pour l'attribut. Une fois l'attribut créé et ajouté à la plateforme de BI, le nom interne ne peut plus être modifié. Pour supprimer un nom interne, les administrateurs doivent supprimer l'attribut associé.
- Le nom de la source de l'attribut
- Sources supplémentaires pour l'attribut

1. Accédez à la zone de gestion *Gestion des attributs utilisateur* de la CMC.
2. Sélectionnez l'attribut à modifier.
3. Cliquez sur l'icône *Modifier l'attribut sélectionné*.
   La boîte de dialogue *Modifier* s'affiche.
4. Modifiez le nom de l'attribut ou les informations source.
5. Cliquez sur *OK* pour enregistrer et soumettre les modifications à la plateforme de BI.
   Les valeurs modifiées apparaissent dans la zone de gestion *Gestion des attributs utilisateur* de la CMC.

Le nom et les valeurs d'attribut modifiés s'affichent après la prochaine actualisation planifiée dans la zone de gestion *Utilisateurs et groupes*.

6.3 Gestion des alias

Si un utilisateur possède plusieurs comptes dans la plateforme de BI, vous pouvez les lier à l'aide de la fonction Affecter un alias. Cette fonction est utile lorsqu'un utilisateur possède un compte tiers mappé à Enterprise et un compte Enterprise.

L'affectation d'un alias à l'utilisateur permet à celui-ci de se connecter à l'aide d'un nom d'utilisateur tiers et d'un mot de passe ou d'un nom d'utilisateur Enterprise et d'un mot de passe. L'alias permet donc à un utilisateur de se connecter via plusieurs types d'authentification.

Dans la CMC, les informations d'alias sont affichées au bas de la page *Propriétés* de l'utilisateur. Un utilisateur peut posséder n'importe quelle combinaison d'alias Enterprise, LDAP ou Windows AD.

6.3.1 Pour créer un utilisateur et ajouter un alias tiers

Lorsque vous créez un utilisateur et sélectionnez un type d'authentification autre qu'Enterprise, le système crée le nouvel utilisateur dans la plateforme de BI et crée un alias tiers pour l'utilisateur.

> **Remarque**
>
> Pour que le système puisse créer l'alias tiers, les conditions suivantes doivent être respectées :
>
> - L'outil d'authentification doit avoir été activé dans la CMC.
> - Le format du nom du compte doit correspondre au format requis pour le type d'authentification.
> - Le compte utilisateur doit exister dans l'outil d'authentification tiers et doit appartenir à un groupe déjà mappé à la plateforme de BI.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Cliquez sur *Gérer* > *Nouveau* > *Nouvel utilisateur*.
   La boîte de dialogue *Nouvel utilisateur* s'affiche.
3. Sélectionnez le type d'authentification pour l'utilisateur, par exemple, Windows AD.
4. Saisissez le nom du compte tiers de l'utilisateur, par exemple, `bsmith`.
5. Sélectionnez le type de connexion pour l'utilisateur.
6. Cliquez sur *Créer et fermer*.

   L'utilisateur est ajouté à la plateforme de BI et un alias lui est attribué pour le type d'authentification sélectionné, par exemple, secWindowsAD:ENTERPRISE:bsmith. Si nécessaire, vous pouvez ajouter, affecter et réaffecter des alias à l'utilisateur.

6.3.2 Pour créer un alias pour un utilisateur existant

Vous pouvez créer des alias pour des utilisateurs existants de la plateforme de BI. Il peut s'agir d'un alias Enterprise ou d'un alias pour un outil d'authentification tiers.

> **Remarque**
>
> Pour que le système puisse créer l'alias tiers, les conditions suivantes doivent être respectées :
>
> - L'outil d'authentification doit avoir été activé dans la CMC.
> - Le format du nom du compte doit correspondre au format requis pour le type d'authentification.
> - Le compte utilisateur doit exister dans l'outil d'authentification tiers et doit appartenir à un groupe mappé à la plateforme de BI.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur auquel vous souhaitez ajouter un alias.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Cliquez sur *Nouvel alias*.
5. Sélectionnez le type d'authentification.
6. Saisissez le nom du compte de l'utilisateur.
7. Cliquez sur *Mettre à jour*.

   Un alias est créé pour l'utilisateur. Lorsque vous affichez l'utilisateur dans la CMC, au moins deux alias apparaissent, celui déjà affecté à l'utilisateur et celui que vous venez de créer.
8. Cliquez sur *Enregistrer & Fermer* pour quitter la boîte de dialogue *Propriétés*.

6.3.3 Pour affecter un alias d'un autre utilisateur

Lorsque vous affectez un alias à un utilisateur, vous déplacez un alias tiers d'un autre utilisateur vers l'utilisateur affiché. Vous ne pouvez pas affecter ou réaffecter des alias Enterprise.

> **Remarque**
>
> Si un utilisateur ne possède qu'un seul alias et si vous affectez cet alias à un autre utilisateur, le système efface le compte de l'utilisateur, ainsi que le dossier Favoris, les catégories personnelles et la boîte de réception correspondant à ce compte.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur auquel vous souhaitez affecter un alias.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Cliquez sur *Affecter un alias*.
5. Saisissez le compte utilisateur possédant l'alias que vous souhaitez affecter, et cliquez sur *Rechercher*.
6. Déplacez l'alias à affecter de la liste *Alias disponibles* vers la liste *Alias à ajouter à* `<Nomutilisateur>`.

   Ici `<Nomutilisateur>` représente le nom de l'utilisateur auquel vous affectez un alias.

   > **→ Conseil**
   >
   > Pour sélectionner plusieurs alias, utilisez la combinaison de touches `MAJ` + `clic` ou `CTRL` + `clic`.

7. Cliquez sur *OK*.

6.3.4 Pour supprimer un alias

Lorsque vous supprimez un alias, celui-ci disparaît totalement du système. Si un utilisateur ne possède qu'un seul alias que vous supprimez, le système efface automatiquement le compte de l'utilisateur, ainsi que le dossier Favoris, les catégories personnelles et la boîte de réception correspondant à ce compte.

> **Remarque**
>
> La suppression de l'alias d'un utilisateur n'empêche pas nécessairement cet utilisateur de se reconnecter à la plateforme de BI. Si le compte utilisateur existe encore dans le système tiers et si le compte appartient à un groupe mappé à la plateforme de BI, celle-ci autorisera toujours l'utilisateur à se connecter. Que le système crée un nouvel utilisateur ou qu'il affecte l'alias à un utilisateur existant dépend des options de mise à jour sélectionnées pour l'outil d'authentification dans la zone de gestion *Authentification* de la CMC.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur dont vous souhaitez supprimer l'alias.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Cliquez sur le bouton *Supprimer l'alias* situé à côté de l'alias que vous souhaitez supprimer.
5. Si vous devez confirmer, cliquez sur *OK*.
   L'alias est supprimé.
6. Cliquez sur *Enregistrer & Fermer* pour quitter la boîte de dialogue *Propriétés*.

6.3.5 Pour désactiver un alias

Vous pouvez empêcher un utilisateur de se connecter à la plateforme de BI à l'aide d'une méthode d'authentification particulière en désactivant l'alias de l'utilisateur associé à cette méthode. Pour empêcher un utilisateur d'accéder totalement à la plateforme, désactivez tous les alias de cet utilisateur.

> **Remarque**
>
> Le fait de supprimer un utilisateur du système ne l'empêche pas nécessairement de se reconnecter à la plateforme de BI. Si le compte utilisateur existe toujours dans le système tiers et s'il appartient à un groupe mappé à la plateforme de BI, le système autorisera toujours l'utilisateur à se connecter. Pour être certain qu'un utilisateur ne peut plus utiliser l'un de ses alias pour se connecter à la plateforme, il est préférable de désactiver cet alias.

1. Accédez à la zone de gestion *Utilisateurs et groupes* de la CMC.
2. Sélectionnez l'utilisateur dont vous souhaitez désactiver l'alias.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Désactivez la case à cocher *Activé* pour l'alias que vous souhaitez désactiver.

Répétez cette étape pour chaque alias que vous souhaitez désactiver.

5. Cliquez sur *Enregistrer & Fermer*.
   L'utilisateur ne peut plus se connecter à l'aide du type d'authentification que vous venez de désactiver.

Informations associées

Pour supprimer un alias [page 126]

7 Définition des droits

7.1 Fonctionnement des droits sur la plateforme de BI

Les droits sont les unités de base permettant de contrôler l'accès des utilisateurs aux objets, utilisateurs, applications, serveurs et autres fonctionnalités de la plateforme de BI. Ils jouent un rôle important dans la sécurisation du système en définissant les actions individuelles que les utilisateurs peuvent exécuter sur les objets. Les droits vous permettent non seulement de contrôler l'accès à votre contenu de la plateforme de BI, mais également de déléguer la gestion des utilisateurs et des groupes à différents services et d'accorder au personnel du service informatique un accès administratif aux serveurs et groupes de serveurs.

Il est important de noter que les droits sont définis sur des objets tels que les rapports et les dossiers plutôt que sur les utilisateurs ou groupes principaux qui y accèdent. Par exemple, pour donner à un directeur l'accès à un dossier particulier, dans la zone *Dossiers*, vous ajoutez le directeur à la liste de contrôle d'accès (liste des utilisateurs et groupes principaux qui ont accès à un objet) pour le dossier. Vous ne pouvez pas accorder l'accès au directeur en configurant ses droits d'accès dans la zone *Utilisateurs et groupes*. Les droits d'accès du directeur dans la zone *Utilisateurs et groupes* sont utilisés pour accorder à d'autres utilisateurs ou groupes principaux (tels que les administrateurs délégués) le droit d'accéder au directeur en tant qu'objet du système. De cette façon, les utilisateurs ou groupes principaux sont eux-mêmes considérés comme des objets par les autres utilisateurs disposant de droits de gestion supérieurs.

Chaque droit sur un objet peut être accordé, refusé ou non spécifié. Le modèle de sécurité de la plateforme de BI consiste à refuser un droit qui n'a pas été spécifié. Par ailleurs, ce même principe s'applique lorsque des paramètres accordent et refusent à la fois un droit à un utilisateur ou à un groupe. Ce modèle « basé sur le refus » permet de veiller à ce que les utilisateurs et les groupes n'acquièrent pas automatiquement des droits qui ne leur ont pas été accordés explicitement.

Il existe une exception importante à cette règle. Si un droit explicitement défini sur un objet enfant est en contradiction avec les droits hérités de l'objet parent, le droit défini sur l'objet enfant remplace les droits hérités. Cette exception s'applique aux utilisateurs qui sont également membres de groupes. Si un utilisateur se voit accorder explicitement un droit refusé au groupe de l'utilisateur, le droit défini sur l'utilisateur remplace les droits hérités.

Informations associées

Remplacement des droits [page 132]

7.1.1 Niveaux d'accès

Les niveaux d'accès sont des groupes de droits dont les utilisateurs ont souvent besoin. Ils permettent aux administrateurs de définir rapidement et uniformément les niveaux de sécurité courants au lieu d'avoir à définir les droits individuels un par un.

La plateforme de BI est fournie avec plusieurs niveaux d'accès prédéfinis. Ces niveaux d'accès prédéfinis reposent sur un modèle de droits progressifs : le premier étant *Visualiser* et le dernier *Contrôle total*, chaque niveau d'accès se construisant sur les droits accordés au niveau précédent.

Cependant, vous pouvez également créer et personnaliser vos propres niveaux d'accès, ce qui peut réduire de façon significative les coûts d'administration et de maintenance associés à la sécurité. Imaginez une situation dans laquelle un administrateur doit gérer deux groupes, des directeurs commerciaux et des employés commerciaux. Les deux groupes doivent accéder à cinq rapports dans le système de la plateforme de BI, mais les directeurs commerciaux requièrent davantage de droits que les employés. Les niveaux d'accès prédéfinis ne répondent aux besoins d'aucun des deux groupes. Au lieu d'ajouter des groupes à chaque rapport en tant que groupes principaux et de modifier leurs droits dans cinq emplacements différents, l'administrateur peut créer deux niveaux d'accès, Directeurs commerciaux et Employés commerciaux. L'administrateur ajoute ensuite aux rapports les deux groupes en tant que groupes principaux et affecte à ces groupes leur niveau d'accès respectif. Si les droits doivent être modifiés, l'administrateur peut modifier les niveaux d'accès. Etant donné que les niveaux d'accès s'appliquent aux deux groupes sur les cinq rapports, les droits affectés à ces groupes sur ces rapports sont rapidement mis à jour.

Informations associées

Utilisation des niveaux d'accès [page 143]

7.1.2 Définition de droits avancés

Pour vous conférer un contrôle total sur la sécurité des objets, la CMC vous permet de définir des droits avancés. Ces paramètres avancés offrent une plus grande flexibilité pour définir les niveaux de sécurité des objets à un niveau granulaire.

Utilisez des paramètres de droits avancés, par exemple, si vous devez personnaliser les droits d'accès d'un utilisateur ou groupe principal sur un objet ou un ensemble d'objets particulier. Les droits avancés sont particulièrement utiles pour refuser explicitement un droit à un utilisateur ou à un groupe, sans changement possible lors de modifications ultérieures de l'appartenance aux groupes ou des niveaux de la sécurité des dossiers.

Le tableau suivant résume les différentes options disponibles lorsque vous définissez des droits avancés.

Options des droits d'accès

Icône	Option	Description
	Accordé	Le droit est accordé à un utilisateur ou groupe principal.
	Refusé	Le droit est refusé à un utilisateur ou groupe principal.
	Non spécifié	Le droit n'est pas spécifié pour un utilisateur ou groupe principal. Par défaut, les droits définis sur *Non spécifié* sont refusés.

Icône	Option	Description
	Appliquer à l'objet	Le droit s'applique à l'objet. Cette option est disponible lorsque vous cliquez sur *Accordé* ou sur *Refusé*.
	Appliquer au sous-objet	Ce droit s'applique aux sous-objets. Cette option est disponible lorsque vous cliquez sur *Accordé* ou sur *Refusé*.

Informations associées

Droits spécifiques au type [page 135]

7.1.3 Héritage

Des droits sont définis sur un objet pour un utilisateur ou groupe principal afin de contrôler l'accès à cet objet. Cependant, il est peu pratique de définir la valeur explicite de chaque droit possible sur chaque objet pour chaque utilisateur ou groupe principal. Imaginez un système comprenant 100 droits, 1 000 utilisateurs et 10 000 objets : pour définir les droits explicitement sur chaque objet, le CMS devrait stocker des milliards de droits dans sa mémoire et, point non négligeable, un administrateur serait tenu de définir manuellement chacun d'eux.

Les profils hérités résolvent cette impraticabilité. Avec l'héritage, les droits dont les utilisateurs disposent sur les objets du système proviennent d'une combinaison de leur appartenance à différents groupes et sous-groupes et des objets qui ont hérité des droits de dossiers et sous-dossiers parents. Ces utilisateurs peuvent hériter des droits du groupe auxquels ils appartiennent ; les sous-groupes peuvent hériter des droits de leurs groupes parents et les utilisateurs et les groupes peuvent hériter des droits issus de leurs dossiers parents.

Par défaut, les utilisateurs ou groupes qui disposent de droits sur un dossier hériteront des mêmes droits sur tout objet ultérieurement publié dans ce dossier. Il est donc préférable de commencer par définir les droits d'accès appropriés pour les utilisateurs et les groupes au niveau du dossier, puis de publier des objets dans ce dossier.

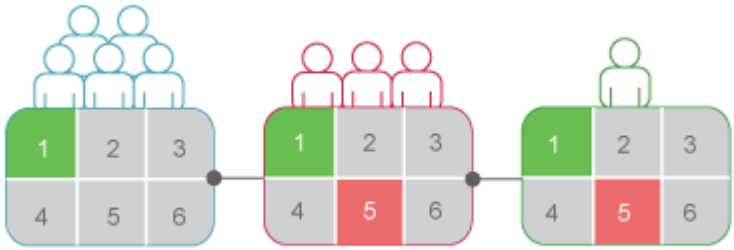
La plateforme de BI reconnaît deux types d'héritage : l'héritage de groupe et l'héritage de dossier.

7.1.3.1 Héritage de groupe

L'héritage de groupe permet aux utilisateurs ou groupes principaux d'hériter des droits des groupes auxquels ils appartiennent. L'héritage de groupe est une fonction particulièrement utile si vous organisez tous vos utilisateurs en groupes répartis selon les règles de sécurité en vigueur dans votre entreprise.

Le diagramme « Héritage de groupe - exemple 1 », illustre le mode de fonctionnement de l'héritage de groupe. Le groupe rouge est un sous-groupe du groupe bleu et il hérite par conséquent des droits du groupe bleu. Dans ce cas, il hérite du droit 1 comme étant accordé et des autres droits comme étant non spécifiés. Chaque membre du groupe rouge hérite de ces droits. En outre, tous les autres droits définis sur le sous-groupe sont

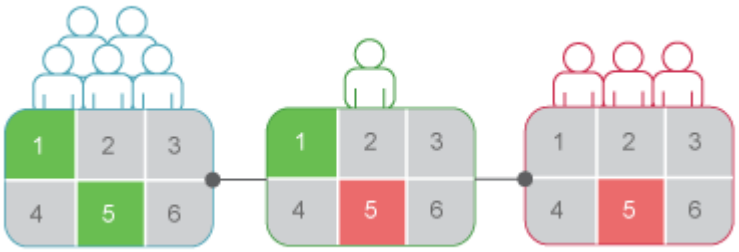
hérités par ses membres. Dans cet exemple, l'utilisateur vert est un membre du groupe rouge et il hérite par conséquent du droit 1 comme étant accordé", des droits 2, 3, 4 et 6 comme étant non spécifiés et du droit 5 comme étant refusé.



Héritage de groupe - exemple 1

Lorsque l'héritage de groupe est activé pour un utilisateur appartenant à plusieurs groupes, le système examine les droits de tous les groupes parents lors de la vérification des références de connexion. L'utilisateur se voit refuser tout droit explicitement refusé dans un groupe parent, ainsi que tout droit non spécifié. Seuls lui sont accordés les droits qu'au moins l'un des groupes lui accorde (explicitement ou par les niveaux d'accès) et qu'aucun groupe ne lui refuse explicitement.

Dans le diagramme « Héritage de groupe - exemple 2 », l'utilisateur vert est un membre de deux groupes non associés. Il hérite du groupe bleu les droits 1 et 5 accordés et les autres droits non spécifiés, cependant, étant donné que l'utilisateur vert appartient également au groupe rouge et que le droit 5 est explicitement refusé au groupe rouge, l'héritage par l'utilisateur vert du droit 5 du groupe bleu est annulé.



Héritage de groupe - exemple 2

Informations associées

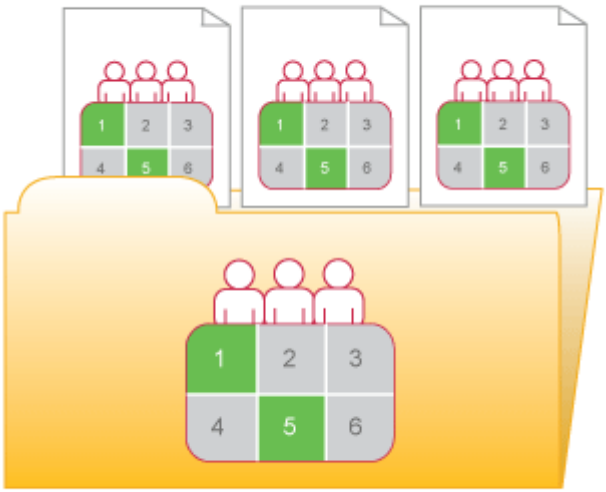
Remplacement des droits [page 132]

7.1.3.2 Héritage de dossier

L'héritage de dossier permet aux utilisateurs ou groupes principaux d'hériter de tous les droits qui leur ont été accordés sur le dossier parent d'un objet. L'héritage de dossier s'avère particulièrement utile lorsque vous

organisez le contenu de la plateforme de BI selon une hiérarchie de dossiers qui reflète les règles de sécurité en vigueur dans votre entreprise. Par exemple, supposons que vous créiez un dossier appelé Rapport des ventes et que vous accordiez à votre groupe Ventes un accès *Visualiser à la demande* pour ce dossier. Par défaut, tous les utilisateurs bénéficiant de droits sur le dossier Rapport des ventes hériteront des mêmes droits sur les rapports que vous publierez ultérieurement dans ce dossier. Le groupe Ventes aura donc un accès *Visualiser à la demande* sur tous les rapports et vous n'aurez besoin de définir les droits d'accès aux objets qu'une seule fois, au niveau du dossier.

Dans l'« Exemple d'héritage de dossier », les droits ont été définis pour le groupe rouge sur un dossier. Les droits 1 et 5 ont été accordés tandis que les autres droits sont restés non spécifiés. Si l'héritage de dossier est activé, les membres du groupe rouge disposent de droits au niveau de l'objet identiques aux droits du groupe au niveau du dossier. Les droits 1 et 5 sont hérités comme étant accordés, tandis que les autres droits restent non spécifiés.



Exemple d'héritage de dossier

Informations associées

Remplacement des droits [page 132]

7.1.3.3 Remplacement des droits

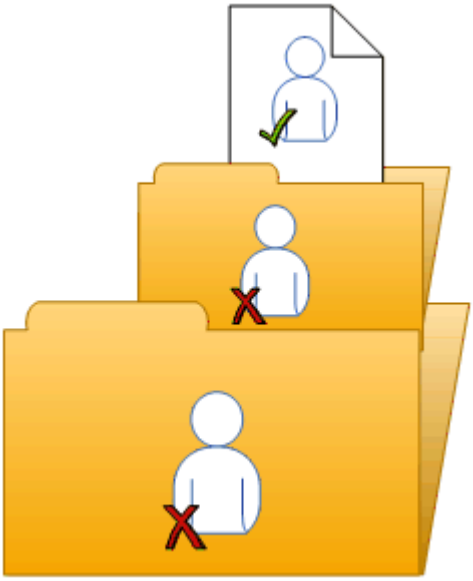
Le remplacement des droits est un comportement des droits selon lequel les droits définis sur les objets enfant remplacent les droits définis sur les objets parent. Le remplacement des droits se produit dans les circonstances suivantes :

- Généralement, les droits définis sur les objets enfant ont priorité sur les droits correspondants définis sur les objets parent.

- Généralement, les droits définis sur des sous-groupes ou membres de groupes ont priorité sur les droits correspondants définis sur les groupes.

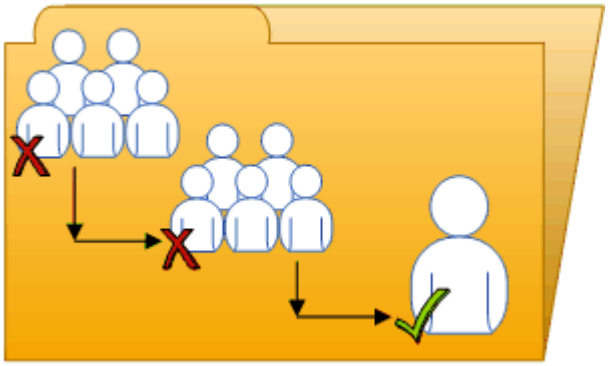
Il n'est pas nécessaire de désactiver l'héritage pour définir des droits personnalisés sur un objet. L'objet enfant hérite des paramètres de droits de l'objet parent sauf pour les droits explicitement définis sur l'objet enfant. De plus, toute modification apportée aux paramètres de droits sur l'objet parent s'applique également à l'objet enfant.

« Remplacement des droits - Exemple 1 » illustre comment fonctionne le remplacement des droits sur les objets parent et enfant. L'utilisateur bleu n'a pas le droit de modifier le contenu d'un dossier ; le sous-dossier hérite de ce paramètre de droit. Cependant, un administrateur accorde à l'utilisateur bleu des droits *Modifier* sur un document du sous-dossier. Le droit *Modifier* que l'utilisateur bleu reçoit sur le document remplace les droits hérités du dossier et du sous-dossier.



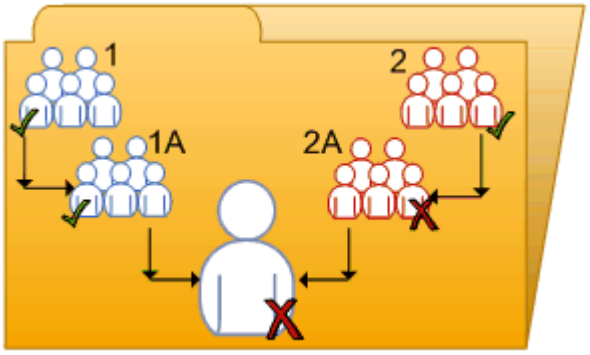
Remplacement des droits - Exemple 1

« Remplacement des droits - Exemple 2 » illustre comment fonctionne le remplacement des droits sur les membres et les groupes. Le groupe bleu n'a pas le droit de modifier un dossier ; le sous-groupe bleu hérite de ce paramètre de droit. Cependant, un administrateur accorde à l'utilisateur bleu, qui est membre du groupe bleu et du sous-groupe bleu, des droits *Modifier* sur le dossier. Les droits *Modifier* que l'utilisateur bleu obtient sur le dossier remplacent les droits hérités du groupe bleu et du sous-groupe bleu.



Remplacement des droits - Exemple 2

La section « Remplacement des droits complexe » illustre une situation dans laquelle les effets du remplacement de droits sont moins évidents. L'utilisateur violet est membre des sous-groupes 1A et 2A, qui se trouvent respectivement dans les groupes 1 et 2. Les groupes 1 et 2 possèdent tous deux des droits *Modifier* sur le dossier. Le groupe 1A hérite des droits *Modifier* du groupe 1, mais un administrateur refuse ces droits *Modifier* au groupe 2A. Les paramètres de droits du groupe 2A remplacent ceux du groupe 2 en raison du remplacement des droits. Par conséquent, l'utilisateur violet hérite de paramètres de droits contradictoires des groupes 1A et 2A. Les groupes 1A et 2A n'ont pas de relation parent-enfant ; par conséquent, le remplacement des droits ne s'applique pas. Les paramètres de droit d'un sous-groupe ne remplacent pas ceux d'un autre car ils ont un statut égal. L'utilisateur violet se voit donc refuser les droits *Modifier* en raison du modèle de droits « basé sur le refus » de la plateforme de BI.



Remplacement des droits complexe

Le remplacement des droits vous permet d'apporter de petites modifications aux paramètres de droits sur un objet enfant sans annuler tous les paramètres de droits hérités. Prenons l'exemple d'un responsable des ventes qui doit visualiser des rapports confidentiels situés dans le dossier Confidentiel. Le responsable des ventes fait partie du groupe Ventes qui n'a pas accès au dossier et à son contenu. L'administrateur accorde au responsable les droits *Visualiser* sur le dossier Confidentiel et continue à en refuser l'accès au groupe Ventes. Dans ce cas, les droits *Visualiser* accordés au responsable des ventes remplacent l'accès refusé dont il a hérité en tant que membre du groupe Ventes.

7.1.3.4 Périmètre des droits

Le périmètre des droits permet de contrôler la portée de l'héritage des droits. Pour définir le périmètre d'un droit, vous décidez si le droit s'applique à l'objet, à ses sous-objets ou aux deux. Par défaut, le périmètre d'un droit s'étend aux objets et aux sous-objets.

Le périmètre des droits peut être utilisé pour protéger un contenu personnel dans des emplacements partagés. Imaginez une situation dans laquelle le service financier possède un dossier Notes de frais partagé contenant un sous-dossier Notes de frais personnelles pour chaque employé. Les employés souhaitent être en mesure de visualiser le dossier Notes de frais et d'y ajouter des objets, mais ils veulent également protéger le contenu de leur sous-dossier Notes de frais personnelles. L'administrateur accorde à tous les employés les droits *Visualiser* et *Ajouter* sur le dossier Notes de frais et limite le périmètre de ces droits à ce dossier uniquement. Les droits *Visualiser* et *Ajouter* ne s'appliquent donc pas aux sous-objets du dossier Notes de frais. L'administrateur accorde ensuite aux employés les droits *Visualiser* et *Ajouter* sur leur propre sous-dossier Notes de frais personnelles.

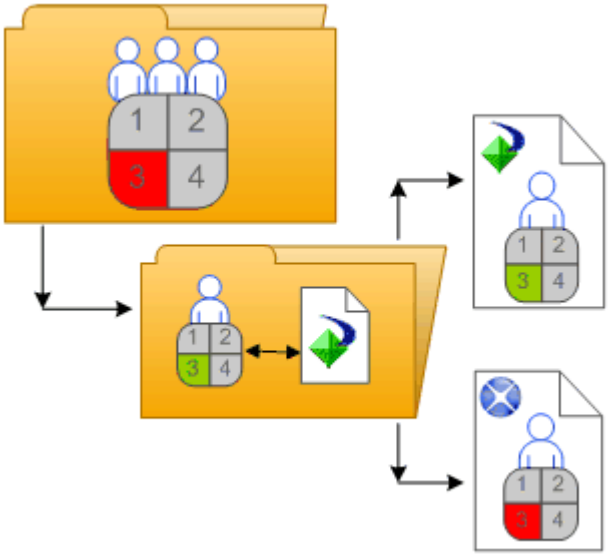
Le périmètre des droits peut également limiter les droits effectifs que possède un administrateur délégué. Par exemple, un administrateur délégué peut disposer de droits *Modifier en toute sécurité* et *Modifier* sur un dossier, mais le périmètre de ces droits est limité au dossier uniquement et ne s'applique pas à ses sous-objets. L'administrateur délégué ne peut pas accorder ces droits à un autre utilisateur sur l'un des sous-objets du dossier.

7.1.4 Droits spécifiques au type

Les droits spécifiques au type sont des droits affectant uniquement des types d'objets spécifiques, tels que des rapports Crystal, des dossiers ou des niveaux d'accès. Les droits spécifiques au type sont répartis comme suit :

- Droits généraux pour le type d'objet
  Ces droits sont identiques aux droits globaux généraux (par exemple, droit d'ajout, de suppression ou de modification d'un objet), mais vous les définissez sur des types d'objet spécifiques qui remplacent les paramètres de droits globaux généraux.
- Droits spécifiques pour le type d'objet
  Ces droits sont disponibles uniquement pour des types d'objets spécifiques. Par exemple, le droit d'exportation des données d'un rapport s'affiche pour les rapports Crystal mais pas pour les documents Word.

Le diagramme « Droits spécifiques au type : exemple » illustre le fonctionnement des droits spécifiques au type. Dans ce diagramme, le droit 3 représente le droit de modification d'un objet Le groupe bleu ne dispose pas du droit *Modifier* sur le dossier de niveau supérieur mais se voit attribuer ce droit, pour les rapports Crystal situés dans le dossier et le sous-dossier. Ces droits *Modifier* sont spécifiques aux rapports Crystal et remplacent les paramètres de droit d'un niveau d'accès global général. Par conséquent, les membres du groupe bleu possèdent des droits *Modifier* pour les rapports Crystal mais pas pour le fichier XLF contenu dans le sous-dossier.



Droits spécifiques au type : exemple

Les droits spécifiques au type sont utiles car ils vous permettent de limiter les droits des utilisateurs ou groupes principaux en fonction du type d'objet. Prenons l'exemple d'un administrateur qui souhaite que les employés puissent ajouter des objets à un dossier mais pas créer de sous-dossiers. L'administrateur accorde les droits *Ajouter* au niveau global général pour le dossier, puis refuse les droits *Ajouter* pour le type d'objet Dossier.

Les droits sont répartis dans les ensembles suivants en fonction des types d'objet auxquels ils s'appliquent :

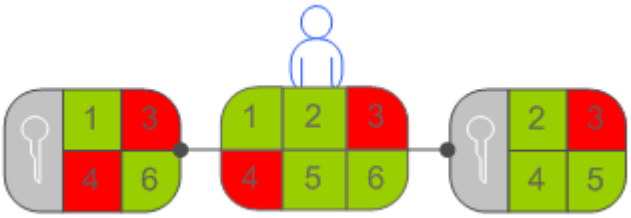
- *Général*
  Ces droits affectent tous les objets.
- *Contenu*
  Ces droits sont répartis en fonction des types de contenu d'objet particuliers. Les types de contenu d'objet peuvent être, par exemple, des rapports Crystal et des fichiers PDF Adobe Acrobat.
- *Application*
  Ces droits sont répartis en fonction de l'application de la plateforme de BI affectée. Les applications peuvent être, par exemple, la CMC et la zone de lancement BI.
- *Système*
  Ces droits sont répartis en fonction du composant système principal affecté. Les composants système principaux peuvent être, par exemple, des calendriers, des événements ou encore des utilisateurs et des groupes.

Les droits spécifiques au type se trouvent dans les ensembles *Contenu*, *Application* et *Système*. Dans chaque ensemble, les droits sont encore répartis dans d'autres catégories en fonction du type d'objet.

7.1.5 Détermination des droits effectifs

Tenez compte des éléments suivants lorsque vous définissez les droits d'accès à un objet :

- Chaque niveau d'accès accorde et refuse certains droits et attribut le statut "non spécifié" aux autres droits. Lorsque plusieurs niveaux d'accès sont accordés à un utilisateur, le système agrège les droits effectifs et, par défaut, refuse tout droit non spécifié.
- Lorsque vous attribuez plusieurs niveaux d'accès à un utilisateur ou groupe principal pour un objet, cet utilisateur ou groupe principal bénéficie de la combinaison des droits de chaque niveau d'accès. Deux niveaux d'accès sont attribués à l'utilisateur de « Plusieurs niveaux d'accès ». L'un des niveaux d'accès accorde à l'utilisateur les droits 3 et 4, alors que l'autre niveau accorde uniquement le droit 3. Les droits effectifs de cet utilisateur sont donc les droits 3 et 4.



Plusieurs niveaux d'accès

- Les droits avancés peuvent être associés aux niveaux d'accès pour personnaliser les paramètres des droits d'accès à un objet d'un utilisateur ou d'un groupe principal. Par exemple, si un droit avancé et un niveau d'accès sont attribués explicitement à un utilisateur ou un groupe principal pour un objet et si le droit avancé est en contradiction avec un des droits du niveau d'accès, le droit avancé remplace le droit du niveau d'accès.
  Les droits avancés peuvent remplacer leurs équivalents dans les niveaux d'accès uniquement s'ils sont définis sur le même objet pour le même utilisateur ou groupe principal. Par exemple, un droit avancé Ajouter défini au niveau global général peut remplacer le droit Ajouter général défini pour un niveau d'accès. En revanche, il ne peut pas remplacer un droit Ajouter spécifique à un type dans un niveau d'accès.
  Toutefois, les droits avancés ne remplacent pas toujours les niveaux d'accès. Imaginons un utilisateur ou un groupe principal ne disposant pas du droit *Modifier* sur un objet parent. En revanche, cet utilisateur ou ce groupe principal dispose d'un niveau d'accès qui lui accorde le droit *Modifier* sur l'objet enfant. L'utilisateur ou le groupe principal dispose donc bien du droit *Modifier* sur l'objet enfant, car les droits définis pour l'objet enfant remplacent ceux définis pour l'objet parent.
- Le droit de priorité permet de remplacer les droits hérités de l'objet parent par les droits définis pour un objet enfant.

7.2 Gestion des paramètres de sécurité des objets dans la CMC

Vous pouvez gérer les paramètres de sécurité de la plupart des objets de la CMC à l'aide des options de sécurité du menu *Gérer*. Ces options permettent d'affecter des utilisateurs ou groupes principaux à la liste de contrôle d'accès d'un objet, à visualiser les droits dont dispose un utilisateur ou groupe principal et à modifier les droits de l'utilisateur ou groupe principal sur cet objet.

La procédure spécifique de gestion de la sécurité varie en fonction de vos besoins en matière de sécurité et du type d'objet pour lequel vous définissez des droits. Toutefois, en règle générale, le workflow des tâches suivantes varie peu :

- Visualisation des droits dont dispose un utilisateur ou groupe principal sur un objet.
- Affectation d'utilisateurs ou de groupes principaux à une liste de contrôle d'accès pour un objet et indication des droits et niveaux d'accès dont ces utilisateurs et groupes principaux disposent.
- Définition des droits sur un dossier de niveau supérieur dans la plateforme de BI.

7.2.1 Pour visualiser les droits d'un utilisateur ou groupe principal sur un objet

En règle générale, vous suivez ce workflow pour visualiser les droits dont dispose un utilisateur ou groupe principal sur un objet.

1. Sélectionnez l'objet dont vous voulez visualiser les paramètres de sécurité.
2. Cliquez sur *Gérer* > *Sécurité de l'utilisateur*.
   La boîte de dialogue *Sécurité de l'utilisateur* apparaît et affiche la liste de contrôle d'accès de l'objet.
3. Sélectionnez un utilisateur/groupe principal dans la liste de contrôle d'accès, puis cliquez sur *Visualiser la sécurité*.

   L'*Explorateur d'autorisations* s'ouvre et affiche la liste des droits effectifs dont dispose l'utilisateur ou groupe principal sur l'objet. En outre, l'*Explorateur d'autorisations* permet d'effectuer les tâches suivantes :

   - Rechercher un autre utilisateur ou groupe principal dont vous voulez visualiser les droits.
   - Filtrer les droits affichés selon les critères suivants :

     Droits affectés
     Droits accordés
     Droits non affectés
     A partir du niveau d'accès
     Type d'objet
     Nom du droit
   - Trier la liste de droits affichée par ordre croissant ou décroissant selon les critères suivants :

     Collection
     Type
     Nom du droit
     Statut du droit (accordé, refusé ou non spécifié)

   En outre, vous pouvez cliquer sur l'un des liens dans la colonne *Source* pour afficher la source des droits hérités.

7.2.2 Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet

Les listes de contrôle d'accès spécifient les utilisateurs auxquels des droits sont accordés ou refusés sur un objet. En règle générale, vous suivez ce workflow pour affecter un utilisateur ou groupe principal à une liste de contrôle d'accès d'un objet et pour spécifier les droits dont dispose l'utilisateur ou le groupe principal sur cet objet.

1. Sélectionnez l'objet auquel ajouter un utilisateur ou groupe principal.
2. Cliquez sur *Gérer* > *Sécurité de l'utilisateur*.
   La boîte de dialogue *Sécurité de l'utilisateur* apparaît et affiche la liste de contrôle d'accès.
3. Cliquez sur *Ajouter des utilisateurs/groupes principaux*.
   La boîte de dialogue *Ajouter des utilisateurs/groupes principaux* s'affiche.
4. Déplacez les utilisateurs et groupes que vous souhaitez ajouter en tant qu'utilisateurs ou groupes principaux de la liste *Utilisateurs/Groupes disponibles* vers la liste *Utilisateurs/Groupes sélectionnés*.
5. Cliquez sur *Ajouter et affecter la sécurité*.
6. Sélectionnez les niveaux d'accès que vous voulez accorder à l'utilisateur ou groupe principal.
7. Choisissez d'activer ou non l'héritage de groupe ou de dossier.

Si nécessaire, vous pouvez également modifier les droits à un niveau granulaire pour remplacer certains droits à un niveau d'accès donné.

Informations associées

Pour modifier les droits d'un utilisateur ou groupe principal sur un objet [page 139]

7.2.3 Pour modifier les droits d'un utilisateur ou groupe principal sur un objet

En règle générale, il est recommandé d'utiliser des droits d'accès pour accorder des droits à un utilisateur ou groupe principal. Toutefois, vous devrez peut-être remplacer certains droits granulaires à un niveau d'accès donné dans certaines circonstances. Les droits avancés permettent de personnaliser les droits d'un utilisateur ou groupe principal en venant s'ajouter aux niveaux d'accès dont dispose déjà cet utilisateur ou groupe principal. En règle générale, vous suivez ce workflow pour attribuer des droits avancés à un utilisateur ou groupe principal sur un objet.

1. Affectez l'utilisateur/groupe principal à la liste de contrôle d'accès pour l'objet.
2. Une fois l'utilisateur/groupe principal ajouté, accédez à *Gérer* > *Sécurité de l'utilisateur* pour afficher la liste de contrôle d'accès de l'objet.
3. Sélectionnez l'utilisateur ou groupe principal dans la liste de contrôle d'accès, puis cliquez sur *Affecter la sécurité*.
   La boîte de dialogue *Affecter la sécurité* s'affiche.
4. Cliquez sur l'onglet *Avancé*.
5. Cliquez sur *Ajouter/Supprimer des droits*.
6. Modifiez les droits de l'utilisateur ou groupe principal.
   Tous les droits disponibles sont résumés dans l'*annexe Droits*.

Informations associées

Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet [page 138]

7.2.4 Définition des droits sur un dossier de niveau supérieur dans la plateforme de BI

En règle générale, vous suivez ce workflow pour définir des droits sur un dossier de niveau supérieur dans la plateforme de BI.

> **Remarque**
>
> Pour cette version, les utilisateurs et groupes principaux ont besoin de droits *Visualiser* pour pouvoir naviguer dans ce dossier et afficher ses sous-objets. Cela signifie qu'ils ont besoin de droits *Visualiser* sur le dossier de niveau supérieur pour visualiser les objets contenus dans les dossiers. Si vous souhaitez limiter les droits *Visualiser* d'un utilisateur ou groupe principal, vous pouvez lui accorder les droits *Visualiser* sur un dossier spécifique et définir le périmètre des droits à appliquer à ce seul dossier.

1. Accédez à la zone de la CMC où se trouve le dossier de niveau supérieur pour lequel définir des droits.
2. Cliquez sur *Gérer* > *Sécurité de niveau supérieur* > *Tous les* `<Objets>`.

   `<Objets>` désigne ici le contenu du dossier de niveau supérieur. Si vous devez confirmer, cliquez sur *OK*.

   La boîte de dialogue *Sécurité de l'utilisateur* apparaît et affiche la liste de contrôle d'accès du dossier de niveau supérieur.
3. Affectez l'utilisateur ou groupe principal à la liste de contrôle d'accès du dossier de niveau supérieur.
4. Si nécessaire, affectez des droits avancés à l'utilisateur ou groupe principal.

Informations associées

Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet [page 138]
Pour modifier les droits d'un utilisateur ou groupe principal sur un objet [page 139]

7.2.5 Vérification des paramètres de sécurité pour un utilisateur ou un groupe principal

Dans certains cas, vous pouvez avoir besoin de savoir quels sont les objets auxquels un utilisateur ou groupe principal s'est vu accorder ou refuser l'accès. Pour ce faire, vous pouvez utiliser une requête de sécurité.
Les requêtes de sécurité permettent de déterminer les objets sur lesquels un utilisateur ou groupe principal possède des droits et de gérer les droits utilisateur. Pour chaque requête de sécurité, vous devez fournir les informations suivantes :

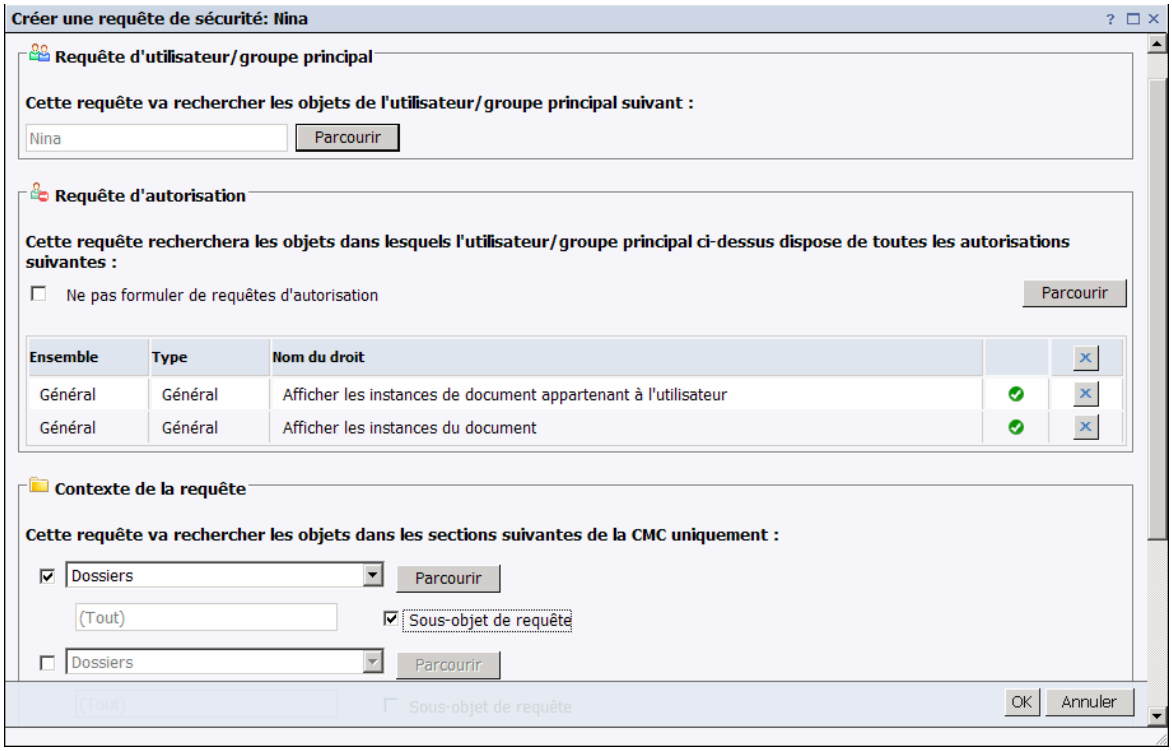
- Requête d'utilisateur/groupe principal
  Spécifiez l'utilisateur ou le groupe pour lequel vous souhaitez exécuter la requête de sécurité. Vous pouvez spécifier un utilisateur ou groupe principal pour chaque requête de sécurité.
- Requête d'autorisation
  Spécifiez les droits pour lesquels vous souhaitez exécuter la requête de sécurité, le statut de ces droits et le type d'objet sur lequel ces droits sont définis. Vous pouvez, par exemple, exécuter une requête de sécurité pour tous les rapports qu'un utilisateur ou groupe principal peut actualiser ou pour tous les rapports qu'un utilisateur ou groupe principal ne peut pas exporter.
- Contexte de la requête
  Spécifiez les zones de la CMC que vous souhaitez faire rechercher par la requête de sécurité. Pour chaque zone, vous pouvez choisir d'inclure ou non des sous-objets dans la requête de sécurité. Une requête de sécurité peut inclure au maximum quatre zones.

Lorsque vous exécutez une requête de sécurité, les résultats s'affichent dans la zone *Résultats de requête* du volet *Arborescence* sous *Requêtes de sécurité*. Si vous souhaitez affiner une requête de sécurité, vous pouvez exécuter une seconde requête à l'intérieur des résultats à partir de la première requête.

Les requêtes de sécurité sont utiles car elles vous permettent de voir les objets sur lesquels un utilisateur ou groupe principal possède des droits, et elles fournissent également les emplacements de ces objets si vous souhaitez modifier ces droits. Imaginez une situation dans laquelle un employé commercial est promu au rang de directeur commercial. Le directeur commercial requiert des droits *Planifier* pour les rapports Crystal sur lesquels il ne possédait auparavant que les droits *Visualiser*, et ces rapports se trouvent dans des dossiers différents. Dans ce cas, l'administrateur exécute une requête de sécurité pour que les droits du directeur commercial lui permettent de visualiser les rapports Crystal dans tous les dossiers et inclut les sous-objets dans la requête. Une fois la requête de sécurité exécutée, l'administrateur peut voir tous les rapports Crystal pour lesquels le directeur commercial possède des droits *Visualiser* dans la zone *Résultats de requête*. Le volet *Détails* affichant l'emplacement de chaque rapport Crystal, l'administrateur peut rechercher chaque rapport et modifier les droits du directeur commercial sur ces rapports.

7.2.5.1 Pour exécuter une requête de sécurité

1. Dans la zone *Utilisateurs et groupes*, dans le volet *Détails*, sélectionnez l'utilisateur ou le groupe pour lequel vous voulez exécuter une requête de sécurité.
2. Cliquez sur *Gérer* > *Outils* > *Créer une requête de sécurité*.



La boîte de dialogue *Créer une requête de sécurité* s'affiche.

3. Assurez-vous que l'utilisateur ou groupe principal dans la zone *Requête d'utilisateur/groupe principal* est correct.

   Si vous souhaitez exécuter une requête de sécurité pour un utilisateur ou groupe principal différent, vous pouvez cliquer sur *Parcourir* pour en sélectionner un autre. Dans la boîte de dialogue *Rechercher la requête d'utilisateur/groupe principal*, développez la *Liste des utilisateurs* ou la *Liste des groupes* pour accéder à l'utilisateur ou au groupe principal ou le rechercher à l'aide de son nom. Lorsque vous avez terminé, cliquez sur *OK* pour revenir à la boîte de dialogue *Créer une requête de sécurité*.

4. Dans la zone *Requête d'autorisation*, spécifiez les droits et le statut de chaque droit pour lequel vous souhaitez exécuter la requête.

   - Si vous souhaitez exécuter une requête pour des droits spécifiques dont dispose un utilisateur/groupe principal sur des objets, cliquez sur *Parcourir*, définissez le statut de chaque droit pour lequel exécuter la requête de sécurité, puis cliquez sur *OK*.

     > → Conseil
     >
     > Vous pouvez supprimer des droits spécifiques de la requête en cliquant sur le bouton Supprimer figurant à droite ou supprimer tous les droits de la requête en cliquant sur le bouton Supprimer figurant dans la ligne d'en-tête.

   - Si vous souhaitez exécuter une requête de sécurité générale, activez la case à cocher *Ne pas formuler de requêtes d'autorisation*.
     Lorsque vous procédez de la sorte, la plateforme de BI exécute une requête de sécurité générale pour tous les objets dans les listes de contrôle d'accès où figure l'utilisateur ou groupe principal, quelles que soient les autorisations dont dispose cet utilisateur ou groupe principal sur ces objets.

5. Dans la zone *Contexte de la requête*, spécifiez les zones de la CMC à interroger.
   a. Activez une case à cocher en regard d'une liste.

b. Dans la liste, sélectionnez une zone de la CMC à interroger.

   Si vous souhaitez interroger un emplacement plus spécifique (par exemple, un dossier particulier sous Dossiers), cliquez sur *Parcourir* pour ouvrir la boîte de dialogue *Rechercher le contexte de la requête*. Dans le volet *Détails*, sélectionnez le dossier à interroger, puis cliquez sur *OK*. Lorsque vous revenez à la boîte de dialogue *Requête de sécurité*, le dossier que vous avez spécifié apparaît dans la zone située sous la liste.

c. Sélectionnez *Sous-objet de requête*.

d. Répétez les étapes ci-dessus pour chaque zone de la CMC que vous souhaitez interroger.

> **ⓘ Remarque**
>
> Vous pouvez interroger jusqu'à quatre zones.

6. Cliquez sur *OK*.
   La requête de sécurité s'exécute et la zone *Résultats de requête* apparaît.
7. Pour visualiser les résultats de la requête, dans le volet *Arborescence*, développez *Requêtes de sécurité*, puis cliquez sur un résultat de requête.

   > **→ Conseil**
   >
   > Les résultats de requête sont répertoriés par nom d'utilisateur ou groupe principal.

   Ces résultats sont affichés dans le volet *Détails*.

La zone *Résultats de requête* contient tous les résultats des requêtes de sécurité formulées au cours d'une session utilisateur jusqu'à ce que cet utilisateur se déconnecte. Si vous souhaitez réexécuter la requête avec de nouvelles spécifications, cliquez sur *Actions* > *Modifier la requête*. Vous pouvez également réexécuter la même requête en la sélectionnant, puis en cliquant sur *Actions* > *Réexécuter la requête*. Si vous souhaitez conserver les résultats de la requête de sécurité, cliquez sur *Actions* > *Exporter* afin d'exporter les résultats de la requête de sécurité sous la forme d'un fichier CSV.

7.3 Utilisation des niveaux d'accès

Vous pouvez effectuer les tâches suivantes avec les niveaux d'accès :

- Copier un niveau d'accès existant, apporter des modifications au niveau d'accès copié, le renommer et l'enregistrer en tant que nouveau niveau d'accès.
- Créer, renommer et supprimer des niveaux d'accès.
- Modifier les droits d'un niveau d'accès.
- Suivre la relation entre les niveaux d'accès et d'autres objets dans le système.
- Répliquer et gérer les niveaux d'accès sur différents sites.
- Utiliser l'un des niveaux d'accès prédéfinis dans la plateforme de BI pour définir des droits rapidement et uniformément pour de nombreux utilisateurs ou groupes principaux.

Le tableau suivant récapitule les droits contenus dans chaque niveau d'accès prédéfini.

Niveaux d'accès prédéfinis

Niveau d'accès	Description	Droits impliqués
Visualiser	Si ce niveau d'accès est défini au niveau d'un dossier, un utilisateur ou groupe principal peut visualiser le dossier, les objets qu'il contient et les instances générées de chaque objet. S'il est défini au niveau d'un objet, un utilisateur ou groupe principal peut visualiser l'objet, son historique et ses instances générées.	• Visualiser les objets • Afficher les instances du document
Planifier	Un utilisateur ou groupe principal peut générer des instances en planifiant l'exécution d'un objet avec une source de données définie une seule fois ou de manière récurrente. L'utilisateur ou le groupe principal peut visualiser, supprimer et suspendre la planification des instances qui lui appartiennent. Il peut également planifier l'exécution vers d'autres formats et destinations, définir des paramètres et des informations de connexion à la base de données, choisir les serveurs qui traiteront les travaux, ajouter du contenu au dossier et copier l'objet ou le dossier.	Droits du niveau d'accès *Visualiser*, plus : • Planifier l'exécution du document • Définir les groupes de serveurs pour traiter les tâches • Copier les objets dans un autre dossier • Planifier vers des destinations • Imprimer les données du rapport • Exporter les données du rapport • Modifier les objets appartenant à l'utilisateur • Supprimer les instances appartenant à l'utilisateur • Suspendre et reprendre les instances de document appartenant à l'utilisateur
Visualiser à la demande	Un utilisateur ou groupe principal peut actualiser les données à la demande par rapport à une source de données.	Droits du niveau d'accès *Planifier*, plus : • Actualiser les données du rapport
Contrôle total	Un utilisateur ou groupe principal a le contrôle administratif total de l'objet.	Tous les droits disponibles, notamment : • Ajouter les objets au dossier • Modifier les objets • Modifier les droits des utilisateurs sur les objets • Supprimer les objets • Supprimer les instances

Le tableau suivant récapitule les droits requis pour effectuer certaines tâches sur des niveaux d'accès.

Tâche de niveau d'accès	Droits requis
Création d'un niveau d'accès	Droit *Ajouter* sur le dossier racine des *niveaux d'accès*
Visualisation de droits granulaires dans un niveau d'accès	Droit *Visualiser* sur le niveau d'accès
Attribution d'un niveau d'accès à un utilisateur ou groupe principal sur un objet	Droit *Visualiser* sur le niveau d'accès

Tâche de niveau d'accès	Droits requis
	Droit *Utiliser le niveau d'accès pour affecter la sécurité* sur le niveau d'accès Droit *Modifier les droits* sur l'objet ou droit *Modifier les droits en toute sécurité* sur l'objet et l'utilisateur ou groupe principal. **Remarque** Les utilisateurs disposant du droit *Modifier les droits en toute sécurité* souhaitant affecter un niveau d'accès à un utilisateur ou groupe principal doivent disposer du même niveau d'accès.
Modification d'un niveau d'accès	Droits *Visualiser* et *Modifier* sur le niveau d'accès
Suppression d'un niveau d'accès	Droits *Visualiser* et *Supprimer* sur le niveau d'accès
Clonage d'un niveau d'accès	Droit *Visualiser* sur le niveau d'accès Droit *Copier* sur le niveau d'accès Droit *Ajouter* sur le dossier racine des *niveaux d'accès*

7.3.1 Choisir entre les niveaux d'accès *Visualiser* et *Visualiser à la demande*

Le choix entre des données réelles ou enregistrées constitue l'une des décisions les plus importantes à prendre en matière de gestion de rapports sur le Web. Quel que soit le choix effectué, la plateforme de BI affiche la première page aussi rapidement que possible, de façon à ce que vous puissiez visualiser votre rapport tandis que le reste des données est traité. Cette section explique la différence entre deux niveaux d'accès prédéfinis que vous pouvez utiliser pour prendre votre décision.

Niveau d'accès *Visualiser à la demande*

Le reporting à la demande permet aux utilisateurs d'accéder en temps réel aux données stockées sur le serveur de base de données. Les données réelles permettent aux utilisateurs d'accéder aux toutes dernières informations à la seconde près. Par exemple, si les responsables d'un centre de distribution de taille importante doivent connaître la situation de leur stock de façon continue, le reporting à partir des données réelles est la meilleure façon de procéder pour leur procurer les informations dont ils ont besoin.

Toutefois, avant de fournir des données réelles pour tous les rapports, vous devez décider s'il est souhaitable que tous les utilisateurs sollicitent sans arrêt le serveur de base de données. Si les données ne sont pas appelées à changer constamment, toutes ces requêtes envoyées à la base de données n'auront pour effet que d'accroître le trafic sur le réseau et de monopoliser les ressources du serveur. Dans ce cas, il est souvent préférable de planifier les rapports à intervalles réguliers afin que les utilisateurs puissent toujours visualiser des données récentes (dans des instances de rapport) sans solliciter le serveur de base de données.

Les utilisateurs doivent disposer d'un accès de type *Visualiser à la demande* pour pouvoir actualiser les rapports par rapport aux informations de la base de données.

Niveau d'accès *Visualiser*

Pour réduire le trafic réseau et le nombre d'accès aux serveurs de base de données, vous pouvez planifier l'exécution des rapports à des heures spécifiées. Une fois le rapport exécuté, les utilisateurs peuvent afficher l'instance du rapport selon leurs besoins, sans effectuer d'accès supplémentaires à la base de données.

Les instances de rapport permettent de traiter les données qui ne sont pas souvent mises à jour. Lorsque les utilisateurs parcourent des instances de rapport et explorent en avant les informations détaillées des colonnes ou des diagrammes, ils n'accèdent pas directement au serveur de base de données, mais aux données enregistrées. Par conséquent, les rapports contenant des données enregistrées permettent non seulement de réduire le transfert de données sur le réseau, mais aussi d'alléger la charge de travail du serveur de base de données.

Par exemple, si votre base de données des ventes est mise à jour quotidiennement, vous pouvez exécuter le rapport selon une planification similaire. Vos représentants commerciaux ont ainsi toujours accès aux données les plus à jour, mais ne sollicitent pas systématiquement la base de données chaque fois qu'ils ouvrent un rapport.

Pour pouvoir afficher les instances de rapport, les utilisateurs ont uniquement besoin d'un accès de type *Visualiser*.

7.3.2 Pour copier un niveau d'accès existant

Voici le meilleur moyen de créer un niveau d'accès qui diffère peu de l'un des niveaux d'accès existants.

1. Accédez à la zone *Niveaux d'accès*.
2. Dans le volet *Détails*, sélectionnez un niveau d'accès.

   > → Conseil
   >
   > Sélectionnez un niveau d'accès contenant des droits similaires à ceux que vous souhaitez attribuez à votre niveau d'accès.

3. Cliquez sur *Organiser* > *Copier*.
   Une copie du niveau d'accès sélectionné apparaît dans le volet *Détails*.

7.3.3 Pour créer un niveau d'accès

Voici le meilleur moyen de créer un niveau d'accès très différent des niveaux d'accès existants.

1. Accédez à la zone *Niveaux d'accès*.
2. Cliquez sur *Gérer* > *Nouveau* > *Créer un niveau d'accès*.

La boîte de dialogue*Créer un niveau d'accès* s'affiche.

3. Saisissez le titre et la description de votre nouveau niveau d'accès, puis cliquez sur *OK*.
   Vous revenez à la zone *Niveaux d'accès* et le nouveau niveau d'accès apparaît dans le volet *Détails*.

7.3.4 Pour renommer un niveau d'accès

1. Dans la zone *Niveaux d'accès* du volet *Détails*, sélectionnez le niveau d'accès que vous souhaitez renommer.
2. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
3. Dans le champ *Titre*, saisissez le nom du niveau d'accès, puis cliquez sur *Enregistrer et fermer*.
   Vous revenez à la zone *Niveaux d'accès*.

7.3.5 Pour supprimer un niveau d'accès

1. Dans la zone *Niveaux d'accès*, dans le volet*Détails*, sélectionnez le niveau d'accès à supprimer.
2. Cliquez sur *Gérer* > *Supprimer un niveau d'accès*.

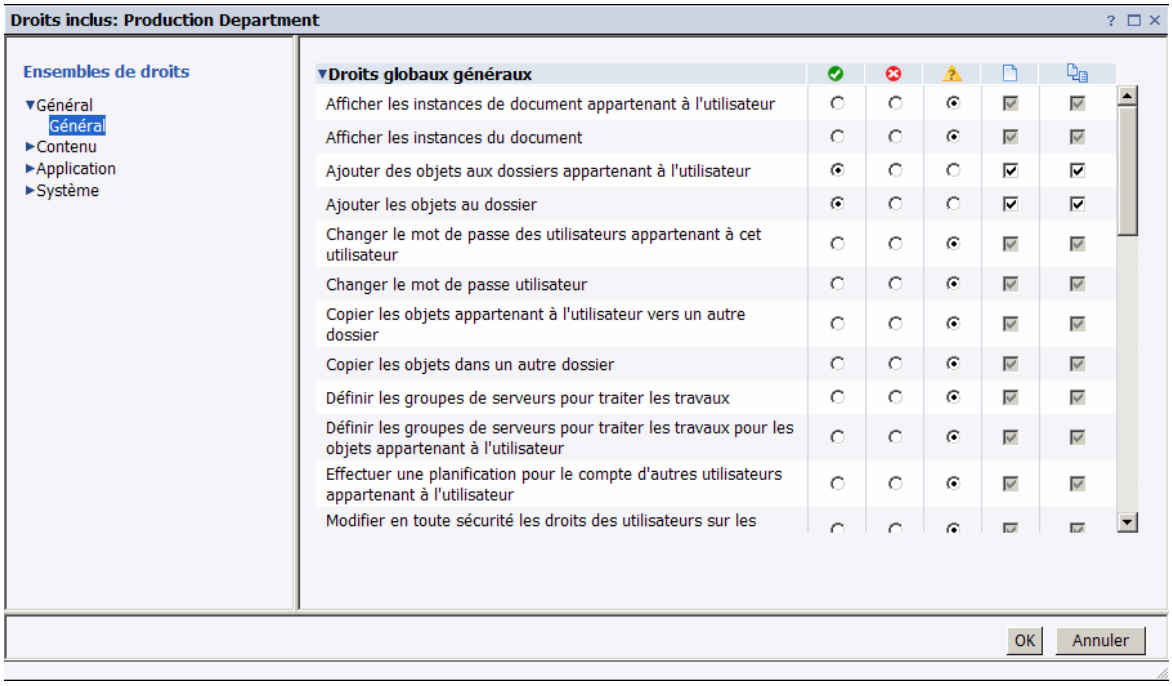
   > ⓘ Remarque
   >
   > Vous ne pouvez pas supprimer de niveaux d'accès prédéfinis.

   Une boîte de dialogue contenant des informations sur les objets auxquels ce niveau d'accès s'applique s'affiche. Si vous ne souhaitez pas supprimer ce niveau d'accès, cliquez sur *Annuler* pour fermer la boîte de dialogue.
3. Cliquez sur *Supprimer*.
   Le niveau d'accès est supprimé et vous revenez à la zone *Niveaux d'accès*.

7.3.6 Pour modifier les droits d'un niveau d'accès

Pour définir les droits d'un niveau d'accès, vous devez d'abord définir les droits globaux généraux qui s'appliquent à tous les objets quels que soient leur type, puis spécifier dans quels cas remplacer les paramètres généraux en fonction du type spécifique de l'objet.

1. Dans la zone *Niveaux d'accès*, dans le volet *Détails*, sélectionnez le niveau d'accès pour lequel vous souhaitez modifier les droits d'accès.
2. Cliquez sur *Actions* > *Droits inclus*.
   La boîte de dialogue *Droits inclus* apparaît et affiche la liste des droits effectifs.
3. Cliquez sur *Ajouter/Supprimer des droits*.



La boîte de dialogue *Droits inclus* affiche les ensembles de droits du niveau d'accès figurant dans la liste de navigation. La section *Droits globaux généraux* est développée par défaut.

4. Définissez les droits globaux généraux.

   Chaque droit peut avoir le statut *Accordé*, *Refusé* ou *Non spécifié*. Vous pouvez également spécifier si ce droit doit être appliqué à l'objet uniquement, à ses sous-objets uniquement, ou aux deux.

5. Pour définir des droits en fonction du type pour le niveau d'accès, cliquez sur l'ensemble de droits dans la liste de navigation, puis cliquez sur le sous-ensemble qui s'applique au type d'objet dont vous voulez définir les droits.

6. Une fois l'opération terminée, cliquez sur *OK*.
   Vous revenez alors à la liste des droits effectifs.

7.3.7 Suivi de la relation entre niveaux d'accès et objets

Avant de modifier ou de supprimer un niveau d'accès, il est important de confirmer que toute modification apportée au niveau d'accès n'affectera pas de façon négative les objets de la CMC. Pour ce faire, exécutez une requête de relation sur le niveau d'accès.

Les requêtes de relation s'avèrent utiles pour la gestion des droits d'accès, étant donné qu'elles vous permettent de voir les objets affectés par un niveau d'accès depuis un emplacement pratique. Imaginez une situation dans laquelle une société restructure son organisation et fusionne deux services, le service A et le service B, dans un service C. L'administrateur décide de supprimer les niveaux d'accès pour les services A et B car ces services n'existent plus. L'administrateur exécute des requêtes de relation pour les deux niveaux d'accès avant de les supprimer. Dans la zone *Résultats de requête*, l'administrateur peut voir les objets qui seront affectés si l'administrateur supprime les niveaux d'accès. Le volet *Détails* indique également à l'administrateur l'emplacement des objets dans la CMC si les droits appliqués à ces objets doivent être modifiés avant que les niveaux d'accès ne soient supprimés.

> **Remarque**
>
> Pour visualiser la liste des objets affectés, vous devez posséder les droits *Visualiser* sur ces objets.

> **Remarque**
>
> Les résultats d'une requête de relation pour un niveau d'accès renvoient uniquement les objets pour lesquels le niveau d'accès est explicitement affecté. Si un objet utilise un niveau d'accès en raison de règles d'héritage, il ne figure pas dans les résultats de la requête.

7.3.8 Gestion des niveaux d'accès sur différents sites

Les niveaux d'accès sont l'un des objets que vous pouvez répliquer depuis un site d'origine vers des sites de destination. Vous pouvez choisir de répliquer des niveaux d'accès s'ils apparaissent dans la liste de contrôle d'accès d'un objet de réplication. Par exemple, si un utilisateur ou un groupe principal reçoit un niveau d'accès A sur un rapport Crystal et que ce rapport est répliqué sur d'autres sites, le niveau d'accès A est également répliqué.

> **Remarque**
>
> S'il existe un niveau d'accès du même nom sur le site de destination, la réplication du niveau d'accès échoue. L'administrateur du site de destination ou vous-même devez renommer un des niveaux d'accès avant la réplication.

Après la réplication d'un niveaux d'accès sur différents sites, gardez en mémoire les remarques de cette section relatives à l'administration.

Modification des niveaux d'accès répliqués sur le site d'origine

Si un niveau d'accès répliqué est modifié sur le site d'origine, le niveau d'accès sur le site de destination sera mis à jour lors de la prochaine exécution planifiée de la réplication. Dans les scénarios de réplication bidirectionnelle, si vous modifiez un niveau d'accès répliqué sur le site de destination, le niveau d'accès sur le site d'origine est également modifié.

> **Remarque**
>
> Assurez-vous que les modifications d'un niveau d'accès sur un site n'affectent pas négativement des objets sur d'autres sites. Contactez les administrateurs du site et conseillez-leur d'exécuter des requêtes de relation pour le niveau d'accès répliqué avant que vous n'apportiez des modifications.

Modification des niveaux d'accès répliqués sur le site de destination

> **Remarque**
>
> Cela s'applique à la réplication unidirectionnelle uniquement.

Toute modification apportée aux niveaux d'accès répliqués sur un site de destination n'est pas appliquée sur le site d'origine. Par exemple, un administrateur de site de destination peut accorder le droit de planifier les rapports Crystal appartenant au niveau d'accès répliqué même si ce droit a été refusé sur le site d'origine. Par conséquent, même si les noms des niveaux d'accès et les noms des objets répliqués sont identiques, les droits effectifs dont les utilisateurs ou groupes principaux disposent sur les objets peuvent différer d'un site de destination à l'autre.

Si le niveau d'accès répliqué diffère entre les sites d'origine et de destination, la différence de droits effectifs sera détectée lors de la prochaine exécution planifiée d'un travail de réplication. Vous pouvez forcer le niveau d'accès du site d'origine à remplacer le niveau d'accès du site de destination ou permettre la conservation du niveau d'accès du site de destination. Toutefois, si vous ne forcez pas le niveau d'accès du site d'origine à remplacer le niveau d'accès du site de destination, tous les objets en attente de réplication utilisant ce niveau d'accès ne pourront pas être répliqués.

Pour empêcher les utilisateurs de modifier les niveaux d'accès répliqués sur le site de destination, vous pouvez ajouter les utilisateurs du site de destination au niveau d'accès en tant qu'utilisateurs principaux et leur accorder uniquement le droit *Visualiser*. Ainsi, les utilisateurs du site de destination peuvent visualiser le niveau d'accès, mais ne sont pas en mesure de modifier la configuration des droits ou de l'affecter à d'autres utilisateurs.

Informations associées

Fédération [page 980]
Suivi de la relation entre niveaux d'accès et objets [page 148]

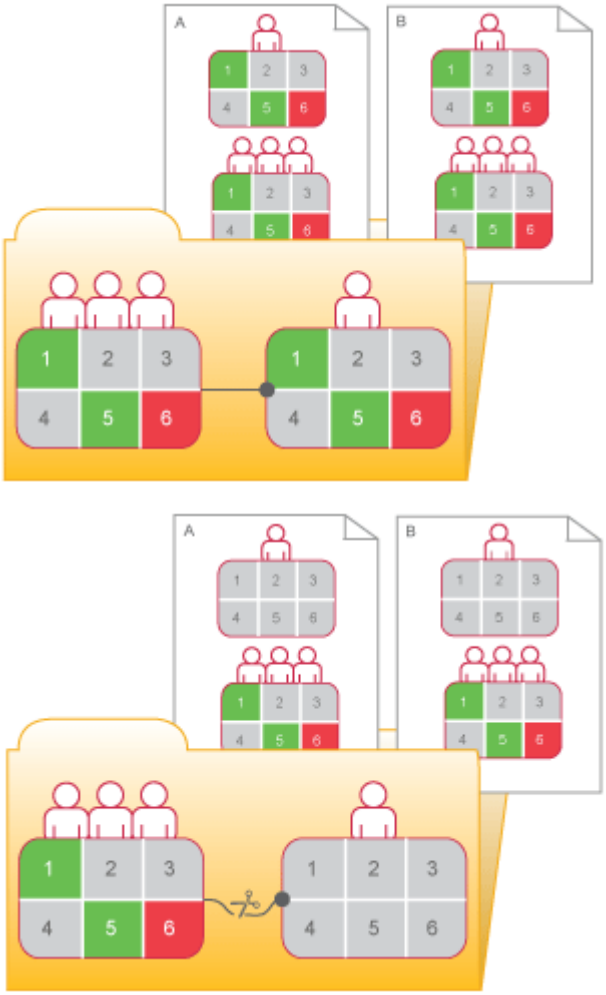
7.4 Rupture de l'héritage

L'héritage permet de gérer les paramètres de sécurité sans définir de droits pour chaque objet. Cependant, dans certains cas, vous ne voudrez peut-être pas que les droits soient hérités. Par exemple, vous souhaiterez peut-être personnaliser les droits pour chaque objet. Vous pouvez désactiver l'héritage pour un utilisateur ou groupe principal dans une liste de contrôle d'accès d'un objet. Dans ce cas, vous pouvez choisir de désactiver l'héritage du groupe, l'héritage du dossier, ou les deux.

> **Remarque**
>
> Lorsque l'héritage est rompu, il l'est pour tous les droits. Il n'est pas possible de désactiver l'héritage pour certains droits uniquement et pas pour d'autres.

Dans le diagramme « Rupture de l'héritage », l'héritage de groupe et l'héritage de dossier sont tous deux activés à l'origine. L'utilisateur rouge hérite des droits 1 et 5 accordés, des droits 2, 3 et 4 non spécifiés et du

droit 6 explicitement refusé. Ces droits, définis au niveau du dossier pour le groupe, signifient que l'utilisateur rouge, ainsi que chaque autre membre du groupe, dispose de ces droits sur les objets du dossier A et B. Si l'héritage est rompu au niveau du dossier, l'ensemble de droits dont l'utilisateur rouge dispose sur les objets de ce dossier est annulé jusqu'à ce qu'un administrateur lui affecte de nouveaux droits.



Rupture de l'héritage

7.4.1 Désactiver l'héritage

Cette procédure vous permet de désactiver l'héritage de groupe ou de dossier, ou les deux, pour un utilisateur ou un groupe principal sur la liste de contrôle d'accès d'un objet.

1. Sélectionnez l'objet pour lequel vous souhaitez désactiver l'héritage.
2. Cliquez sur *Gérer* > *Sécurité de l'utilisateur*.
   La boîte de dialogue *Sécurité de l'utilisateur* s'affiche.
3. Sélectionnez l'utilisateur ou le groupe principal pour lequel vous souhaitez désactiver l'héritage, puis cliquez sur *Affecter la sécurité*.
   La boîte de dialogue *Affecter la sécurité* s'affiche.
4. Configurez vos paramètres d'héritage.

- Si vous souhaitez désactiver l'héritage de groupe (droits dont l'utilisateur ou le groupe principal hérite de son appartenance au groupe), désactivez la case à cocher *Hériter du groupe parent*.
- Si vous souhaitez désactiver l'héritage de dossier (paramètres de droits dont l'objet hérite du dossier), désactivez la case à cocher *Hériter du dossier parent*.

5. Cliquez sur *OK*.

7.5 Utilisation des droits pour déléguer l'administration

Les droits vous permettent non seulement de contrôler l'accès aux objets et aux paramètres, mais également de répartir les tâches administratives entre les divers groupes fonctionnels de votre organisation. Par exemple, vous pouvez souhaiter que les personnes de différents services gèrent leurs propres utilisateurs et groupes. Vous pouvez également être dans la situation où un administrateur assure la gestion de haut niveau de la plateforme de BI mais où vous souhaitez que la totalité de la gestion des serveurs soit assurée par le personnel du service informatique.

En supposant que votre structure de groupe et votre structure de dossier s'alignent sur votre structure de sécurité de l'administration déléguée, vous devez accorder à votre administrateur délégué des droits sur l'intégralité des groupes d'utilisateurs, mais vous devez lui accorder des droits inférieurs aux droits de contrôle total sur les utilisateurs qu'il contrôle. Par exemple, vous ne voudrez peut-être pas que l'administrateur délégué modifie les attributs des utilisateurs ou qu'il les réaffecte à des groupes différents.

> **Remarque**
>
> Les migrations d'objet sont mieux exécutées par des membres du groupe d'administrateurs, en particulier du groupe d'utilisateurs Administrateur. Pour migrer un objet, il se peut qu'un grand nombre d'objets liés doivent également être migrés. Dans le cas d'un compte administrateur délégué, il ne sera peut-être pas possible d'obtenir les droits de sécurité requis pour l'ensemble des objets.

Le tableau « Droits des administrateurs délégués » récapitule les droits requis pour que les administrateurs délégués effectuent les actions courantes.

Droits des administrateurs délégués

Action de l'administrateur délégué	Droits requis par l'administrateur délégué
Créer des utilisateurs	Droit *Ajouter* sur le dossier *Utilisateurs* de niveau supérieur
Créer des groupes	Droit *Ajouter* sur le dossier *Groupes d'utilisateurs* de niveau supérieur
Supprimer les groupes contrôlés, ainsi que les utilisateurs individuels appartenant à ces groupes	Droit *Supprimer* sur les groupes concernés
Supprimer uniquement les utilisateurs créés par l'administrateur délégué	Droit *Supprimer par le propriétaire* sur le dossier *Utilisateurs* de niveau supérieur
Supprimer uniquement les utilisateurs et les groupes créés par l'administrateur délégué	Droit *Supprimer par le propriétaire* sur le dossier *Groupes d'utilisateurs* de niveau supérieur

Action de l'administrateur délégué	Droits requis par l'administrateur délégué
Manipuler uniquement les utilisateurs créés par l'administrateur délégué (y compris l'ajout de ces utilisateurs à ces groupes)	Droits *Modifier par le propriétaire* et *Modifier en toute sécurité les droits par le propriétaire* sur le dossier *Utilisateurs* de niveau supérieur
Manipuler uniquement les groupes créés par l'administrateur délégué (y compris l'ajout de ces utilisateurs à ces groupes)	Droits *Modifier par le propriétaire* et *Modifier en toute sécurité les droits par le propriétaire* sur le dossier de niveau supérieur *Groupes d'utilisateurs*
Modifier les mots de passe des utilisateurs dans leurs groupes contrôlés	Droit *Modifier le mot de passe* sur les groupes concernés
Modifier les mots de passe des utilisateurs ou groupes principaux créés par l'administrateur délégué uniquement	Droit *Modifier le mot de passe par le propriétaire* sur le dossier *Utilisateurs* de niveau supérieur ou sur les groupes concernés **Remarque** La définition du droit *Modifier le mot de passe par le propriétaire* sur un groupe ne prend effet sur un utilisateur que lorsque vous ajoutez l'utilisateur au groupe concerné.
Modifier les noms d'utilisateur, les descriptions et les autres attributs, et réaffecter les utilisateurs à d'autres groupes	Droit *Modifier* sur les groupes concernés
Modifier les noms d'utilisateur, les descriptions et les autres attributs, et réaffecter les utilisateurs à d'autres groupes, mais uniquement pour les utilisateurs créés par l'administrateur délégué	Droit *Modifier le mot de passe par le propriétaire* sur le dossier *Utilisateurs* de niveau supérieur ou sur les groupes concernés **Remarque** La définition du droit *Modifier par le propriétaire* sur les groupes concernés ne prend effet sur un utilisateur que lorsque vous ajoutez l'utilisateur au groupe concerné.

7.5.1 Choisir entre les options « *Modifier les droits des utilisateurs sur les objets* »

Lorsque vous configurez l'administration déléguée, accordez à votre administrateur délégué des droits sur les utilisateurs ou groupes principaux qu'il va contrôler. Vous souhaiterez peut-être lui accorder tous les droits (*Contrôle total*) ; cependant, il est conseillé d'utiliser les paramètres Droits avancés pour refuser le droit *Modifier les droits* et accorder à la place à votre administrateur délégué le droit *Modifier en toute sécurité les droits*. Vous pouvez également accorder à votre administrateur le droit *Modifier en toute sécurité les règles d'héritage des droits* au lieu du droit *Modifier les règles d'héritage des droits*. Les différences entre ces droits sont récapitulées ci-après.

Modifier les droits des utilisateurs sur les objets

Ce droit autorise un utilisateur à modifier tout droit de tout utilisateur sur cet objet. Par exemple, si l'utilisateur A dispose des droits *Visualiser les objets* et *Modifier les droits des utilisateurs sur les objets* sur un objet, il peut modifier les droits pour cet objet afin que lui-même ou tout autre utilisateur détienne le contrôle total de cet objet.

Modifier en toute sécurité les droits des utilisateurs sur les objets

Ce droit permet à un utilisateur d'accorder, de refuser ou d'annuler uniquement les droits qui lui sont déjà accordés. Par exemple, si l'utilisateur A dispose des droits *Visualiser* et *Modifier en toute sécurité les droits des utilisateurs sur les objets*, il ne peut pas s'octroyer de droits supplémentaires et peut uniquement accorder ou refuser aux autres utilisateurs ces deux droits (*Visualiser* et *Modifier en toute sécurité les droits des utilisateurs sur les objets*). De plus, l'utilisateur A peut uniquement modifier les droits des utilisateurs sur les objets pour lesquels il dispose lui-même du droit de *modification des droits en toute sécurité*.

Les conditions dans lesquelles un utilisateur A peut modifier les droits de l'utilisateur B sur l'objet O sont les suivantes :

- L'utilisateur A dispose du droit de *modification des droits en toute sécurité* sur l'objet O.
- Chaque droit ou niveau d'accès que l'utilisateur A modifie pour l'utilisateur B est accordé à l'utilisateur A lui-même.
- L'utilisateur A dispose du droit de *modification des droits en toute sécurité* sur l'utilisateur B.
- Si un niveau d'accès est en cours d'affectation, l'utilisateur A dispose du droit *Affecter un niveau d'accès* sur le niveau d'accès qui est modifié pour l'utilisateur B.

Le périmètre des droits peut limiter davantage les droits effectifs qu'un administrateur délégué peut affecter. Par exemple, un administrateur délégué peut disposer de droits *Modifier en toute sécurité* et *Modifier* sur un dossier, mais le périmètre de ces droits est limité au dossier uniquement et ne s'applique pas à ses sous-objets. En réalité, l'administrateur délégué peut accorder uniquement le droit *Modifier* sur le dossier (mais non sur ses sous-objets) et seulement avec un périmètre « Appliquer à l'objet ». Si l'administrateur délégué dispose du droit *Modifier* sur un dossier avec un périmètre « Appliquer au sous-objet » uniquement, il peut accorder à d'autres utilisateurs ou groupes principaux le droit *Modifier* avec les deux périmètres sur les sous-objets du dossier, mais sur le dossier lui-même, il ne peut accorder que le droit *Modifier* avec un périmètre « Appliquer au sous-objet ».

En outre, la modification des droits sur les groupes par l'administrateur délégué sera limitée pour les autres utilisateurs ou groupes principaux auxquels aucun droit *Modifier en toute sécurité* n'est appliqué. Cela est utile, par exemple, lorsque deux administrateurs délégués sont responsables de l'affectation des droits à différents groupes d'utilisateurs pour le même dossier, mais que vous ne voulez pas que l'un d'eux puisse refuser l'accès aux groupes contrôlés par l'autre administrateur délégué. Le droit *Modifier en toute sécurité les droits* garantit cela, étant donné que les administrateurs délégués n'auront généralement pas le droit *Modifier en toute sécurité les droits* l'un sur l'autre.

Modifier en toute sécurité les règles d'héritage des droits

Ce droit permet à un administrateur délégué de modifier les règles d'héritage d'autres utilisateurs ou groupes principaux sur les objets auxquels il peut accéder. Pour pouvoir modifier les règles d'héritage d'autres utilisateurs ou groupes principaux, un administrateur délégué doit disposer de ce droit sur l'objet et sur les comptes utilisateur des utilisateurs ou groupes principaux.

7.5.2 Droits de propriétaire

Les droits de propriétaire sont les droits qui s'appliquent uniquement au propriétaire de l'objet pour lequel les droits sont vérifiés. Sur la plateforme de BI, le propriétaire d'un objet est l'utilisateur ou le groupe principal qui a créé l'objet. Si cet utilisateur ou groupe principal est supprimé du système, la propriété de l'objet revient à l'administrateur.

Les droits de propriétaire permettent de gérer la sécurité liée à la propriété. Par exemple, vous souhaiterez peut-être créer une hiérarchie de dossiers ou un dossier dans lequel divers utilisateurs peuvent créer et visualiser des documents, mais uniquement modifier ou supprimer leurs propres documents. En outre, les droits de propriétaire sont utiles pour permettre aux utilisateurs de manipuler les instances de rapports qu'ils créent, mais pas les instances des autres. Dans le cas du niveau d'accès de planification, cela permet aux utilisateurs de modifier, supprimer, suspendre et replanifier uniquement leurs propres instances.

Les droits de propriétaire fonctionnent de la même manière que les droits réguliers correspondants. Toutefois, les droits de propriétaire ne sont appliqués que lorsque l'utilisateur ou groupe d'utilisateurs principal dispose des droits de propriétaire mais que les droits réguliers lui sont refusés ou ne sont pas spécifiés.

7.6 Récapitulatif des recommandations concernant l'administration des droits

Tenez compte des remarques suivantes relatives à l'administration des droits :

- Utilisez des niveaux d'accès partout où c'est possible. Ces ensembles de droits prédéfinis simplifient l'administration en regroupant les droits liés aux besoins courants des utilisateurs.
- Définissez des droits et des niveaux d'accès sur les dossiers de niveau supérieur. L'activation de l'héritage permet à ces droits d'être transmis à tout le système avec un minimum d'interventions administratives.
- Evitez de rompre l'héritage dans la mesure du possible. Vous pouvez ainsi réduire le temps nécessaire pour sécuriser le contenu que vous avez ajouté à la plateforme de BI.
- Définissez des droits appropriés pour les utilisateurs et les groupes au niveau du dossier, puis publiez les objets dans ce dossier. Par défaut, si des utilisateurs ou des groupes bénéficient de droits sur un dossier et que vous publiez un objet dans ce dossier, ils hériteront des mêmes droits sur cet objet.
- Organisez les utilisateurs en groupes d'utilisateurs, affectez des droits et des niveaux d'accès à tout le groupe, puis affectez des droits et des niveaux d'accès à des membres spécifiques si nécessaire.
- Créez des comptes Administrateur distincts pour chaque administrateur du système, puis ajoutez-les au groupe Administrateurs afin d'améliorer la responsabilité des modifications apportées au système.

- Par défaut, le groupe Tout le monde dispose de droits très limités sur les dossiers de niveau supérieur de la plateforme de BI. Après l'installation, il est recommandé de vérifier les droits des membres du groupe Tout le monde et d'accorder les droits de sécurité en fonction.

8 Sécurisation de la plateforme de BI

8.1 Présentation de la sécurité

Cette section décrit les différentes manières dont la plateforme de BI aborde les questions de sécurité de l'entreprise, fournissant ainsi aux administrateurs et aux architectes système des réponses aux questions qu'ils se posent le plus souvent à ce sujet.

L'architecture de la plateforme de BI permet de traiter les nombreuses préoccupations auxquelles se trouvent aujourd'hui confrontées les entreprises et les organisations en termes de sécurité. La version actuelle prend en charge des fonctionnalités telles que la sécurité distribuée, la connexion unique, la sécurité d'accès aux ressources, les droits d'accès aux objets granulaires et les authentifications tierces afin de se prémunir contre les accès non autorisés.

Sachant que la plateforme de BI offre la structure adaptée à un nombre croissant de composants de la famille Enterprise des produits SAP BusinessObjects, cette section expose en détail les fonctions de sécurité et leur fonctionnalité associée pour montrer comment la structure même renforce et garantit la sécurité. Ce chapitre ne fournit pas de détails de procédure explicites, mais se focalise plutôt sur des informations conceptuelles et fournit des liens vers des procédures clé.

Après une brève introduction aux concepts de sécurité du système, des renseignements sont fournis pour les rubriques suivantes :

- Utilisation du cryptage et des modes de sécurité du traitement des données pour protéger les données.
- Configuration SSL (Secure Sockets Layer) pour les déploiements de la plateforme de Business Intelligence.
- Instructions de configuration et de gestion des pare-feu pour la plateforme de BI.
- Configuration des serveurs proxy inverses

8.2 Utilisation sécurisée des objets de programme

Si un utilisateur dispose des droits de planification sur les objets programme, alors l'utilisateur a le droit de l'exécuter.

Pour les programmes Java, les utilisateurs peuvent effectuer les opérations suivantes :

- Les utilisateurs peuvent indiquer la classe principale. L'auteur du programme doit s'assurer qu'aucune classe principale secondaire/test ne reste involontairement dans le programme.
- Les utilisateurs peuvent indiquer le chemin d'accès à la classe. Ils ne devraient pas avoir le droit de télécharger le fichier `jar` sur le système. Il peut être utilisé pour exécuter un code spécialement conçu.

Recommandations générales pour sécuriser les objets programme

- Ne fournissez à l'utilisateur aucune information d'identification de connexion au serveur.
- Accordez un minimum de droits au compte utilisateur qui exécute le programme sur le serveur. Interdisez en particulier l'accès au chemin d'installation de la plateforme SAP BusinessObjects Business Intelligence.
- Il est recommandé de sélectionner l'option *Échec du job* dans *Applications* > *Central Management Console* > *Droits sur les objets du programme*.
- Il est recommandé d'utiliser des dossiers pour le contrôle d'accès. Les objets programme avec des niveaux de sécurité différents doivent être placés dans différents dossiers.

8.3 Planification de récupération d'urgence

Certaines étapes doivent être suivies pour protéger la détention de la plateforme de BI par votre entreprise et assurer une continuité maximale du fonctionnement des lignes d'activité dans le cas d'une urgence. Cette section fournit des instructions pour ébaucher un plan de récupération d'urgence pour votre entreprise. Vous pouvez également consulter cette Note SAP pour plus d'informations.

Instructions générales

- Effectuez des sauvegardes système régulières et envoyez des copies de certains supports de sauvegarde hors site si besoin.
- Stockez de manière sûre tous les supports logiciels.
- Stockez de manière sûre toute la documentation de licence.

Instructions spécifiques

Il existe trois ressources système requérant une attention particulière en termes de planification de récupération d'urgence :

- Contenu des serveurs de référentiels de fichiers : cela comprend le contenu propriétaire tel que les rapports. Vous devez sauvegarder régulièrement ce contenu ; en cas d'accident, il n'existe aucun moyen de régénérer un tel contenu sans avoir mis en place un processus de sauvegarde régulière.
- La base de données système utilisée par le CMS : cette ressource contient toutes les métadonnées essentielles à votre déploiement, telles que les informations utilisateur, les rapports et autres informations sensibles propres à votre entreprise.
- Le fichier de clé des informations de base de données (fichier .dbinfo) : cette ressource contient la clé maître de la base de données système. Si, pour une raison quelconque, cette clé n'est pas disponible, vous ne serez pas en mesure d'accéder à la base de données système. Il est vivement recommandé de stocker le mot de passe pour cette ressource dans un emplacement sûr et connu après le déploiement

de la plateforme de BI. Sans le mot de passe, vous ne serez pas en mesure de régénérer le fichier et vous perdrez par conséquent l'accès à la base de données système.

8.4 Recommandations générales pour la sécurité de votre déploiement

Les instructions suivantes concernent la sécurisation de vos déploiements de la plateforme de BI.

- Utilisez les pare-feu pour protéger la communication entre le CMS et d'autres composants du système. Si possible, masquez toujours votre CMS derrière le pare-feu. Tout au moins, assurez-vous que la base de données système est sécurisée derrière le pare-feu.
- Ajoutez un cryptage supplémentaire aux File Repository Servers. Une fois que fonctionne le système, le contenu propriétaire est stocké sur ces serveurs. Ajoutez un cryptage supplémentaire par le biais du système d'exploitation ou utilisez un outil tiers.
- Déployez les serveurs proxy inverses devant les serveurs d'applications Web afin de les masquer derrière une adresse IP unique. Cette configuration permet d'acheminer tout le trafic Internet adressé aux serveurs d'applications Web privés via le serveur proxy inverse, masquant ainsi les adresses IP privées.
- Appliquez de manière stricte les stratégies de l'entreprise en matière de mots de passe . Assurez-vous que les mots de passe des utilisateurs sont changés régulièrement.
- Si vous avez choisi d'installer la base de données système et le serveur d'applications Web fournis avec la plateforme de BI, consultez la documentation correspondante et assurez-vous que ces composants sont déployés avec les configurations de sécurité adéquates.
- Utilisez le protocole SSL (Secure Sockets Layer) pour toutes les communications réseau établies entre clients et serveurs au sein de votre déploiement.
- Assurez-vous que le répertoire et les sous-répertoires d'installation de la plateforme sont sécurisés. Des données temporaires de haute importance peuvent être stockées dans ces répertoires durant le fonctionnement du système.
- L'accès à la CMC (Central Management Console) doit être limité à l'accès local uniquement. Pour en savoir plus sur les options de déploiement pour la CMC, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.
- Par défaut, les messages d'erreur Web Intelligence incluent des informations sur le schéma de la base de données. Pour afficher les messages d'erreur sans ces informations, exécutez les étapes suivantes :
  1. Ouvrez le fichier de configuration `WebIContainer_ServerDescriptor.xml` pour le modifier. Par défaut, il se trouve à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64config`.
  2. Changez la valeur de ce paramètre en False : `WebiParamDetailedDbErrorsEnabled = False`.

> ⚠ Attention
>
> Les espaces réservés non destinés à la modification ne doivent en aucun cas être modifiés. L'administrateur système doit s'assurer que seule la personne appropriée du groupe d'administrateurs (qui assure la gestion des nœuds) dispose de droits de modification sur le nœud. Tous les autres utilisateurs, y compris les autres membres du groupe d'administrateurs, doivent disposer de droits limités à l'affichage/la gestion des objets du nœud. Les droits de sécurité appropriés doivent donc s'appliquer. Si l'une des valeurs d'espace réservé est accidentellement corrompue et que le CMS n'apparaît pas, reportez-vous à la note SAP 3269127.

> **Remarque**
>
> Reportez-vous à l'article 3278916 de la base de connaissances SAP pour savoir comment limiter la modification des espaces réservés et ainsi éviter toute interférence malveillante avec l'infrastructure BI.

Informations associées

Configuration du protocole SSL [page 192]
Restrictions relatives aux mots de passe [page 166]
Configuration de la sécurité pour les serveurs tiers fournis [page 160]

8.5 Configuration de la sécurité pour les serveurs tiers fournis

Si vous avez choisi d'installer des composants de serveur tiers qui sont fournis avec la plateforme de BI, il est recommandé de consulter les sections de sécurité de la documentation officielle pour SAP SQL Anywhere et Apache Tomcat .

8.6 Relation de confiance active

Dans un environnement en réseau, une relation de confiance entre deux domaines est généralement une connexion qui permet à un domaine de reconnaître les utilisateurs ayant été authentifiés par l'autre domaine. Tout en garantissant la sécurité, la relation de confiance permet aux utilisateurs d'accéder aux ressources dans plusieurs domaines sans avoir à fournir leurs références de connexion à chaque fois.

Dans l'environnement de la plateforme de BI, la relation de confiance active fonctionne de manière similaire pour fournir à chaque utilisateur un accès ininterrompu aux ressources de la totalité du système. Une fois que l'utilisateur a été authentifié et qu'il s'est vu accorder une session active, tous les autres composants de la plateforme de BI peuvent traiter les requêtes et les actions de l'utilisateur sans demander de références de connexion. En tant que telle, la relation de confiance fournit la base de la sécurité distribuée de la plateforme de BI.

8.6.1 Jetons de connexion

Un jeton de connexion est une chaîne codée qui définit ses propres attributs d'utilisation et contient les informations de session d'un utilisateur. Les attributs d'utilisation d'un jeton de connexion sont spécifiés lors de la génération de ce dernier. Ces attributs permettent de placer des restrictions sur le jeton de connexion afin

de réduire le risque d'utilisation du jeton par des utilisateurs malveillants. Les attributs d'utilisation actuels du jeton de connexion sont :

- *Le nombre de minutes*
  Cet attribut restreint la durée de vie du jeton de connexion.
- *Le nombre de connexions*
  Cet attribut restreint le nombre d'utilisations du jeton de connexion pour se connecter à la plateforme de BI.

Les deux attributs empêchent les utilisateurs malveillants d'accéder, sans autorisation, à la plateforme de BI avec des jetons de connexion récupérés auprès d'utilisateurs légitimes.

> **Remarque**
>
> L'enregistrement d'un jeton de connexion dans un cookie peut représenter un risque potentiel pour la sécurité si le réseau entre le navigateur et le serveur Web ou d'applications n'est pas sécurisé ; par exemple, si la connexion est effectuée via un réseau public et n'utilise pas SSL ou l'authentification sécurisée. Il est conseillé d'utiliser SSL (Secure Sockets Layer) pour réduire les risques de sécurité entre le navigateur et le serveur Web ou d'applications.

Lorsque le cookie de connexion a été désactivé et que le serveur Web ou le navigateur Web expire, l'écran de connexion s'affiche. Lorsque le cookie est activé et que le serveur ou le navigateur expire, l'utilisateur est reconnecté automatiquement au système. Toutefois, les informations d'état étant liées à la session Web, l'état de l'utilisateur est perdu. Par exemple, si l'utilisateur a développé une arborescence de navigation et sélectionné un élément particulier, l'arborescence est réinitialisée.

Sur la plateforme de BI, les jetons de connexion sont activés par défaut sur le client Web, mais vous pouvez les désactiver pour la zone de lancement BI. Lorsque vous désactivez les jetons de connexion dans le client, la session utilisateur est limitée par le délai d'expiration du serveur Web ou du navigateur Web. Lorsque cette session expire, l'utilisateur doit de nouveau se connecter à la plateforme de BI.

8.6.2 Système de ticket pour la sécurité distribuée

Les systèmes d'entreprise dédiés au service d'un grand nombre d'utilisateurs nécessitent généralement une certaine forme de sécurité distribuée. Un système d'entreprise peut nécessiter une sécurité distribuée pour prendre en charge des fonctions comme le transfert de confiance (la possibilité d'autoriser un autre composant à agir au nom de l'utilisateur).

La plateforme de BI aborde la question de la sécurité distribuée en mettant en œuvre un système de ticket (rappelant le système de ticket Kerberos). Le CMS accorde des tickets pour autoriser les composants à exécuter des actions au nom d'un utilisateur particulier. Sur la plateforme de BI, le ticket est appelé jeton de connexion.

Ce jeton de connexion est le jeton le plus couramment utilisé sur le Web. Lors de la première authentification des utilisateurs par la plateforme de BI, le CMS leur fournit des jetons de connexion. Le navigateur Web de l'utilisateur met en cache ce jeton de connexion. Lorsque l'utilisateur effectue une nouvelle requête, d'autres composants de la plateforme de BI peuvent lire le jeton de connexion à partir du navigateur Web de l'utilisateur.

8.7 Sessions et suivi de session

En général, une session est une connexion de type client-serveur qui permet à deux ordinateurs d'échanger des informations. Le statut d'une session est constitué d'un ensemble de données qui décrivent les attributs de la session, sa configuration ou son contenu. Lorsque vous établissez une connexion client-serveur sur le Web, la nature du protocole HTTP limite la durée de chaque session à une seule page d'informations ; par conséquent, votre navigateur Web conserve le statut de chaque session en mémoire uniquement pendant la durée de l'affichage de cette page Web unique. Dès que vous passez d'une page Web à une autre, le statut de la première session est remplacé par le statut de la session suivante. Par conséquent, les sites et les applications Web doivent d'une manière ou d'une autre stocker le statut d'une session s'ils doivent réutiliser leurs informations dans une autre session.

La plateforme de BI utilise deux méthodes courantes pour stocker le statut d'une session :

- Cookies : Un cookie est un petit fichier texte qui stocke le statut d'une session côté client : le navigateur Web de l'utilisateur met en cache le cookie pour une utilisation ultérieure. Le jeton de connexion de la plateforme de BI illustre cette méthode.
- Variables de session : Une variable de session est un fragment de mémoire qui stocke le statut d'une session côté serveur. Lorsque la plateforme de BI accorde à l'utilisateur une identité active sur le système, les informations telles que le type d'authentification de l'utilisateur sont stockées dans une variable de session. Tant que la session est maintenue, le système ne doit ni inviter l'utilisateur à saisir les informations une deuxième fois, ni répéter une tâche nécessaire à l'exécution de la requête suivante.
  Dans les déploiements Java, la session permet de prendre en charge les requêtes .jsp ; dans les déploiements .NET, la session permet de prendre en charge les requêtes .aspx.

> **Remarque**
>
> L'idéal serait que le système préserve la variable de session tant que l'utilisateur reste actif sur le système. En outre, pour garantir la sécurité et minimiser l'utilisation des ressources, le système devrait détruire la variable de session dès que l'utilisateur a terminé de travailler sur le système. Mais, étant donné que l'interaction entre un navigateur Web et un serveur Web peut être sans statut, il est parfois difficile de savoir à quel moment les utilisateurs quittent le système, s'ils ne se déconnectent pas de manière explicite. Pour répondre à ce problème, la plateforme de BI met en œuvre le suivi de session.

8.7.1 Suivi de session du CMS

Le CMS implémente un algorithme de suivi simple. Lorsqu'un utilisateur se connecte, il reçoit une session du CMS, que le CMS conserve jusqu'à ce qu'il se déconnecte, ou que la variable de session du serveur d'applications Web soit publiée.

La session du serveur d'applications Web est conçue pour aviser le CMS périodiquement qu'elle est toujours active, de manière à conserver la session du CMS tant que la session du serveur d'applications Web existe. Si la session du serveur d'applications Web ne parvient pas à communiquer avec le CMS pendant une durée de dix minutes, le CMS détruit la session du CMS. Ceci prend en compte des scénarios dans lesquels les composants côté client s'interrompent de manière irrégulière.

8.7.2 Gestion des sessions

Vous pouvez afficher et mettre fin à des sessions dans la CMC.

Vous pouvez afficher et terminer des sessions d'utilisateur dans la CMC (Central Management Console). Vous pourrez par exemple afficher les utilisateurs qui utilisent plusieurs sessions ou mettre fin à des sessions qui consomment trop de ressources système ou trop anciennes. Vous devrez peut-être également terminer des sessions pour anticiper les temps d'arrêt du système ou les mises à niveau.

8.7.2.1 Affichage de la liste des sessions

Affichez des sessions dans la CMC.

Vous pouvez afficher une liste de sessions dans la CMC (Central Management Console).

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Dans la zone *Gérer*, cliquez sur *Sessions*.

La liste des sessions utilisateur du cluster s'affiche. Vous pouvez cliquer sur les en-têtes de colonne pour trier la liste par nom d'utilisateur, par nombre de sessions ouvertes ou par heures de connexion. Vous pouvez aussi cliquer sur le nom d'utilisateur ou le nombre de sessions ou l'heure de connexion pour afficher les détails relatifs aux sessions d'un utilisateur dans le volet inférieur.

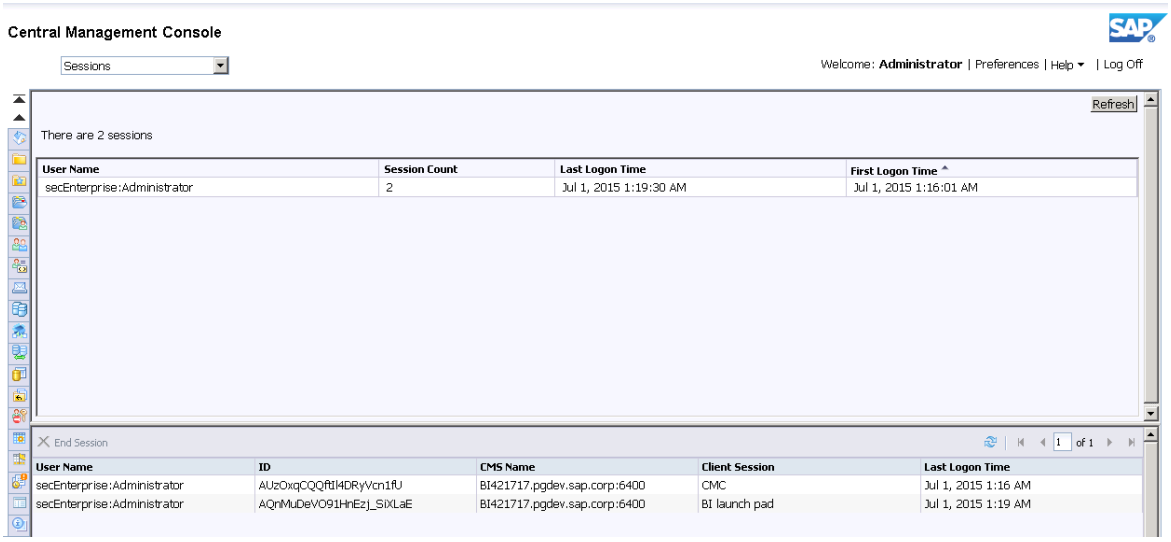
8.7.2.2 Pour mettre fin à des sessions

Terminez des sessions dans la CMC.

Vous pouvez mettre fin à une ou plusieurs sessions.

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Dans la zone *Gérer*, cliquez sur *Sessions*.

   La liste des sessions utilisateur du cluster s'affiche.



3. Cliquez sur un nom d'utilisateur ou un nombre de sessions ou une heure de connexion pour afficher les sessions d'un utilisateur dans le volet inférieur.
4. Cliquez pour sélectionner une seule session, ou utilisez la combinaison de touches `CTRL` + `clic` pour sélectionner plusieurs sessions.
5. Cliquez sur *Terminer la session*.

> **Remarque**
>
> La session Utilisateur est libérée dès que l'utilisateur ferme le navigateur.

> **Remarque**
>
> Pour terminer des sessions, vous devez disposer du droit « Modifier les objets » sur l'objet du CMS.

> **Remarque**
>
> Vous ne pouvez pas mettre fin à votre session d'administrateur actuelle.

8.7.3 Script permettant d'effacer les sessions obsolètes

Script

Un nouveau script permet d'effacer les sessions obsolètes et de libérer les licences inutilisées afin de les rendre disponibles pour les utilisateurs qui attendent de se connecter. Ce script continue à s'exécuter jusqu'à ce qu'il soit fermé manuellement. Il recherche les sessions obsolètes et les interrompt toutes les 10 minutes.

- Pour Windows, vous trouverez un script ici : `<Rép_Install_BI>\SAP BusinessObjects Enterprise XI 4.0\java\lib\StaleSessionCleaner.jar`
- Pour Unix, vous trouverez un script ici : `<Rép_Install_BI>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar`

La syntaxe utilisée pour le script est la suivante :

> **Syntaxe de code**
>
> ```
> java -jar StaleSessionCleaner.jar <username> <password>
> <machine:port><authentication> <logdir>
> ```

8.8 Protection de l'environnement

La protection de l'environnement fait référence à la sécurité de tout l'environnement dans lequel communiquent les composants client et serveur. Même si la popularité d'Internet et des systèmes de type Web ne cesse d'augmenter grâce à leur souplesse d'utilisation et à la gamme de fonctionnalités qu'ils offrent, ils fonctionnent néanmoins dans un environnement difficile à sécuriser. Lors du déploiement de la plateforme

de BI, la protection de l'environnement est divisée en deux zones de communication : du navigateur Web au serveur Web et du serveur Web à la plateforme de BI.

8.8.1 Du navigateur Web au serveur Web

Lors du transfert de données entre le navigateur Web et le serveur Web, un certain degré de sécurité est généralement requis. Les mesures de sécurité qui s'imposent impliquent deux tâches d'ordre général :

- S'assurer que la communication des données est sécurisée ;
- S'assurer que seuls les utilisateurs autorisés récupèrent des informations sur le serveur Web.

> **Remarque**
>
> Ces tâches sont généralement prises en charge par les serveurs Web grâce à divers systèmes de sécurité, qu'il s'agisse du protocole SSL (Secure Sockets Layer) ou d'autres mécanismes similaires. Il est conseillé d'utiliser SSL pour réduire les risques de sécurité entre le navigateur et le serveur Web ou d'applications.

Vous devez sécuriser la communication entre le navigateur Web et le serveur Web indépendamment de la plateforme de BI. Pour plus d'informations sur la sécurisation des connexions client, consultez la documentation de votre serveur Web.

8.8.2 Serveur Web vers la plateforme de BI

Les pare-feu sont communément utilisés pour sécuriser le domaine de communication entre le serveur Web et le reste de l'intranet d'entreprise (y compris la plateforme de BI). La plateforme prend en charge les pare-feu appliquant un filtrage des adresses IP ou une traduction des adresses réseau statiques (NAT). Les environnements pris en charge peuvent impliquer plusieurs pare-feu, serveurs Web ou serveurs d'applications.

8.8.3 Protection contre les tentatives de connexion malveillantes

Même si un système est sécurisé, il existe souvent un emplacement vulnérable à attaquer : l'emplacement à partir duquel les utilisateurs se connectent au système. Il est quasiment impossible de protéger entièrement cet emplacement, car le processus consistant à deviner tout simplement un nom d'utilisateur et un mot de passe valides reste une manière envisageable de "craquer" le système.

La plateforme de BI met en œuvre plusieurs techniques pour réduire la probabilité qu'un utilisateur malveillant parvienne à accéder au système. Les différentes restrictions énumérées ci-dessous s'appliquent uniquement aux comptes Enterprise ; elles ne s'appliquent pas aux comptes que vous avez mappés à une base de données d'utilisateurs externe (LDAP ou Windows AD). Toutefois, et de manière générale, votre système externe vous permettra de placer des restrictions similaires sur les comptes externes.

8.8.4 Restrictions relatives aux mots de passe

Les restrictions relatives au mot de passe incitent les utilisateurs appliquant l'authentification Entreprise par défaut à créer des mots de passe relativement complexes. Vous pouvez activer les options suivantes :

1. Appliquer des mots de passe à casse mixte
   Cette option permet de s'assurer que les mots de passe contiennent au moins un caractère en majuscule et un caractère en minuscule. Cette option est cochée par défaut à moins que l'Administrateur ne le modifie.
2. Appliquer les chiffres dans les mots de passe
   Cette option permet de vérifier que les mots de passe comportent au moins un caractère numérique.
3. Appliquer les caractères spéciaux dans les mots de passe
   Cette option permet de vérifier que les mots de passe comportent au moins un caractère spécial.

En exigeant une complexité minimale dans le choix d'un mot de passe, vous réduisez les chances qu'un utilisateur malveillant devine le mot de passe valide d'un autre utilisateur.

8.8.5 Restrictions relatives aux connexions

Les restrictions relatives aux connexions servent principalement à éviter les attaques à l'aide de dictionnaires (méthode par laquelle un utilisateur malveillant obtient un nom d'utilisateur valide et tente de retrouver le mot de passe correspondant en essayant chaque mot du dictionnaire). Grâce à la vitesse du matériel moderne, des programmes nuisibles peuvent deviner des millions de mots de passe à la minute. Pour éviter les attaques à l'aide du dictionnaire, la plateforme de BI dispose d'un mécanisme interne qui impose un délai (0,5 à 1 seconde) entre chaque tentative de connexion. En outre, la plateforme fournit plusieurs options personnalisables permettant de réduire les risques de ce type d'attaque :

- Désactiver le compte après N échecs de connexion
- Réinitialiser le compte dont la connexion a échoué après N minute(s)
- Réactiver le compte après N minute(s)

8.8.6 Restrictions relatives aux utilisateurs

Les restrictions relatives au mot de passe incitent les utilisateurs appliquant l'authentification Entreprise par défaut à créer régulièrement de nouveaux mots de passe. Vous pouvez activer les options suivantes :

- Le mot de passe doit être modifié tous les N jour(s)
- Les N derniers mots de passe ne peuvent être réutilisés
- Le mot de passe peut être modifié après N minute(s)

Ces options sont pratiques à bien des égards. Premièrement, un utilisateur malveillant qui tente une attaque à l'aide d'un dictionnaire devra recommencer chaque fois qu'un mot de passe est modifié. En outre, étant donné que les modifications d'un mot de passe sont basées sur l'heure de la première connexion de chaque utilisateur, l'utilisateur malveillant ne peut pas facilement déterminer à quel moment un mot de passe particulier est modifié. De plus, même si un utilisateur malveillant devine ou obtient de quelque manière que ce soit les références d'un autre d'utilisateur, celles-ci ne seront valides que pour une durée limitée.

8.8.7 Restrictions relatives au compte Guest

La plateforme de BI prend en charge la connexion unique anonyme pour le compte Guest. Par conséquent, lorsque les utilisateurs se connectent à la plateforme de BI sans spécifier de nom d'utilisateur ni de mot de passe, le système les connecte automatiquement sous le compte Guest. Si vous affectez un mot de passe sécurisé à un compte "Guest", ou si vous désactivez entièrement le compte "Guest", vous désactivez par la même occasion ce fonctionnement par défaut.

8.9 Audit des modifications de la configuration de sécurité

Les modifications apportées aux configurations de sécurité par défaut pour les éléments suivants ne seront pas auditées par la plateforme de BI :

- Fichiers de propriétés pour les applications Web (BOE, services Web)
- TrustedPrincipal.conf
- Personnalisation réalisée sur la zone de lancement BI et OpenDocument

En règle générale, les modifications de configuration de sécurité effectuées en dehors de la CMC ne sont pas auditées. Cela s'applique aussi aux modifications effectuées par le biais du Central Configuration Manager (CCM). Les modifications validées par le biais de la CMC peuvent être auditées.

8.10 Extensions de traitement

La plateforme de BI vous permet de renforcer la sécurité de votre environnement de reporting grâce à l'utilisation d'extensions de traitement personnalisées. Une extension de traitement est une bibliothèque de codes chargée dynamiquement qui applique une logique d'entreprise à des requêtes particulières de visualisation ou de planification sur la plateforme de BI avant qu'elles ne soient traitées par le système.

A travers sa prise en charge des extensions de traitement, le SDK d'administration de la plateforme de BI livre essentiellement un "descripteur" qui permet aux développeurs d'intercepter la requête. Les développeurs peuvent ensuite ajouter des formules de sélection à la requête avant que le rapport ne soit traité.

L'exemple standard est représenté par une extension de traitement de rapport qui renforce la sécurité au niveau ligne. Ce type de sécurité restreint l'accès aux données par ligne dans une ou plusieurs tables de base de données. Le développeur écrit une bibliothèque chargée dynamiquement qui intercepte les requêtes de visualisation ou de planification d'un rapport (avant que les requêtes ne soient traitées par un Job Server, un serveur de traitement ou un Report Application Server). Le code du développeur détermine d'abord le propriétaire du traitement, puis il recherche les droits d'accès aux données de l'utilisateur dans un système tiers. Le code génère ensuite et ajoute une formule de sélection d'enregistrements au rapport afin de limiter la quantité de données renvoyées par la base de données. Dans ce cas, l'extension de traitement sert à intégrer une sécurité de niveau ligne personnalisée dans l'environnement de la plateforme de BI.

En activant des extensions de traitement, vous configurez les composants serveur de la plateforme de BI appropriés pour charger dynamiquement vos extensions de traitement au moment de l'exécution. Le SDK contient une API entièrement documentée que les développeurs peuvent utiliser pour écrire des extensions de

traitement. Pour en savoir plus, voir la documentation pour développeur figurant sur la distribution de votre produit.

8.11 Interface d'analyse anti-virus

Vous pouvez valider différents types de fichiers (Adobe Acrobat, Microsoft Excel, Microsoft Word, Microsoft Powerpoint, Lumira, Crystal Reports, Web Intelligence, etc.) dans la plateforme de BI via les applications de la CMC, la zone de lancement BI, les services Web de type REST et le SDK personnalisé. Ces fichiers sont soumis à une vérification de taille (pour s'assurer que la taille de fichier n'est pas nulle) et à une vérification d'autorisation sur le répertoire de destination. Avec l'introduction de l'interface d'analyse anti-virus dans BI 4.2 SP4, les fichiers que vous validez dans la plateforme de BI sont également soumis à une analyse anti-virus pour s'assurer que le contenu de ces fichiers est exempt de virus et d'infection.

Les fichiers sont soumis à une analyse anti-virus lorsque vous effectuez les opérations suivantes :

- Ajouter un fichier
- Enregistrer un document
- Copier un document
- Envoyer un document vers une boîte de réception BI
- Créer une instance de document
- Ou opération quelconque qui valide un nouveau fichier dans les File Repository Servers.

> **Remarque**
>
> Seuls les fichiers récemment validés dans la plateforme de BI dans BI 4.2 SP4 (après activation de l'analyse anti-virus) sont soumis à une analyse anti-virus.

8.11.1 Activation de l'analyse anti-virus

Vous pouvez activer l'analyse anti-virus pour les fichiers validés dans la plateforme de BI du Input File Repository Server et du Output File Repository Server.

Vous avez téléchargé la bibliothèque de l'adaptateur de l'analyse anti-virus (VSA) à partir d'un fournisseur certifié SAP. Pour obtenir une liste de fournisseurs certifiés SAP, consultez http://global.sap.com/community/ebook/2013_09_adpd/enEN/search.html#search=NW-VSI.

> **Remarque**
>
> Si vous avez besoin d'aide pour une nouvelle plateforme ou un nouveau fournisseur, contactez les fournisseurs à ce propos.

Pour activer l'analyse anti-virus dans l'Input File Repository Server, effectuez les étapes suivantes :

1. Connectez-vous à la CMC.
2. Accédez à *Serveurs* > *Liste des serveurs*.

3. Cliquez avec le bouton droit de la souris sur l'Input File Repository Server puis sélectionnez *Propriétés* dans la liste déroulante.

   La fenêtre *Propriétés* s'affiche.
4. Dans la section *Service de stockage des fichiers d'entrée*, cochez la case *Activer l'analyse anti-virus*.
5. Dans le champ *Emplacement du fichier de l'adaptateur de l'analyse anti-virus*, saisissez le chemin absolu d'accès au fichier de bibliothèque de l'adaptateur de l'analyse anti-virus.
6. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> - Par défaut, l'analyse anti-virus est désactivée pour tous les fichiers validés dans la plateforme de BI dans BI 4.2 SP4.
> - Vous pouvez activer l'analyse anti-virus à l'aide de GUI ou CLI. L'argument de ligne de commande que vous devez fournir dans les File Repository Servers pour l'activation de l'analyse anti-virus est `vsaFileLoc`.
> - Vous pouvez suivre les étapes similaires pour activer l'analyse anti-virus dans le Output File Repository Server. Si vous possédez plusieurs Intput File Repository Server et Output File Repository Server, veillez à activer l'analyse anti-virus sur chaque serveur.
> - Vous devez redémarrer les Files Repository Servers après avoir activé l'analyse anti-virus pour que les modifications prennent effet.

8.12 Sécurité des données de la plateforme de BI

Les administrateurs des systèmes de la plateforme de BI gèrent la sécurisation des données sensibles de la façon suivante :

- Un paramètre de sécurité au niveau du cluster qui détermine quelles applications et quels clients ont accès au CMS. Ce paramètre est géré via le Central Configuration Manager.
- Un système de cryptage à deux clés qui contrôle à la fois l'accès au référentiel du CMS et les clés utilisées pour crypter/décrypter les objets du référentiel. L'accès au référentiel du CMS est configuré via le Central Configuration Manager, tandis que la Central Management Console dispose d'une zone de gestion dédiée pour les clés de cryptage.

Ces fonctions permettent aux administrateurs de définir les déploiements de la plateforme de BI à des niveaux de conformité de sécurité des données spécifiques et de gérer les clés de cryptage utilisées pour crypter et décrypter les données du référentiel du CMS.

8.12.1 Modes de sécurité du traitement des données

La plateforme de BI peut fonctionner selon deux modes de sécurité du traitement des données :

- Mode de sécurité du traitement des données par défaut Dans certaines instances, les systèmes exécutés dans ce mode utilisent des clés de cryptage codées en dur et n'appliquent pas de norme spécifique.

Le mode par défaut active la rétrocompatibilité avec les applications et les outils client des versions précédentes de la plateforme de BI.

- Un mode de sécurité des données conçu pour appliquer des directives FIPS (Federal Information Processing Standard), notamment FIPS 140-2. Dans ce mode, des modules de cryptage et des algorithmes compatibles FIPS protègent les données sensibles. Lorsque la plateforme est exécutée en mode compatible FIPS, la totalité des applications et des outils client ne répondant pas aux directives FIPS sont automatiquement désactivés. Les applications et outils client de la plateforme sont conçus pour répondre au standard FIPS 140-2. Les clients et applications plus anciens ne fonctionnent pas lorsque la plateforme de BI est exécutée en mode compatible FIPS.

Le mode de traitement des données est transparent pour les utilisateurs du système. Dans les deux modes de sécurité du traitement des données, les données sensibles sont cryptées et décryptées en arrière-plan par un moteur de cryptage interne.

Nous recommandons d'utiliser le mode compatible FIPS dans les cas suivants :

- Votre déploiement de la plateforme de BI ne sera pas amené à utiliser ou à interagir avec des applications ou outils client hérités de la plateforme de BI.
- Les normes et directives de traitement des données établies par votre organisation interdisent l'utilisation de clés de cryptage codées en dur.
- Votre organisation est tenue de sécuriser ses données sensibles conformément aux réglementations FIPS 140-2.

Le mode de sécurité du traitement des données est défini via le Central Configuration Manager sur les plateformes Windows comme sur les plateformes UNIX. Chaque nœud d'un environnement en cluster doit être défini dans le même mode.

8.12.1.1 Activation du mode compatible FIPS sous Windows

Par défaut, le mode compatible FIPS est activé lorsque la plateforme de BI est installée.

1. Pour lancer le CCM, cliquez sur *Programmes* > *SAP Business Intelligence* > *Plateforme SAP BusinessObjects BI 4* > *Central Configuration Manager*.
2. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Arrêter*.

   > ⚠ Attention
   >
   > Ne passez à l'étape 3 que lorsque le statut du SIA est Arrêté.

3. Cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*.
   La boîte de dialogue *Propriétés* apparaît et affiche l'onglet *Propriétés*.
4. Ajoutez `-fips` dans le champ *Commande* et cliquez sur *Appliquer*.
5. Cliquez sur *OK* pour fermer la boîte de dialogue *Propriétés*.
6. Redémarrez le SIA.

Le SIA fonctionne désormais en mode compatible FIPS.

Vous devez activer le paramètre compatible FIPS sur tous les SIA de votre déploiement de la plateforme de BI.

8.12.1.2 Activation du mode compatible FIPS sous UNIX

Tous les nœuds du déploiement de la plateforme de BI doivent être arrêtés avant de tenter la procédure suivante.

Par défaut, le mode compatible FIPS est désactivé après l'installation de la plateforme de BI. Suivez les instructions ci-dessous pour activer le paramètre compatible FIPS sur tous les nœuds de votre déploiement.

1. Dans le répertoire `<REPINSTALL>/sap_bobj`, ouvrez le fichier `ccm.config` pour le modifier.
2. Ajoutez `-fips` au paramètre de commande de lancement du nœud.

   Le paramètre de commande de lancement du nœud est affiché au format suivant : `<NOMNŒUD>LAUNCH`. Par exemple, pour un nœud nommé « SAP », le paramètre de commande de lancement du nœud est `SAPLAUNCH`.
3. Enregistrez vos modifications et cliquez sur *Quitter*.
4. Redémarrez le nœud.

Le nœud fonctionne désormais en mode compatible FIPS.

Vous devez activer le paramètre compatible FIPS sur tous les nœuds de votre déploiement de la plateforme de BI.

8.12.1.3 Désactivation du mode compatible FIPS sous Windows

Tous les serveurs de votre déploiement de la plateforme de BI doivent être arrêtés avant de tenter la procédure suivante.

Si votre déploiement est exécuté en mode compatible FIPS, procédez comme suit pour désactiver ce paramètre.

1. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Arrêter*.

   > ⚠ Attention
   >
   > Ne passez à l'étape 2 que lorsque le statut du nœud affiche *Arrêté*.
2. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche avec l'onglet*Propriétés* ouvert.
3. Supprimez `-FIPS` du champ *Commande* et cliquez sur *Appliquer*.
4. Cliquez sur *OK* pour fermer la boîte de dialogue *Propriétés*.
5. Redémarrez le SIA.

8.12.2 Comptes Administrateur

La plateforme de BI crée automatiquement un compte administrateur initial. Nous vous recommandons de créer un compte dans le groupe Administrateurs pour chaque personne.

L'utilisateur Administrateur obtient automatiquement l'autorisation *Modifier les droits des utilisateurs sur les objets*. Une fois que vous avez créé le compte de l'administrateur, n'oubliez pas de désactiver le compte administrateur initial.

8.12.3 Droits de connexion

Par défaut, les administrateurs ont accès aux détails de connexion, y compris les mots de passe, si les connexions sont définies avec des identifiants.

Cette section explique comment appliquer le principe du droit d'accès minimal aux connexions si les administrateurs ne sont pas censés accéder aux sources de données.

Restriction du droit "Télécharger la connexion localement"

Le droit *Télécharger la connexion localement* est strictement nécessaire uniquement pour les utilisateurs qui gèrent les connexions (voir Droits de connexion [page 1166]). Il ne doit être accordé qu'à des utilisateurs individuels et non à des groupes. Si un groupe dispose d'un droit, tout utilisateur ajouté au groupe peut avoir accès aux détails de connexion.

Pour sécuriser entièrement les connexions :

1. Accordez le droit *Télécharger la connexion localement* aux utilisateurs qui gèrent les connexions.
2. Refusez le droit *Télécharger la connexion localement* dans le dossier supérieur Connexions pour les groupes d'utilisateurs Administrateurs et Concepteurs d'univers.

Pour empêcher les utilisateurs de s'accorder eux-mêmes le droit, voir la section ci-dessous.

Sécurisation du droit "Modifier les droits des utilisateurs sur les objets"

Le droit par défaut *Modifier les droits des utilisateurs sur les objets* permet aux utilisateurs d'accorder un droit même s'ils n'en disposent pas eux-mêmes. Pour les connexions, il doit être remplacé par le droit *Modifier en toute sécurité les droits des utilisateurs sur les objets*. Si les administrateurs ne disposent pas du droit *Télécharger la connexion localement*, ils ne doivent pas être autorisés à l'accorder à d'autres utilisateurs.

Dans le dossier Connexions de niveau supérieur :

1. Accordez aux groupes Administrateurs et Concepteurs d'univers le droit *Modifier en toute sécurité les droits des utilisateurs sur les objets*.

2. Accordez le droit *Modifier en toute sécurité les droits des utilisateurs sur les objets* aux utilisateurs qui gèrent les connexions, comme défini dans la section précédente. Ils auront le droit d'octroyer le droit *Télécharger la connexion localement*.
3. Refusez aux groupes Administrateurs et Concepteurs d'univers le droit *Modifier les droits des utilisateurs sur les objets*.

8.13 Cryptographie sur la plateforme de BI

Données sensibles

La fonction de cryptage de la plateforme de BI est conçue pour protéger les données sensibles stockées dans le référentiel CMS. Les données sensibles incluent les références de connexion utilisateur, les données de connectivité des sources de données et tout autre objet d'information stockant un mot de passe.
Ces données sont cryptées afin d'en garantir la confidentialité, de les protéger de la corruption et d'en contrôler l'accessibilité. Toutes les ressources de cryptage requises (notamment le moteur de cryptage, les bibliothèques RSA) sont installées par défaut sur chaque déploiement de la plateforme de BI.

La plateforme de BI utilise un système de cryptage à deux clés.

Clés de cryptage

Le cryptage et le décryptage des données sensibles sont traités en arrière-plan via l'interaction du SDK avec le moteur de cryptage interne. Les administrateurs système gèrent la sécurité des données à l'aide de clés de cryptage symétriques, sans crypter ou décrypter directement des blocs de données spécifiques.

Sur la plateforme de BI, des clés de cryptage symétriques, également appelées clés de chiffrement, sont utilisées pour crypter et décrypter les données sensibles. La Central Management Console dispose d'une zone de gestion dédiée aux clés de cryptage. La zone *Clés de cryptage* permet d'afficher, de générer, de désactiver, de bloquer et de supprimer des clés. Le système veille à ce qu'aucune clé nécessaire au décryptage de données sensibles ne puisse être supprimée.

Clés de cluster

Les clés de cluster sont des clés symétriques qui "enveloppent" les clés protégeant les clés de cryptage stockées dans le référentiel CMS. Grâce à des algorithmes de clés symétriques, les clés de cluster garantissent un certain niveau d'accessibilité au référentiel CMS. Une clé de cluster est affectée à chaque nœud de la plateforme de BI au cours de la configuration de l'installation. Les administrateurs système peuvent utiliser le CCM pour réinitialiser la clé de cluster.

8.13.1 Utilisation de clés de cluster

Au cours de la configuration d'installation de la plateforme de BI, une clé de cluster à huit caractères est créée pour le Server Intelligence Agent. Cette clé permet de crypter toutes les clés de cryptage du référentiel du CMS. Si vous ne disposez pas de la clé de cluster adéquate, vous ne pouvez pas accéder au CMS.

La clé de cluster est stockée en format chiffré dans un fichier `dbinfo`. Le nom de fichier `dbinfo` respecte cette convention : `_boe_<nom_sia>.dbinfo`, où `<nom_sia>` est le nom du Server Intelligence Agent du cluster.

Sous Windows, le fichier est stocké dans le répertoire suivant : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

Dans les systèmes Unix, le fichier est stocké dans le répertoire de la plateforme sous `<REPINSTALL>/sap_bobj/enterprise_xi40/`.

Plateforme Unix	Répertoire de la plateforme
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`

> **Remarque**
>
> La clé de cluster d'un nœud ne peut pas être extraite du fichier `dbinfo`. Nous recommandons aux administrateurs système de prendre des mesures scrupuleuses pour protéger les clés de cluster.

Seuls les utilisateurs disposant des droits d'administrateur peuvent réinitialiser les clés de cluster. Si nécessaire, utilisez le CCM pour réinitialiser la clé de cluster de chaque nœud de votre déploiement. De nouvelles clés de cluster sont automatiquement utilisées pour "envelopper" les clés de cryptage dans le référentiel du CMS.

8.13.1.1 Réinitialisation de la clé de cluster sous Windows

Avant de réinitialiser la clé de cluster pour votre nœud, veillez à ce que tous les serveurs gérés par le Server Intelligence Agent soient à l'arrêt.

1. Pour lancer le CCM, accédez à *Programmes* > *SAP Business Intelligence* > *Plateforme SAP BusinessObjects 4 de BI* > *Central Configuration Manager*.
2. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Arrêter*.

   > **Attention**
   >
   > Ne passez à l'étape 3 que lorsque le statut du SIA est Arrêté.

3. Cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Propriétés*. La boîte de dialogue *Propriétés* s'affiche.

4. Cliquez sur l'onglet *Configuration*.
5. Cliquez sur *Modifier* sous *Configuration de clé de cluster CMS*.
   Un message d'avertissement apparaît.
6. Cliquez sur *Oui* pour continuer.
   La boîte de dialogue *Modifier la clé de cluster* s'affiche.
7. Saisissez la même clé à huit caractères dans le champ *Nouvelle clé de cluster* et le champ *Confirmer la nouvelle clé de cluster*.

   > **Remarque**
   >
   > Sous Windows, les clés de cluster doivent contenir une combinaison de caractères en majuscules et en minuscules. Les utilisateurs peuvent aussi générer une clé aléatoire. La clé aléatoire est requise pour la compatibilité FIPS.

8. Cliquez sur *OK* pour soumettre la nouvelle clé de cluster au système.
   Un message confirmant que la clé de cluster a été correctement réinitialisée s'affiche.
9. Redémarrez le SIA.

En cas de cluster multi-nœuds, vous devez réinitialiser les clés de cluster pour tous les SIA de votre déploiement de la plateforme de BI avec cette nouvelle clé.

8.13.1.2 Réinitialisation de la clé de cluster sous UNIX

Avant de réinitialiser la clé de cluster d'un nœud, veillez à ce que tous les serveurs gérés par le nœud soient à l'arrêt.

1. Accédez au répertoire `<REPINSTALL>/sap_bobj`.
2. Saisissez **`./cmsdbsetup.sh`** et appuyez sur la touche *Entrée*.
   L'écran *Configuration de la base de données CMS* s'affiche.
3. Saisissez le nom du nœud et appuyez sur la touche *Entrée*.
4. Tapez **2** pour modifier la clé de cluster.
   Un message d'avertissement apparaît.
5. Sélectionnez *Oui* pour continuer.
6. Dans le champ proposé, saisissez une nouvelle clé de cluster et appuyez sur la touche *Entrée*.

   > **Remarque**
   >
   > Assurez-vous que la clé comporte au moins six caractères et combine deux des types de caractères suivants : majuscules, minuscules, nombres ou signes de ponctuation. Par exemple, vous pouvez avoir un caractère en minuscule avec un nombre, un caractère en majuscule avec un signe de ponctuation, etc.

7. Saisissez à nouveau la nouvelle clé de cluster dans le champ proposé et appuyez sur la touche *Entrée*.
   Un message s'affiche, vous informant que la clé de cluster a bien été réinitialisée.
8. Redémarrez le nœud.

Vous devez réinitialiser tous les nœuds de votre déploiement de la plateforme de BI pour utiliser la même clé de cluster.

8.13.2 Agents de cryptographie

Pour gérer les clés de cryptage dans la CMC, vous devez être membre du groupe Agents de cryptographie. Le compte administrateur par défaut créé pour la plateforme de BI est également membre du groupe Agents de cryptographie. Utilisez ce compte pour ajouter des utilisateurs au groupe Agents de cryptographie selon vos besoins. Nous recommandons de restreindre les membres du groupe à un nombre limité d'utilisateurs.

> ⓘ Remarque
>
> Lorsque des utilisateurs sont ajoutés au groupe Administrateurs, ils n'héritent pas des droits requis pour effectuer des tâches de gestion sur des clés de cryptage.

8.13.2.1 Ajout d'un utilisateur au groupe Agents de cryptographie

Un compte utilisateur doit exister sur la plateforme de BI avant de pouvoir être ajouté au groupe Agents de cryptographie.

> ⓘ Remarque
>
> Vous devez être membre des groupes *Administrateurs* et *Agents de cryptographie* pour ajouter un utilisateur au groupe Agents de cryptographie.

1. Dans la zone de gestion des *Utilisateurs et groupes* de la CMC, sélectionnez le groupe *Agents de cryptographie*.
2. Cliquez sur *Actions* > *Ajouter des membres au groupe*.
   La boîte de dialogue *Ajouter* apparaît.
3. Cliquez sur *Liste des utilisateurs*.
   La liste *Utilisateurs ou groupes disponibles* est actualisée et affiche tous les comptes utilisateur du système.
4. Déplacez le compte utilisateur que vous souhaitez ajouter au groupe Agents de cryptographie de la liste *Utilisateurs ou groupes disponibles* vers la liste *Utilisateurs ou groupes sélectionnés*.

   > → Conseil
   >
   > Pour rechercher un utilisateur particulier, utilisez le champ Rechercher.

5. Cliquez sur *OK*.

En qualité de membre du groupe Agents de cryptographie, le compte récemment ajouté aura accès à la zone de gestion des *Clés de cryptage* de la CMC.

8.13.2.2 Affichage des clés de cryptage dans la CMC

L'application de la CMC contient une zone de gestion dédiée aux clés de cryptage utilisées par le système de la plateforme de BI. L'accès à cette zone est réservé aux membres du groupe Agents de cryptographie.

1. Pour démarrer la CMC, cliquez sur *Programmes* > *SAP Business Intelligence* > *Plateforme SAP BusinessObjects BI 4* > *Central Management Console de la plateforme SAP BusinessObjects BI*.
   La page d'accueil de la CMC s'affiche.
2. Cliquez sur l'onglet *Clés de cryptage*.
   La zone de gestion *Clés de cryptage* s'affiche.
3. Double-cliquez sur la clé de cryptage sur laquelle vous souhaitez afficher de plus amples détails.

Informations associées

Affichage des objets associés à une clé de cryptage [page 179]

8.13.3 Gestion des clés de cryptage dans la CMC

Les agents de cryptographie utilisent la zone de gestion des *clés de cryptage* pour examiner, générer, désactiver, bloquer et supprimer les clés servant à protéger les données sensibles stockées dans le référentiel du CMS.

Toutes les clés de cryptage actuellement définies dans le système sont répertoriées dans la zone de gestion des *clés de cryptage*. Les informations de base concernant chaque clé sont fournies dans les en-têtes présentés dans le tableau suivant :

En-tête	Description
Title (Titre)	Nom permettant d'identifier la clé de cryptage
Statut	Statut actuel de la clé
Dernière modification de statut	Horodatage de la dernière modification associée à la clé de cryptage
Objets	Nombre d'objets associés à la clé

Informations associées

Statut des clés de cryptage [page 178]
Création d'une clé de cryptage [page 179]
Suppression d'une clé de cryptage du système [page 181]
Blocage d'une clé de cryptage [page 180]
Affichage des objets associés à une clé de cryptage [page 179]
Définition des clés de cryptage sur le statut Compromis [page 179]

8.13.3.1 Statut des clés de cryptage

Le tableau suivant répertorie toutes les options de statut possibles pour les clés de cryptage dans la plateforme de BI :

Statut	Description
Actif	Une seule clé de cryptage peut être définie sur le statut *Actif* dans le système. Cette clé permet de crypter les données sensibles qui seront stockées dans la base de données du CMS. Cette clé permet également de décrypter tous les objets qui apparaissent dans la liste Objet. Une fois qu'une clé de cryptage est créée, le statut *Actif* devient *Désactivé*. Une clé active ne peut pas être supprimée du système.
Désactivé	Une clé définie sur le statut *Désactivé* ne peut plus être utilisée pour crypter des données. Elle permet toutefois de décrypter tous les objets qui apparaissent dans la liste Objet. La réactivation d'une clé n'est plus possible dès lors qu'elle a été désactivée. Une clé définie sur le statut *Désactivé* ne peut pas être supprimée du système. Vous devez définir le statut de la clé sur *Bloqué* pour pouvoir la supprimer.
Compromis	Une clé de cryptage dont la sécurité est douteuse peut être définie sur le statut Compromis. En l'indiquant de la sorte, vous pouvez procéder ultérieurement au recryptage des objets de données encore associés à cette clé. Une fois qu'une clé est définie sur le statut Compromis, elle doit être bloquée pour pouvoir être supprimée du système.
Bloqué	Lorsqu'une clé de cryptage est bloquée, un processus est lancé dans lequel tous les objets actuellement associés à la clé sont recryptés avec la clé de cryptage actuellement définie sur le statut Actif. Une fois qu'une clé est définie sur le statut Bloqué, elle peut être supprimée du système en toute sécurité. Le mécanisme de blocage garantit que les données de la base de données du CMS peuvent toujours être déchiffrées. Il n'existe aucun moyen de réactiver une clé une fois qu'elle a été bloquée.
Désactivé : renouvellement du cryptage en cours de traitement	Indique que la clé de cryptage est sur le point d'être bloquée. Une fois ce processus terminé, la clé passe au statut *Bloqué*.
Désactivé : régénération de clé suspendue	Indique que le processus de blocage de la clé de cryptage a été suspendu. Cela survient généralement lorsque le processus a été suspendu délibérément ou si un objet de données associé à la clé n'est pas disponible.
Bloqué-Compromis	Une clé affiche le statut Bloqué-Compromis si elle a été définie sur le statut Compromis et que toutes les données qui lui étaient préalablement associées ont été chiffrées avec une autre clé. Lorsqu'une clé définie sur le statut *Désactivé* prend le statut Compromis, vous avez le choix entre ne rien faire ou bloquer la clé. Une fois qu'une clé

Statut	Description
	définie sur le statut Compromis est bloquée, elle peut être supprimée.

8.13.3.2 Affichage des objets associés à une clé de cryptage

1. Sélectionnez la clé dans la zone de gestion des *Clés de cryptage* de la CMC.
2. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* de la clé de cryptage apparaît.
3. Cliquez sur *Liste d'objets*dans le volet de navigation situé à gauche de la boîte de dialogue *Propriétés*.
   Tous les objets associés à la clé de cryptage sont répertoriés à droite du volet de navigation.

> → Conseil
>
> Utilisez les fonctions de recherche pour rechercher un objet spécifique.

8.13.3.3 Création d'une clé de cryptage

> ⚠ Attention
>
> Lors de la création d'une clé de cryptage, le système désactive automatiquement la clé dont le statut est *Actif*. Lorsqu'une clé a été désactivée, elle ne peut plus reprendre le statut *Actif*.

1. Dans la zone de gestion des *clés de cryptage*de la CMC, cliquez sur *Gérer* > *Créer* > *Clé de cryptage*.
   La boîte de dialogue *Créer une clé de cryptage* s'affiche.
2. Cliquez sur *Continuer* pour créer la clé de cryptage.
3. Saisissez le nom et la description de la nouvelle clé de cryptage, puis cliquez sur *OK* pour enregistrer vos informations.
   La nouvelle clé est répertoriée comme l'unique clé active dans la zone de gestion des *clés de cryptage*. La clé qui affichait auparavant le statut *Actif* apparaît désormais avec le statut *Désactivé.*

Toutes les nouvelles données sensibles générées et stockées dans la base de données du CMS seront à présent cryptées avec la nouvelle clé de cryptage. Vous avez la possibilité de bloquer la clé précédente et de recrypter tous ses objets de données avec la nouvelle clé active.

8.13.3.4 Définition des clés de cryptage sur le statut Compromis

Vous pouvez définir une clé de cryptage sur le statut Compromis si, pour une raison ou une autre, cette clé n'est plus considérée comme sûre. Cette fonction est utile dans le cadre du suivi des objectifs et permet

d'identifier les objets de données associés à la clé. Une clé de cryptage doit être désactivée avant de pouvoir être définie sur le statut Compromis.

> **Remarque**
>
> Vous pouvez également définir une clé sur le statut Compromis après l'avoir bloquée.

1. Accédez à la zone de gestion *Clés de cryptage* de la CMC.
2. Sélectionnez la clé de cryptage à définir sur le statut Compromis.
3. Cliquez sur *Actions* > *Marquer comme compromise*.
   La boîte de dialogue *Marquer comme compromis* s'affiche.
4. Cliquez sur *Continuer*.
5. Sélectionnez l'une des options suivantes dans la boîte de dialogue *Marquer comme compromis* :
   - *Oui* : lance le processus de recryptage de tous les objets de données associés à la clé définie sur le statut Compromis.
   - *Non* : la boîte de dialogue *Marquer comme compromise* est fermée et la clé de cryptage est définie sur le statut *Compromis* dans la zone de gestion *Clés de cryptage*.

     > **Remarque**
     >
     > Si vous sélectionnez *Non*, les données sensibles restent associées à la clé définie sur le statut Compromis. Celle-ci sera utilisée par le système pour décrypter les objets associés.

Informations associées

Blocage d'une clé de cryptage [page 180]
Statut des clés de cryptage [page 178]
Affichage des objets associés à une clé de cryptage [page 179]

8.13.3.5 Blocage d'une clé de cryptage

Une clé de cryptage portant le statut Désactivé peut être utilisée par les objets de données qui lui sont associés. Pour annuler l'association entre les objets cryptés et la clé désactivée, vous devez bloquer cette clé.

1. Sélectionnez la clé que vous souhaitez bloquer dans les clés répertoriées dans la zone de gestion des *Clés de cryptage*.
2. Cliquez sur *Actions* > *Bloquer*.
   La boîte de dialogue *Bloquer* s'affiche.
3. Cliquez sur *OK*.
   Un processus est lancé pour crypter tous les objets de données de la clé avec la clé actuellement active. Si la clé est associée à de nombreux objets de données, elle porte le statut *Désactivé : renouvellement du cryptage en cours de traitement* jusqu'à la fin du processus de recryptage.

Lorsqu'une clé de cryptage a été bloquée, elle peut être supprimée du système en toute sécurité du fait qu'aucun objet de données sensibles ne requiert cette clé pour être décrypté.

8.13.3.6 Suppression d'une clé de cryptage du système

Avant de pouvoir supprimer une clé de cryptage de la plateforme de BI, vous devez vérifier qu'aucun objet de données du système ne requiert cette clé. Cette restriction garantit que toutes les données sensibles stockées dans le référentiel du CMS puissent toujours être décryptées.

Une fois la clé de cryptage bloquée, suivez les instructions ci-dessous pour supprimer la clé du système.

1. Accédez à la zone de gestion des *clés de cryptage* de la CMC.
2. Sélectionnez la clé de cryptage à supprimer.
3. Cliquez sur *Gérer* > *Supprimer*.
   La boîte de dialogue *Supprimer* apparaît.
4. Cliquez sur *Supprimer* pour supprimer la clé de cryptage du système.
   La clé supprimée n'est plus affichée dans la zone de gestion *Clés de cryptage* de la CMC.

> **Remarque**
>
> Lorsqu'une clé de cryptage a été supprimée du système, elle ne peut plus être restaurée.

Informations associées

Blocage d'une clé de cryptage [page 180]
Statut des clés de cryptage [page 178]

8.14 Protection et confidentialité des données

Plusieurs problématiques en matière de confidentialité et exigences légales pèsent sur la protection des données. Outre la conformité aux réglementations applicables en matière de confidentialité des données, la conformité aux lois spécifiques du secteur en vigueur dans les divers pays doit également être garantie. SAP fournit des fonctionnalités spécifiques permettant de garantir la conformité aux exigences légales, notamment la protection des données. SAP n'indique pas si ces fonctionnalités constituent ou non le meilleur moyen de respecter les exigences de l'entreprise, du secteur, régionales, ou nationales. Par ailleurs, ces informations n'apportent aucun conseil et aucune recommandation concernant les fonctionnalités supplémentaires requises dans des environnements informatiques spécifiques. Les décisions relatives à la protection des données doivent être prises au cas par cas, en tenant compte de l'infrastructure système et des exigences légales applicables.

> **Remarque**
>
> Dans la plupart des cas, la conformité aux réglementations applicables en matière de protection et de confidentialité des données ne sera pas couverte par une fonctionnalité produit. Les logiciels SAP assurent la conformité aux exigences de protection des données grâce à des fonctionnalités de sécurité et à des fonctions spécifiques de protection des données, telles que le blocage et la suppression simplifiés des

données personnelles. SAP ne fournit aucun conseil juridique d'aucune façon que ce soit. Les définitions et autres termes utilisés dans le présent document ne proviennent d'aucune source juridique que ce soit.

8.14.1 Glossaire

Terme	Définition
Données personnelles	Toute information concernant une personne physique identifiée ou identifiable ("personne concernée"). Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, en particulier par référence à un identificateur tel qu'un nom, à un numéro d'identification, à des données d'emplacement, à un identificateur en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.
Objectif	Motif justifié de manière juridique, contractuelle, ou autre pour le traitement des **données personnelles**. L'hypothèse est que tout objectif a une fin qui est généralement définie au début de l'objectif.
Blocage	Méthode de restriction de l'accès aux données pour lesquelles l'**objectif commercial** est terminé.
Suppression	Destruction irréversible des **données personnelles**.
Période de rétention	Période entre la fin de l'utilisation d'un ensemble de données et la suppression de cet ensemble de données conformément aux réglementations applicables. Cette valeur combine la période de résidence et la période de blocage.
Fin de l'utilisation	Méthode d'identification du point dans le temps d'un ensemble de données lorsque le traitement des **données personnelles** n'est plus requis pour l'**objectif commercial** principal. Une fois la **fin de l'utilisation** atteinte, les données sont **bloquées** et elles deviennent accessibles uniquement aux utilisateurs dotés d'une autorisation spéciale (par exemple, les auditeurs fiscaux).

Terme	Définition
Données personnelles confidentielles	Catégorie de données personnelles qui inclut généralement le type d'informations ci-dessous : • Catégories spéciales de données personnelles telles que les données révélant l'origine ethnique ou raciale, les opinions politiques, religieuses ou croyances philosophiques, ou l'appartenance à un syndicat et le traitement des données génétiques, biométriques, ainsi que les données concernant la santé, la vie sexuelle ou l'orientation sexuelle • Données personnelles assujetties au secret professionnel • Données personnelles relatives aux infractions administratives ou pénales • Données personnelles relatives aux assurances et aux comptes bancaires ou de carte de crédit
Période de résidence	Période suivant la fin de l'utilisation d'un ensemble de données pendant laquelle les données sont conservées dans la base de données et peuvent être utilisées en cas de processus suivants liés à l'objectif d'origine. À la fin de la période de résidence configurée la plus longue, les données sont bloquées ou supprimées. La période de résidence est incluse dans la période de rétention globale.
Contrôle de l'emplacement d'utilisation	Processus conçu pour garantir l'intégrité des données en cas de blocage des données partenaire. Le contrôle de l'emplacement d'utilisation d'une application détermine si des données dépendantes pour un partenaire spécifique sont présentes dans la base de données. Si tel est le cas, les données sont toujours requises pour les activités commerciales. Le blocage des partenaires indiqués dans les données est donc impossible.
Consentement	Action de la personne concernée confirmant que l'utilisation de ses données personnelles doit être autorisée pour un objectif donné. La fonctionnalité de consentement permet de stocker l'enregistrement du consentement pour un objectif spécifique et indique si la personne concernée a accordé, retiré ou refusé son consentement.

8.14.2 Consentement de l'utilisateur

Les applications SAP demandent à l'utilisateur de donner son accord avant de collecter des données personnelles le concernant. La plateforme SAP BusinessObjects Business Intelligence fournit une

fonctionnalité permettant aux personnes concernées de donner leur consentement pour la collecte et le traitement de leurs données personnelles. SAP considère que l'utilisateur, un client SAP collectant des données par exemple, a obtenu, auprès de la personne concernée (personne physique telle qu'un client, un contact, ou un compte), l'autorisation de collecter ou de transférer des données à la solution.

> ⓘ Remarque
>
> *Message de consentement utilisateur*
>
> Ce produit contient des champs de saisie ouverts et librement configurables qui ne doivent pas être dédiés au stockage des données personnelles sans mesures techniques et organisationnelles supplémentaires pour assurer la protection et la confidentialité desdites données.

8.14.3 Rapport d'informations

Chaque personne a le droit de savoir si les données à caractère personnel la concernant font l'objet d'un traitement. Dans la plateforme SAP BusinessObjects Business Intelligence, il est possible d'afficher toutes les informations stockées concernant une personne concernée spécifique.

Pour en savoir plus sur la manière dont un utilisateur peut accéder aux informations stockées sur une personne concernée, consultez la section "Accès aux informations" dans le *Guide de l'utilisateur de la zone de lancement BI façon Fiori* publié sur le SAP Help Portal.

> ⓘ Remarque
>
> Les documents stockés localement ne sont pas protégés par la plateforme SAP BusinessObjects Business Intelligence. Une protection doit être fournie par le gestionnaire de périphériques respectif (par exemple, par le contrôle d'accès, le chiffrement, etc.).

8.14.4 Journalisation d'accès en lecture

La fonctionnalité de journalisation d'accès en lecture permet de surveiller et de journaliser les accès en lecture aux données sensibles. Ces données peuvent être classées comme sensibles par une loi, ou par une politique externe ou interne d'une société. Les questions fréquentes ci-dessous peuvent concerner les applications qui utilisent la fonctionnalité de journalisation d'accès en lecture :

- Qui a accédé aux données d'une entité de gestion spécifique, par exemple un compte bancaire ?
- Qui a accédé aux données personnelles, par exemple d'un partenaire ?
- Quel employé a accédé aux informations personnelles, par exemple concernant la religion ?
- Quels utilisateurs ont accédé aux comptes ou partenaires ?

Les informations concernant le ou les utilisateurs qui ont accédé à des données particulières dans une période spécifique permettent de répondre à ces questions. D'un point de vue technique, cela signifie que toutes les infostructures d'interface utilisateur et API distantes (qui accèdent à ces données) doivent être activées pour la journalisation.

La plateforme SAP BusinessObjects BI ne peut pas identifier, traiter ou stocker des données personnelles confidentielles. En conséquence, les accès en lecture ne sont pas journalisés par la plateforme de BI.

8.14.5 Suppression des données personnelles

- Blocage et suppression simplifiés : outre la conformité aux réglementations applicables en matière de confidentialité des données, la conformité aux lois spécifiques du secteur en vigueur dans les divers pays doit également être garantie. Dans certains pays, ces données personnelles doivent être supprimées une fois que l'objectif explicite et légitime spécifié pour le traitement des données personnelles arrive à expiration, mais uniquement si aucune autre période de rétention n'est définie par la loi, par exemple, des périodes de rétention pour les documents financiers. Souvent, dans certains scénarios ou pays, les exigences légales requièrent également le blocage des données lorsque l'objectif explicite et légitime spécifié pour le traitement de ces données arrive à expiration, mais que les données doivent être conservées dans la base de données en raison d'autres périodes de rétention légalement définies. Dans certains scénarios, les données personnelles incluent également des données référencées. Le défi en matière de suppression et de blocage des données consiste donc à gérer les données référencées en premier, puis les autres données, telles que les données partenaire.
- Suppression des données personnelles : la gestion des données personnelles est soumise aux lois applicables en matière de suppression de données de ce type à la fin de l'utilisation Si aucun objectif légitime ne requiert l'utilisation des données personnelles, celles-ci doivent être supprimées. Lorsque vous supprimez des données d'un jeu de données, tous les objets référencés liés à ce jeu de données doivent eux aussi être supprimés. Il convient également de prendre en compte les lois spécifiques du secteur en vigueur dans divers pays en plus des lois générales relatives à la protection des données. Les données doivent être supprimées une fois la période de rétention la plus longue arrivée à expiration.

Suppression des données personnelles dans la plateforme SAP BusinessObjects BI

La plateforme SAP BusinessObjects BI et ses clients n'identifient pas et ne catégorisent pas les données (acquises à partir de sources de données à des fins d'analyse et de reporting) dans les données personnelles. Pour ces données, les exigences en matière de récupération et de transparence des données doivent être gérées par le système sur lequel résident les données. La suppression des données est une fonctionnalité standard du système sur lequel résident les données. Par ailleurs, la plateforme SAP BusinessObjects BI et ses clients fournissent des fonctionnalités (connectivité active à des sources de données) permettant d'assurer la synchronisation des données avec le système sur lequel elles résident.

Cependant, les données utilisateur conservées sur le système sont accessibles aux utilisateurs eux-mêmes ou aux utilisateurs autorisés à gérer ces données à leur place. Les utilisateurs importés à partir d'un fournisseur d'identités (par exemple, Windows AD, LDAP, etc.) sont synchronisés avec ce fournisseur et doivent être gérés dans le fournisseur d'identités lui-même.

Les utilisateurs Enterprise créés sur la plateforme SAP BusinessObjects BI peuvent être supprimés ou désactivés par les utilisateurs autorisés à gérer ces données à leur place. Dans ce cas, la rétention peut être gérée en désactivant les utilisateurs dans le système. Une fois la période de conservation écoulée, ces utilisateurs peuvent être supprimés manuellement du système par les utilisateurs autorisés à gérer ces données à leur place.

Lorsque vous supprimez un compte d'utilisateur, le dossier Favoris, les catégories personnelles et la boîte de réception de cet utilisateur sont également supprimés. La propriété des artefacts dans le dossier public sera transférée de l'utilisateur supprimé à l'administrateur. Notez que pour les utilisateurs désactivés, cette opération doit être effectuée manuellement par les utilisateurs autorisés à gérer ces données à leur place.

L'identifiant de l'objet utilisateur est stocké à la fois dans la base de données d'audit et la base de données de commentaires. Cependant, ceci n'est pas effacé lors de la suppression des utilisateurs, car l'ID utilisateur est nécessaire dans les journaux d'audit, conformément aux exigences légales et de sécurité. De même, les commentaires faits par l'utilisateur sont à des fins de gestion, par conséquent, ils doivent être conservés pour historique conversationnel. Les commentaires ne sont pas censés contenir des données personnelles : les utilisateurs sont informés à l'avance qu'ils ne doivent pas divulguer de données personnelles dans des champs publics.

De plus, les entrées des bases de données d'audit et de commentaire peuvent être supprimées manuellement par les utilisateurs autorisés.

Pour en savoir plus sur la manière de désactiver un utilisateur, voir Pour modifier un compte d'utilisateur [page 107].

Pour en savoir plus sur la suppression des entrées de commentaire effectuées par un utilisateur, voir Gestion des paramètres de l'application des commentaires BI [page 738].

8.14.6 Journal des modifications

Le journal des modifications disponible dans la plateforme SAP BusinessObjects Business Intelligence traite les données personnelles des partenaires impliqués dans les demandes et activités de modification. Si une modification est apportée concernant le partenaire, le système journalise les informations suivantes dans les données personnelles à chaque demande et activité de modification :

- Nom de l'utilisateur qui a modifié les données
- Date et heure de la modification
- Type de modification (mise à jour, insertion, suppression, documentation d'un champ unique)
- Clés d'identification et valeurs respectives dans les enregistrements de données
- Ancienne et nouvelle valeur de l'attribut qui a été modifié
- Nom d'en-tête de l'attribut qui a été modifié

Vous pouvez définir les champs à journaliser.

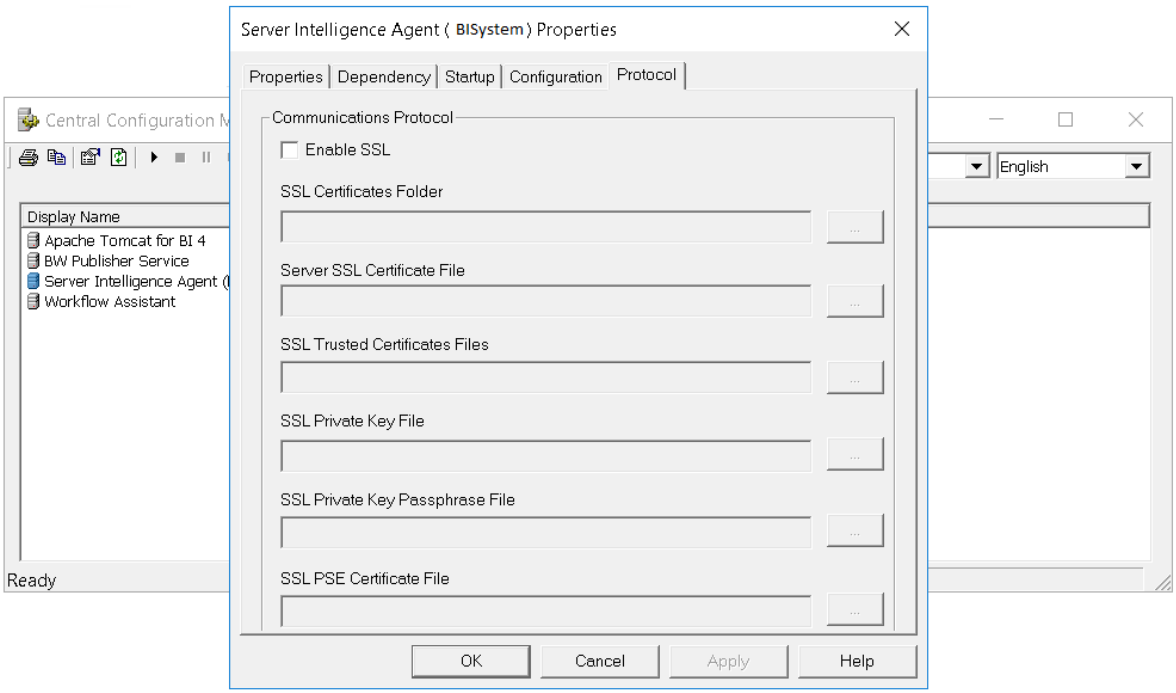
Pour en savoir plus sur les journaux de mise à jour du compte utilisateur, voir l'ID de type d'événement : 1007 dans Audit events and details [page 928].

8.15 Configuration des serveurs principaux pour SSL

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour toutes les communications réseau établies entre clients BI et serveurs BI au sein de votre déploiement de la plateforme de BI.

Pour configurer le protocole SSL pour toutes les communications serveur, vous devez effectuer les opérations suivantes :

- Déployer la plateforme de BI avec le protocole SSL activé.
- Créer des fichiers de clé et de certificat pour chaque ordinateur faisant partie de votre déploiement.
- Configurer l'emplacement de ces fichiers dans le CCM (Central Configuration Manager) et votre serveur d'applications Web.
- Vous pouvez également configurer SSL pour les certificats auto-signés ou gérés par une autorité de certification.



> **Remarque**
>
> Si vous utilisez des clients lourds, tels que Crystal Reports, vous devez également les configurer pour SSL si vous vous connectez au CMS. Sinon, vous obtiendrez des messages d'erreur lorsque vous tenterez de vous connecter à un CMS configuré pour SSL à partir d'un client lourd non configuré de la même manière.

8.15.1 Pour créer le fichier de configuration par défaut

Vous pouvez créer un fichier de configuration par défaut afin d'éviter d'avoir à ajouter des valeurs pendant la génération d'un certificat ou d'une demande de signature de certificat.

> **Remarque**
>
> Vous devez suivre les règles ci-dessous lorsque vous créez le fichier de configuration par défaut.
>
> - Vous devez ajouter les valeurs sur le côté gauche exactement comme mentionné ci-après.
> - Les valeurs sur la gauche ne sont pas sensibles à la casse.

- Un seul espace doit exister entre une valeur et le signe "égal à" (=). Par exemple, il existe un seul espace entre *CA_Common_Name* et le signe "égal à".
- Vous devez vous assurer qu'aucun espace ne suit les valeurs situées à droite.

Suivez les étapes ci-dessous pour créer un fichier de configuration par défaut avec le nom **Name.cnf** :

1. Ouvrez un nouveau document dans un éditeur de texte.
2. Ajoutez les valeurs comme ci-dessous :

```
CA_Common_Name = rootnm
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. Enregistrez le fichier avec le nom **Name.cnf** sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` sous Windows et sous `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` dans l'environnement Unix.

8.15.2 Création de fichiers de clé et de certificat

Pour configurer le protocole SSL pour vos communications serveur, créez un fichier de clé et un fichier de certificat pour chaque ordinateur faisant partie de votre déploiement à l'aide de l'outil de ligne de commande GENPSE.

> **Remarque**
>
> Vous devez recréer les certificats pour tous les ordinateurs du déploiement, y compris ceux qui exécutent des composants client lourds tels que Crystal Reports. Pour ces ordinateurs client, utilisez l'outil de ligne de commande `sslconfig` pour effectuer la configuration.

> **Remarque**
>
> Pour une sécurité maximale, toutes les clés privées doivent être protégées et ne doivent pas être transférées sur des canaux de communication non protégés.

8.15.2.1 Pour créer un fichier de clé et un fichier de certificat pour un ordinateur

Cette section couvre la génération de la clé et des certificats auto-signés requis pour sécuriser les communications entre les serveurs, ou entre le serveur et le client. Vous pouvez générer les certificats à

l'aide de l'outil GENPSE, un outil de ligne de commande permettant d'exécuter de nombreuses tâches liées à l'infrastructure à clé publique. L'outil GENPSE est utilisé pour générer des certificats X.509, des demandes de certificat et des fichiers PSE qui sont utilisés dans le workflow de CORBA SSL. Il est basé sur la bibliothèque cryptographique de SAP **CommonCryptoLib** et prend en charge le mécanisme de hachage SHA-2.

Pour créer les certificats requis pour la communication sécurisée, procédez comme suit :

> **Remarque**
>
> Vous pouvez créer un fichier de configuration par défaut **Name.cnf** avec les valeurs par défaut des informations demandées lors de la génération des certificats. Vous évitez ainsi d'avoir à ajouter les détails pour chaque certificat. Pour en savoir plus, voir Pour créer le fichier de configuration par défaut [page 187].

1. Accédez à `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` sous Windows et à `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` sous Unix.
2. Exécutez la commande suivante :
   - Sous Windows : `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - Sous Unix : `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

   Reportez-vous au tableau ci-dessous pour comprendre la commande :

Commande	Fonction
GenPSE.exe ou GenPSE.sh	Démarrer l'outil de cryptographie
selfsigned	Générer des certificats auto-signés
<Name.pse>	Nom de fichier PSE du serveur
<Name.der>	Nom de fichier du certificat de serveur
<root Cert.der>	Nom de certificat de l'autorité de certification
<Name.key>	Nom du fichier de clé privée du serveur
<private key password.txt>	Phrase de passe pour le fichier de clé privée du serveur
<path to Name.cnf>	Chemin d'accès du fichier de configuration par défaut

3. Saisissez les détails suivants pour générer le certificat de l'autorité de certification, du serveur et du client.
   - *Nom du pays*
   - *Nom de l'état ou de la province*
   - *Nom de la ville*
   - *Nom de l'organisation*
   - *Nom de l'entité organisationnelle*
   - *Saisissez votre nom*
   - *Nom commun*
   - *Adresse électronique*

- *Saisissez la date d'expiration au format AAMMJJ*

4. Votre fichier PSE et les certificats sont générés et stockés sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` sous Windows et sous `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` sous Unix.

> → Conseil
>
> Lors de la génération d'un certificat utilisateur, un paramètre supplémentaire *Type de certificat utilisateur* permet à l'outil d'identifier et de créer le certificat pour l'authentification du serveur ou du client. Actuellement, la valeur sélectionnée pour ce paramètre n'a aucun impact sur la configuration de CORBA SSL.

> ⓘ Remarque
>
> - Le nom du fichier de certificat PSE du serveur et le nom du fichier de certificat de l'autorité de certification doivent être différents.
> - La date d'expiration maximale est 2049.

8.15.3 Configuration de SSL lorsque le certificat est géré par une autorité de certification

Vous devez générer une demande de signature de certificat pour qu'une autorité de certification tierce signe les certificats. L'outil GenPSE génère une demande de signature de certificat en exécutant des commandes simples et en fournissant les informations requises lorsque nécessaire.

Suivez les étapes ci-dessous pour générer une demande de signature de certificat :

> ⓘ Remarque
>
> Vous pouvez créer un fichier de configuration par défaut `Name.cnf` avec les valeurs par défaut des informations demandées lors de la génération des certificats. Vous évitez ainsi d'avoir à ajouter les détails pour chaque certificat. Pour en savoir plus, voir Pour créer le fichier de configuration par défaut [page 187].

1. Accédez à `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` sous Windows et à `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` sous Unix.
2. Exécutez la commande suivante :
   - Sous Windows : `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
   - Sous Unix : `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

Commande	Fonction
GenPSE.exe ou GenPSE.sh	Démarrer l'outil de cryptographie
gencsr	Générer la demande de signature de certificat

Commande	Fonction
<csrname.p10>	Nom de fichier de la demande de signature de certificat
<Name.key>	Nom du fichier de clé privée du serveur
<private key password.txt>	Phrase de passe pour le fichier de clé privée du serveur
<path to Name.cnf>	Chemin d'accès du fichier de configuration par défaut

3. Saisissez les informations suivantes :
   - *Saisissez la phrase de passe de clé privée à définir*
   - *Saisissez à nouveau la phrase de passe de clé privée pour la confirmer*
   - *Nom du pays*
   - *Nom de l'état ou de la province*
   - *Nom de la ville*
   - *Nom de l'entité organisationnelle*
   - *Nom commun*
   - *Adresse électronique*
4. Votre fichier CSR au format P10, la clé privée du serveur et le fichier contenant la phrase de passe sont générés et stockés sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` sous Windows et sous `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` sous Unix. Le fichier CSR généré est envoyé à l'autorité de certification pour générer un certificat signé.

8.15.3.1 Génération d'un fichier pse

Lorsque vos certificats sont gérés par une autorité de certification externe, vous devez créer un fichier PSE. Suivez les étapes ci-dessous pour générer un fichier PSE :

1. Ouvrez `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Lancez la console de ligne de commande et exécutez `set SECUDIR=.` pour Windows et `export SECUDIR=.` pour Linux.
3. Exécutez `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>`.

   Reportez-vous au tableau ci-dessous pour mieux comprendre la commande :

Commande	Description
sapgenpse	Démarrer l'outil de cryptographie

Commande	Description
import_p8	Créer un nouveau fichier PSE à partir d'une clé privée au format PKCS#8 (protection facultative avec un chiffrement par mot de passe PKCS#5) avec tous les certificats X.509 nécessaires
-p <file_path_PSE>	Chemin d'accès au nouveau fichier PSE créé
-c <file_path_server_certificate>	Chemin d'accès au certificat de serveur
-r <file_path_CA_certificate>	Chemin d'accès au certificat CA
-z <file_path_passphrase_text_file>	Chemin d'accès vers le fichier texte de phrase de passe
<file_path_server_key>	Chemin d'accès au fichier de clé privée du serveur

Exemple

sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key

4. Fournissez un mode de passe vide en appuyant sur Entrée dans l'invite du mot de passe.
5. Ajoutez les identifiants utilisateur pour le fichier pse créé.

Conseil

Si le SIA est exécuté avec le compte LocalSystem, vous devez alors exécuter la commande suivante : `sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM` pour ajouter les identifiants utilisateur dans le fichier pse.

Remarque

Vous pouvez utiliser le nom de votre choix pour le fichier pse.

8.15.4 Configuration du protocole SSL

Après avoir créé des fichiers de clé et de certificat pour chaque ordinateur de votre déploiement et les avoir stockés en lieu sûr, vous devez indiquer l'emplacement de ces fichiers au CCM (Central Configuration Manager) et à votre serveur d'applications Web.

Vous devez également implémenter certaines étapes pour configurer le protocole SSL pour le serveur d'applications Web et pour tout ordinateur exécutant une application client lourd.

Activation des FIPS dans une plateforme basée sur UNIX pour la configuration de SSL

Le mode FIPS est activé par défaut pour une installation complète de la version 4.2 SP04 ou supérieure, mais vous devez l'activer manuellement pour les scénarios mentionnés ci-dessous :

- Mise à jour de correctif de la version 4.1 SPXX vers la version 4.2 SP04
- Mise à jour de correctif de la version 4.1 SPXX vers la version 4.2 SP02 ou SP03 et mise à jour ultérieure vers la version 4.2 SP04

> **Remarque**
>
> Sous Windows, CORBA SSL fonctionne même lorsque les FIPS ne sont pas activés, alors que dans les plateformes basées sur UNIX, il est nécessaire de s'assurer que les FIPS sont activées pour les serveurs avant de configurer CORBA SSL.

Étapes pour la configuration des FIPS

- Accédez à `<INSTALLDIR>/sap_bobj.`
- Exécutez `./stopservers`
- Ouvrez le fichier ccm.config.
- Ajoutez le texte "-FIPS" de la liste des propriétés du nœud SIA.
- Exécutez `./startservers`

8.15.4.1 Pour configurer le protocole SSL pour le CCM

1. Dans le CCM, cliquez avec le bouton droit sur le Server Intelligence Agent et choisissez *Propriétés*.
2. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet *Protocole*.
3. Assurez-vous que le paramètre *Activer SSL* est sélectionné.
4. Indiquez le chemin d'accès au répertoire dans lequel sont stockés les fichiers de clé et de certificat.

Champ	Description
Dossier des certificats SSL	Dossier dans lequel sont stockés tous les certificats et fichiers SSL requis. Par exemple : `d:\ssl`
Fichier du certificat SSL du serveur	Nom du fichier utilisé pour stocker le certificat SSL du serveur. Par défaut, `servercert.der`
Fichier des certificats SSL approuvés	Nom du fichier contenant les certificats SSL approuvés. Le nom par défaut est : `cacert.der`
Fichier de la clé privée SSL	Nom du fichier de clé privée SSL utilisé pour accéder au certificat. Le nom par défaut est : `server.key`
Fichier contenant la phrase de passe de la clé privée SSL	Nom du fichier texte contenant la phrase de passe utilisée pour accéder à la clé privée. Le nom par défaut est : `passphrase.txt`

Champ	Description
Fichier des certificats PSE SSL	Nom de ce fichier pse qui contient les informations relatives aux certificats de serveur et aux certificats approuvés.

> **Remarque**
>
> Vérifiez que le répertoire mentionné se trouve sur l'ordinateur sur lequel s'exécute le serveur.

8.15.4.2 Configuration du protocole SSL sous UNIX

Vous devez utilisez le script `serverconfig.sh` pour configurer le protocole SSL pour un SIA. Ce script fournit un programme textuel qui vous permet d'afficher des informations sur les serveurs et d'ajouter et de supprimer des serveurs de votre installation. Le script `serverconfig.sh` se trouve dans le répertoire `sap_bobj` de l'installation.

1. Utilisez le script `ccm.sh` pour arrêter le SIA et tous les serveurs SAP BusinessObjects.
2. Exécutez le script `serverconfig.sh`.
3. Sélectionnez *3 - Modifier un nœud*, puis appuyez sur la touche `Entrée`.
4. Spécifiez le SIA cible et appuyez sur `Entrée`.
5. Sélectionnez *1 - Modifiez la configuration SSL du Server Intelligence Agent*.
6. Sélectionnez *ssl*.
   Lorsque vous y êtes invité, spécifiez les emplacements de certificats SSL.
7. Répétez les étapes 1 à 6 pour chaque SIA si le déploiement de la plateforme de BI est un cluster de SIA.
8. Démarrez le SIA avec le script `ccm.sh` et attendez le démarrage des serveurs.

8.15.4.3 Pour configurer le protocole SSL pour le serveur d'applications Web

1. Si vous disposez d'un serveur d'applications Web J2EE, exécutez le SDK Java avec les propriétés système suivantes : Par exemple :

   ```
   -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl
   -DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key
   -Dpassphrase=passphrase.txt
   ```

   Le tableau ci-dessous affiche les descriptions correspondant à ces exemples :

Exemple	Description
`<DcertDir>=d:\ssl`	Répertoire de stockage des certificats et des clés.

Exemple	Description
`<DtrustedCert>=cacert.der`	Fichier de certificat approuvé. Si vous en spécifiez plusieurs, séparez-les par des points-virgules.
`<DsslCert>=clientcert.der`	Certificat utilisé par le SDK.
`<DsslKey>=client.key`	Clé privée du certificat SDK.
`<Dpassphrase>=passphrase.txt`	Fichier de stockage de la phrase de passe de la clé privée.
`<Dpsecert>=cert.pse`	Un PSE est un référentiel qui contient les clés et les certificats utilisés pour sécuriser une communication. Pour en savoir plus, voir 3026364.

2. Si vous disposez d'un serveur d'applications Web IIS, exécutez l'outil `sslconfig` à partir de la ligne de commande et suivez les étapes de configuration.

8.15.4.4 Pour configurer les clients lourds

Avant d'effectuer la procédure suivante, vous devez créer et enregistrer toutes les ressources SSL nécessaires (les certificats et les clés privées, par exemple) dans un répertoire connu.

Dans la procédure ci-dessous, il est supposé que vous avez suivi les instructions de création des ressources SSL suivantes :

Ressource SSL	
Dossier des certificats SSL	`d:\ssl`
Nom du fichier du certificat SSL du serveur	`servercert.der`
Certificat approuvé SSL ou nom du fichier de certificat racine	`cacert.der`
Nom du fichier de la clé privée SSL	`server.key`
Fichier contenant la phrase de passe pour accéder au fichier de la clé privée SSL	`passphrase.txt`
Nom du fichier des certificats PSE SSL	cert.pse

Une fois les ressources ci-dessus créées, observez les instructions suivantes pour configurer les applications client lourd telles que le Central Configuration Manager (CCM).

1. Assurez-vous que l'application de type client lourd n'est pas en cours d'opération.

   > **Remarque**
   >
   > Vérifiez que le répertoire mentionné se trouve sur l'ordinateur sur lequel s'exécute le serveur.

2. Exécutez l'outil de ligne de commande `sslconfig.exe`. Selon votre configuration, assurez-vous d'exécuter l'outil à partir des clients win32_x86 pour 32 bits ou win64_x64 pour 64 bits.

L'outil SSLC est installé avec votre logiciel de plateforme de BI. (Sous Windows par exemple, il se trouve par défaut dans le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

3. Saisissez la commande suivante :

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey
server.key
-passphrase     passphrase.txt -psecert cert.pse -protocol ssl
```

4. Relancez l'application client lourd.

Informations associées

Pour créer un fichier de clé et un fichier de certificat pour un ordinateur [page 188]

8.15.4.4.1 Pour configurer la connexion SSL pour l'outil de gestion de la traduction

Pour permettre aux utilisateurs d'utiliser la connexion SSL avec l'outil de gestion de la traduction, les informations concernant les ressources SSL doivent être ajoutées au fichier de configuration (`.ini`) de l'outil.

1. Cherchez le fichier `TransMgr.ini` dans le répertoire suivant : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. A l'aide d'un éditeur de texte, ouvrez le fichier `TransMgr.ini`.
3. Ajoutez les paramètres suivants :

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Enregistrez le fichier et fermez l'éditeur de texte.

Les utilisateurs peuvent à présent utiliser SSL pour se connecter à l'outil de gestion de la traduction.

8.15.4.4.2 Pour configurer SSL pour l'outil de conversion de rapports

RCT est obsolète dans la version BI 4.3. Pour en savoir plus, voir la note SAP 2801797

8.16 Description de la communication entre les composants de la plateforme de BI

Si votre système de la plateforme de BI est déployé entièrement sur le même sous-réseau sécurisé, il n'est pas nécessaire d'appliquer une configuration spéciale à vos pare-feu. Toutefois, vous pouvez choisir de déployer certains composants sur différents sous-réseaux séparés par un ou plusieurs pare-feu.

Il est important de bien comprendre la communication entre les serveurs de la plateforme de BI, les applications client enrichi et le serveur d'applications Web qui héberge le SDK de SAP BusinessObjects Enterprise avant de configurer votre système afin qu'il fonctionne avec les pare-feu.

Informations associées

Configuration de la plateforme de BI pour les pare-feu [page 211]
Exemples de scénarios classiques de pare-feu [page 216]

8.16.1 Présentation des serveurs de la plateforme de BI et des ports de communication

Il est important de comprendre le fonctionnement des serveurs de la plateforme de BI et de leurs ports de communication si le système déployé comporte des pare-feu.

8.16.1.1 Chaque serveur de la plateforme de BI est lié à un port de requêtes

Les serveurs de la plateforme de BI, l'Input File Repository Server par exemple, sont liés à un port de requêtes lors de leur démarrage. D'autres composants de la plateforme de BI, notamment les serveurs, les applications client enrichi et le SDK hébergé sur le serveur d'applications Web peuvent utiliser ce port de requêtes pour communiquer avec le serveur.

Les serveurs sélectionnent dynamiquement leur numéro de port de requêtes au démarrage ou redémarrage, sauf s'ils sont configurés pour utiliser un numéro de port spécifique. Un numéro de port de requêtes spécifique

doit être configuré manuellement pour les serveurs qui communiquent avec d'autres composants de la plateforme de BI à travers un pare-feu.

8.16.1.2 Chaque serveur de la plateforme de BI s'enregistre auprès du CMS

Lorsqu'ils démarrent, les serveurs de la plateforme de BI s'enregistrent auprès du CMS. Le CMS enregistre alors :

- le nom d'hôte (ou l'adresse IP) de l'ordinateur hôte du serveur ;
- le numéro du port de requêtes du serveur.

8.16.1.3 Le CMS utilise deux ports

Le CMS utilise deux ports : le port de requêtes et le port du serveur de noms. Le port de requêtes est sélectionné dynamiquement par défaut. Le port du serveur de noms par défaut est 6400.

Tous les serveurs de la plateforme de BI et applications client contactent tout d'abord le CMS™ sur son port de serveur de noms. Le CMS™ répondra à ce contact initial en renvoyant la valeur de son port de requêtes. Les serveurs utilisent ensuite ce port de requêtes pour communiquer avec le CMS™.

8.16.1.4 Répertoire des services enregistrés du CMS (Central Management Server)

Le CMS fournit un répertoire des services qu'il a enregistrés. Les autres composants de la plateforme de BI, tels que les services, les clients enrichis et le SDK hébergé sur le serveur d'applications Web peuvent contacter le CMS et demander une référence à un serveur particulier. La référence d'un service contient le numéro du port de requêtes du service, le nom d'hôte (ou l'adresse IP) de l'ordinateur hôte du serveur et l'ID du service.

Les composants de la plateforme de BI peuvent résider sur un sous-réseau différent de celui du serveur qu'ils utilisent. Le nom d'hôte (ou l'adresse IP) contenu dans la référence du service doit pouvoir être acheminé depuis l'ordinateur sur lequel se trouve le composant.

> **Remarque**
>
> La référence à un serveur de la plateforme de BI contient le nom d'hôte par défaut de l'ordinateur sur lequel se trouve le serveur. (Si un ordinateur a plusieurs noms d'hôte, le principal est choisi). Vous pouvez configurer un serveur de façon à ce que sa référence contiennent l'adresse IP et non le nom d'hôte.

Informations associées

Communication entre les composants de la plateforme de BI [page 200]

8.16.1.5 Les Server Intelligence Agents communiquent avec le Central Management Server

Votre déploiement ne pourra pas fonctionner si le SIA (Server Intelligence Agent) et le CMS (Central Management Server) ne peuvent pas communiquer entre eux. Assurez-vous que les ports de votre pare-feu sont configurés de façon à autoriser la communication entre tous les SIA et tous les CMS du cluster.

8.16.1.6 Les processus enfants du Job Server communiquent avec le niveau données et le CMS

La plupart des Job Servers créent un processus enfant pour gérer des tâches telle que la génération d'un rapport. Le Job Server crée un ou plusieurs processus enfants. Chaque processus enfant dispose de son propre port de requêtes.

Par défaut, chaque Job Server sélectionne dynamiquement un port de requêtes pour chaque processus enfant. Vous pouvez spécifier une plage de ports dans laquelle le Job Server peut effectuer sa sélection.

Tous les processus enfants communiquent avec le CMS. Si cette communication s'effectue via un pare-feu, vous devez effectuer les tâches suivantes :

- Spécifiez la plage de numéros de port depuis lesquels le Job Server peut effectuer sa sélection en ajoutant les paramètres `-requestJSChildPorts <port inférieur>-<port supérieur>` et `-requestPort <port>` à la ligne de commande du serveur. Cette plage doit être suffisamment grande pour autoriser le nombre maximal de processus enfants spécifié par `-maxJobs`.
- Ouvrir la plage de port spécifiée sur le pare-feu.

De nombreux processus enfants communiquent avec le niveau données. Par exemple, un processus enfant peut se connecter à une base de données de reporting, extraire les données, puis calculer des valeurs pour un rapport. Si le processus enfant du Job Server communique avec le niveau données via un pare-feu, vous devez :

- Ouvrir un chemin de communication sur le pare-feu à partir de n'importe quel port de l'ordinateur hébergeant le Job Server vers le port d'écoute de base de données de l'ordinateur hébergeant le serveur de base de données.

Informations associées

Présentation des lignes de commande [page 1124]

8.16.2 Communication entre les composants de la plateforme de BI

Dans les workflows classiques, les composants de la plateforme de BI tels que les clients navigateur, les applications client enrichi, les serveurs et le SDK hébergé sur le serveur d'applications Web, communiquent les uns avec les autres par le biais du réseau. Il est indispensable que vous compreniez ces workflows pour déployer les produits SAP Business Objects sur différents sous-réseaux séparés par un pare-feu.

8.16.2.1 Spécifications requises pour la communication entre les composants de la plateforme de BI

Les déploiements de la plateforme de BI doivent être conformes à ces spécifications.

1. Chaque serveur doit pouvoir établir la communication avec tous les autres serveurs de la plateforme de BI sur le port de requêtes de ce serveur.
2. Le Central Management Server utilise deux ports. Chaque serveur de la plateforme de BI, application Rich Client et le serveur d'applications Web qui héberge le SDK doivent pouvoir établir la communication avec le CMS sur ses deux ports.
3. Chaque processus enfant du Job Server doit pouvoir communiquer avec le CMS.
4. Les clients lourds doivent pouvoir établir la communication avec le port de requêtes des Input et Output File Repository Servers.
5. Si l'audit est activé pour les clients lourds et les applications Web, ils doivent être en mesure d'initier la communication avec le port de requêtes des serveurs de traitement adaptatif qui hébergent le service du proxy d'audit client.
6. Généralement, le serveur d'applications Web qui héberge le SDK doit pouvoir communiquer avec le port de requêtes de chaque serveur de la plateforme de BI.

   > **Remarque**
   >
   > Le serveur d'applications Web n'a besoin de communiquer qu'avec les serveurs de la plateforme de BI utilisés dans le déploiement. Par exemple, si Crystal Reports n'est pas utilisé, le serveur d'applications Web n'a pas besoin de communiquer avec les Crystal Reports Cache Servers.

7. Les Job Servers utilisent les numéros de port spécifiés avec la commande `-requestJSChildPorts <portinférieur>-<portsupérieur>`. Si aucune plage n'est spécifiée sur la ligne de commande, les serveurs utilisent des numéros de port aléatoires. Pour permettre à un Job Server de communiquer avec un CMS, un serveur FTP, SFTP ou un serveur de messagerie sur un autre ordinateur, ouvrez tous les ports de la plage spécifiée par `-requestJSChildPorts` sur votre pare-feu.
8. Le CMS doit être en mesure de communiquer avec le port d'écoute de la base de données du CMS.
9. Le serveur de connexion, la plupart des processus enfant du Job Server et tous les serveurs de traitement d'audit et bases de données système doivent pouvoir établir une communication avec le port d'écoute de la base de données de reporting.

Informations associées

Configuration requise pour les ports de la plateforme de Business Intelligence [page 201]

8.16.2.2 Configuration requise pour les ports de la plateforme de Business Intelligence

Cette section répertorie les ports de communication utilisés par les serveurs de la plateforme de BI, les applications client lourd, le serveur d'applications Web hébergeant le SDK et les applications logicielles tierces. Si vous déployez la plateforme de BI avec des pare-feu, ces informations vous permettront d'ouvrir le nombre minimal de ports dans ces pare-feu.

8.16.2.2.1 Ports requis pour les applications de la plateforme de BI

Ce tableau répertorie les serveurs et les numéros de port utilisés par les applications de la plateforme de BI.

Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
Crystal Reports	Concepteur SAP Crystal Reports 2020	CMS Input FRS Output FRS Report Application Server (RAS) de Crystal Reports 2020 Serveur de traitement Crystal Reports 2020 Crystal Reports Cache Server	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS Port de requêtes de l'Output FRS Port de requêtes du Report Application Server de Crystal Reports 2020 Port de requêtes du serveur de traitement Crystal Reports 2020 Port de requêtes du Crystal Reports Cache Server

Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
Crystal Reports	Concepteur SAP Crystal Reports pour Enterprise	CMS Input FRS Output FRS Crystal Reports Processing Server Serveur de mise en cache Crystal Reports	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS Port de requêtes de l'Output FRS Port de requêtes du serveur de traitement Crystal Reports Port de requêtes du Crystal Reports Cache Server
Live Office	Client Live Office	Application de fournisseur de services Web (`dswsbobje.war`) hébergeant le service Web Live Office	Port HTTP (80 par défaut)
SAP Analysis pour Microsoft Office	SAP Analysis pour Microsoft Office	CMS Serveur de traitement adaptatif hébergeant le service MDAS (Multi-Dimensional Analysis Service) Input FRS Output FRS	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes du serveur de traitement adaptatif Port de requêtes de l'Input FRS Port de requêtes de l'Output FRS
Plateforme de BI	SAP BusinessObjects Web Intelligence Rich Client	CMS Input FRS	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS
Plateforme de BI	Outil de conception d'univers	CMS Input FRS Serveur de connexion	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS Port du serveur de connexion
Plateforme de BI	Gestionnaire de vues d'entreprise	CMS Input FRS	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS

Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
Plateforme de BI	Central Configuration Manager (CCM)	CMS Server Intelligence Agent	Les ports suivants doivent être ouverts pour permettre au CCM de gérer des serveurs de la plateforme de BI distants : Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Les ports suivants doivent être ouverts pour permettre au CCM de gérer des processus SIA distants : Microsoft Directory Services (port TCP 445) NetBIOS Session Service (port TCP 139) NetBIOS Datagram Service (port UDP 138) NetBIOS Name Service (port UDP 137) DNS (port TCP/UDP 53) (Notez que certains ports mentionnés ci-dessus peuvent ne pas être requis. Consultez votre administrateur Windows).
Plateforme de BI	Server Intelligence Agent	Tous les serveurs de la plateforme de BI y compris le CMS	Port de requêtes du Server Intelligence Agent (6410 par défaut) Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS
Plateforme de BI	Repository Diagnostic Tool	CMS Input FRS Output FRS	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes de l'Input FRS Port de requêtes de l'Output FRS
Plateforme de BI	SDK de la plateforme de BI hébergé dans le serveur d'applications Web	Tous les serveurs de la plateforme de BI requis par les produits déployés. Par exemple, la communication avec le port de requêtes du serveur de traitement Crystal Reports 2020 est requise si le SDK extrait des rapports Crystal du CMS et interagit avec eux.	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes pour chaque serveur requis. Par exemple, le port de requêtes du serveur de traitement Crystal Reports 2020

Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
Plateforme de BI	Fournisseur de services Web (`dswsbobje.war`)	Tous les serveurs de la plateforme de BI requis par les produits accédant aux services Web. Par exemple, la communication avec les ports de requêtes de Cache Server et de serveur de traitement Dashboards est requise si SAP BusinessObjects Dashboards accède aux connexions de sources de données Enterprise par le biais du fournisseur de services Web.	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes pour chaque serveur requis. Par exemple, les ports de requête de Dashboards Cache Server et de serveur de traitement Dashboards.
Plateforme de BI	SAP BusinessObjects Analysis, édition pour OLAP	CMS Serveur de traitement adaptatif hébergeant le service MDAS (Multi-Dimensional Analysis Service) Input FRS Output FRS	Port de serveur de noms du CMS (6400 par défaut) Port de requêtes du CMS Port de requêtes du serveur de traitement adaptatif Port de requêtes de l'Input FRS Port de requêtes de l'Output FRS

8.16.2.2.2 Spécifications requises pour les ports des applications tierces

Ce tableau répertorie les logiciels tiers utilisés par les produits SAP BusinessObjects. Il contient des exemples spécifiques de certains distributeurs de logiciels, mais les spécifications de port diffèrent d'un distributeur à l'autre.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
Base de données système du CMS	Central Management Server (CMS)	Port d'écoute du serveur de base de données	Le CMS est le seul serveur qui communique avec la base de données système du CMS.
Base de données d'audit du CMS	Central Management Server (CMS)	Port d'écoute du serveur de base de données	Le CMS est le seul serveur qui communique avec la base de données d'audit du CMS.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
Base de données de reporting	Serveur de connexion Chaque processus enfant du Job Server Chaque serveur de traitement	Port d'écoute du serveur de base de données	Ces serveurs extraient les informations de la base de données de reporting.
Serveurs d'applications Web	Tous les services Web et applications Web SAP BusinessObjects, notamment la zone de lancement BI et la CMC	Port HTTP et port HTTPS. Par exemple, sur Tomcat, le port HTTP par défaut est le 8080 et le port HTTPS le 443.	Le port HTTPS n'est requis qu'en cas d'utilisation d'une communication HTTP sécurisée.
Serveur FTP	Chaque Job Server	FTP In (port 21) FTP Out (port 22)	Les Job Servers utilisent les ports FTP pour autoriser l'envoi vers FTP (*send to FTP*).

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
Serveur SFTP	Chaque Job Server	SFTP (port 22)	Les Job Servers utilisent les ports SFTP pour autoriser *l'envoi vers SFTP*. **Remarque** Une empreinte de clé d'hôte est utilisée pour sécuriser une connexion SSH et empêcher les attaques internes. Il s'agit d'un paramètre non nul obligatoire requis pour configurer SFTP. Le processus de génération de l'empreinte de clé d'hôte varie selon le serveur SFTP utilisé. L'administrateur/L'utilisateur doit configurer l'empreinte SHA-2 pour activer SFTP. Il peut se reporter à la documentation produit de ses implémentations de serveur SSH/SFTP pour générer une empreinte SHA-2. **Exemple** Les clients SFTP courants, tels que PuTTY et WinSCP, utilisent des empreintes MD5 pour identifier de façon unique les serveurs SFTP. Les empreintes MD5 ne fonctionnent pas. Pour en savoir plus sur l'extraction des empreintes SHA-2, voir la documentation relative au serveur SFTP. Voici un exemple de méthode avec un fichier de clé publique et des outils OpenSSH Unix. Avec un fichier de clé publique nommé RSAKey.pub qui contient : `ssh-rsa <base64 encoded key>`, exécutez le script suivant : `cut -d ' ' -f 2 < RSAKey.pub | base64 -d | openssl dgst -c -sha256`.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
			qui génère, par exemple, `(stdin)= 00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`, où la série de 20 chiffres dépend de la valeur de la clé publique codée en base64. Utilisez la valeur à 20 chiffres `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` pour l'empreinte de clé d'hôte. → Recommandation Il est recommandé d'activer la configuration SFTP sur la page des serveurs de la CMC dans BOE et d'utiliser les paramètres par défaut lors de l'envoi vers les serveurs SFTP.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
Serveur de messagerie	Chaque Job Server	SMTP (port du serveur SMTP)	Vous pouvez utiliser le même port pour SMTPS et SMTP. Toutefois, pour SMTPS, assurez-vous que SSL/TLS soit activé sur le serveur à l'aide de la commande smtp STARTTLS. Les Job Servers utilisent les ports SMTP pour autoriser l'envoi vers la messagerie (*send to email*). **Configuration de l'Adaptative Job Server :** Pour configurer l'Adaptative Job Server, réalisez les étapes ci-dessous : 1. Lancez la CMC (Central Management Console). 2. Sélectionnez *Serveurs* dans le menu déroulant. 3. Cliquez avec le bouton droit sur **AdaptiveJobServer** et sélectionnez *Destination*. 4. Sélectionnez *Adresse électronique* dans le menu déroulant. Si vous n'avez pas déjà ajouté le serveur de messagerie comme destination, vous devez alors d'abord ajouter le serveur de messagerie avant de continuer. 5. Saisissez les informations nécessaires. 6. Cochez l'option *Activer SSL* si nécessaire. 7. Choisissez *Enregistrer et fermer*. **Configuration SMTP sur SSL :** Pour configurer SMTP sur SSL, le serveur et le système BOE client doivent comporter le même serveur SMTP. Pour configurer SMTP sur SSL, suivez les étapes mentionnées ci-dessous :

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
			1. Générez un certificat à partir d'un serveur SMTP. 2. Dans la fenêtre *Destination*, cochez la case *Activer SSL*. 3. Saisissez le chemin absolu d'accès au certificat SMTP. **Remarque** Saisissez le chemin absolu d'accès au certificat SMTP. Si vous ne saisissez pas de chemin absolu d'accès au certificat SMTP, vous pouvez saisir un espace réservé (%SI_DEFAULT_CERT_LOC%) et le système le lit comme l'emplacement par défaut, c'est-à-dire `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` ou `\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` et recherche le certificat (le nom par défaut du certificat est certificate.crt). 4. Sélectionnez la *Sécurité de connexion*. **Remarque** Par défaut, l'option *StartTLS* est sélectionnée. Vous pouvez choisir de sélectionner *SSL/TLS*. 5. Sélectionnez la version TLS souhaitée.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
			Remarque Par défaut, TLS v1.0 est sélectionnée. Vous pouvez choisir de sélectionner TLS v1.1 ou TLS v1.2. 6. Cliquez sur *Enregistrer et fermer*. La configuration SMTP sur SSL est terminée. **Remarque** Lorsque vous réalisez une mise à jour de correctif de la version BI 4.1 SP6 vers une version ultérieure, par défaut, les options StartTLS et TLS v1.0 sont sélectionnées. **Remarque** • En cochant la case *Activer SSL*, l'utilisateur active un canal sécurisé. Cela permet de sécuriser la communication SMTP sur SSL. • Vous pouvez configurer un seul certificat SMTP par Adaptative Job Server. Vous ne pouvez pas avoir plusieurs certificats configurés pour un job server. • L'option *Activer SSL* est disponible uniquement dans l'Adaptive Job Server et non au niveau du document.
Serveurs UNIX auxquels les Job Servers peuvent envoyer du contenu	Chaque Job Server	rexec out (port 512) (UNIX uniquement) rsh out (port 514)	(UNIX uniquement) Les Job Servers utilisent ces ports pour autoriser l'envoi vers le disque.

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
Serveur d'authentification	CMS™ Serveur d'applications Web qui héberge le SDK Chaque client lourd, comme Live Office.	Port de connexion pour l'authentification tierce Par exemple, le serveur de connexion pour le serveur LDAP Oracle est défini par l'utilisateur dans le fichier ldap.ora.	Les références de connexion utilisateur sont stockées sur le serveur d'authentification tiers. Le CMS™, le SDK et les clients lourds répertoriés ici doivent communiquer avec le serveur d'authentification tiers lorsqu'un utilisateur se connecte.

8.17 Configuration de la plateforme de BI pour les pare-feu

Cette section explique de façon progressive comment configurer un système de la plateforme de BI de façon à ce qu'il fonctionne dans un environnement équipé d'un pare-feu.

8.17.1 Pour configurer le système pour des pare-feu

1. Déterminez quels composants de la plateforme de BI doivent communiquer via un pare-feu.
2. Configurez manuellement le port de requêtes de chaque serveur de la plateforme de BI devant communiquer via un pare-feu.
3. Configurez une plage de ports pour les enfants de Job Server devant communiquer à travers un pare-feu en ajoutant les paramètres `-requestJSChildPorts <port inférieur>-<port supérieur>` et `-requestPort <port>` à la ligne de commande du serveur.
4. Configurez le pare-feu de façon à permettre la communication avec les ports de requêtes et la plage de ports du Job Server sur les serveurs de la plateforme de BI configurés à l'étape précédente.
5. (Facultatif) Configurez le fichier hosts sur chaque ordinateur qui héberge un serveur de la plateforme de BI devant communiquer via un pare-feu.

Informations associées

Communication entre les composants de la plateforme de BI [page 200]
Configuration des numéros de port [page 477]
Présentation des lignes de commande [page 1124]
Spécification des règles de pare-feu [page 212]
Configurer le fichier hosts pour les pare-feu qui utilisent NAT [page 213]

8.17.1.1 Spécification des règles de pare-feu

Vous devez configurer le pare-feu de façon à permettre le trafic entre les différents composants de la plateforme de BI. Pour en savoir plus sur la spécification de ces règles, consultez la documentation de votre pare-feu.

Spécifiez une règle d'accès entrant pour chaque chemin de communication qui passe par le pare-feu. Il se peut que vous n'ayez pas à spécifier de règle d'accès pour chaque serveur de la plateforme de BI protégé par le pare-feu.

Utilisez le numéro de port spécifié dans la zone *Port de requêtes* du serveur sur la page Propriétés du serveur dans la CMC. N'oubliez pas que chaque serveur d'un même ordinateur doit utiliser un numéro de port unique. Certains serveurs SAP BusinessObjects utilisent plusieurs ports.

> **Remarque**
>
> Si la plateforme de BI est déployée via des pare-feu utilisant NAT, chaque serveur sur chaque ordinateur doit utiliser un numéro de port de requêtes unique. Autrement dit, aucun serveur d'un même déploiement ne peut partager le même port de requêtes.

> **Remarque**
>
> Il n'est pas nécessaire de spécifier de règles d'accès sortant. Les serveurs de la plateforme de BI n'établissent pas de communication pas avec le serveur d'applications Web ou avec les applications client. Les serveurs de la plateforme de BI peuvent établir la communication vers d'autres serveurs de la plateforme de BI du même cluster. Les déploiements avec des serveurs en cluster dans un environnement dont la sortie est protégée par pare-feu ne sont pas pris en charge.

Exemple

Cet exemple montre les règles d'accès entrant pour un pare-feu situé entre le serveur d'applications Web et les serveurs de la plateforme de BI. Dans ce cas, vous devez ouvrir deux ports pour le CMS, l'un pour l'Input FRS (File Repository Server) et l'autre pour l'Output FRS. Les numéros de port de requêtes sont les numéros de port spécifiés dans la zone *Port de demande* de la page de configuration de la CMC d'un serveur.

Ordinateur source	Port	Ordinateur de destination	Port	Action
Serveurs d'applications Web	N'importe lequel	CMS	6400	Autoriser
Serveurs d'applications Web	N'importe lequel	CMS	<Numéro de port de requêtes>	Autoriser
Serveurs d'applications Web	N'importe lequel	Input FRS	<Numéro de port de requêtes>	Autoriser

Ordinateur source	Port	Ordinateur de destination	Port	Action
Serveurs d'applications Web	N'importe lequel	Output FRS	<Numéro de port de requêtes>	Autoriser
N'importe lequel	N'importe lequel	CMS	N'importe lequel	Rejeter
N'importe lequel	N'importe lequel	Autres serveurs de plateforme	N'importe lequel	Rejeter

Informations associées

Communication entre les composants de la plateforme de BI [page 200]

8.17.1.2 Configurer le fichier hosts pour les pare-feu qui utilisent NAT

Cette étape est requise uniquement si les serveurs de la plateforme de BI doivent communiquer à travers un pare-feu sur lequel est activé Network Address Translation (NAT). Cette étape permet aux ordinateurs clients de mapper le nom d'hôte d'un serveur sur une adresse IP accessible.

> **Remarque**
>
> La plateforme de BI peut être déployée sur des ordinateurs utilisant DNS (Domain Name System). Dans ce cas, les noms d'hôte de l'ordinateur serveur peuvent être mappés sur une adresse IP accessible sur le serveur DNS, au lieu de le faire dans le fichier `hosts` de chaque ordinateur.

Traduction d'adresses réseau (NAT)

Un pare-feu est déployé pour protéger un réseau interne des accès non autorisés. Les pare-feu utilisant NAT mapperont les adresses IP à partir du réseau interne sur une adresse différente utilisée par le réseau externe. Cette traduction d'adresses améliore la sécurité en masquant les adresses IP internes du réseau externe.

Les composants de la plateforme de BI tels que les serveurs, les applications client lourd et le serveur d'applications Web hébergeant le SDK de utilisent une référence de service pour contacter un serveur. La référence de service contient le nom d'hôte de l'ordinateur serveur. Ce nom d'hôte doit être accessible à partir de l'ordinateur du composant de la plateforme de BI. Cela signifie que le fichier `hosts` sur l'ordinateur du composant doit mapper le nom d'hôte du serveur sur l'adresse IP externe du serveur. L'adresse IP externe du serveur est accessible du côté extérieur du pare-feu, tandis que l'adresse IP interne ne l'est pas.

La procédure de configuration du fichier `hosts` est différente pour Windows et UNIX.

8.17.1.2.1 Pour configurer le fichier hôtes sous Windows

1. Localisez tous les ordinateurs exécutant un composant de la plateforme de BI qui doit communiquer à travers un pare-feu sur lequel Network Address Translation (NAT) est activé.
2. Sur chaque ordinateur localisé à l'étape précédente, ouvrez le fichier `hosts` à l'aide d'un éditeur de texte tel que Notepad. Le fichier `hosts` est situé dans `\WINNT\system32\drivers\etc\hosts`.
3. Suivez les instructions du fichier `hosts` pour ajouter une entrée pour chaque ordinateur se trouvant derrière le pare-feu qui exécute un ou plusieurs serveurs de la plateforme de BI. Mappez le nom d'hôte de l'ordinateur serveur ou le nom de domaine complet sur son adresse IP externe.
4. Enregistrez le fichier `hosts`.

8.17.1.2.2 Configuration du fichier hosts sous UNIX

> **Remarque**
>
> Votre système d'exploitation UNIX doit être d'abord configuré de façon à consulter le fichier hosts pour résoudre les noms de domaine avant de consulter le DNS. Consultez votre documentation UNIX pour plus de détails.

1. Localisez tous les ordinateurs exécutant un composant de la plateforme de BI qui doit communiquer à travers un pare-feu sur lequel Network Address Translation (NAT) est activé.
2. Ouvrez le fichier hosts à l'aide d'un éditeur tel que `vi`. Le fichier `hosts` est situé dans le répertoire `\etc`.
3. Suivez les instructions du fichier `hosts` pour ajouter une entrée pour chaque ordinateur se trouvant derrière le pare-feu qui exécute un ou plusieurs serveurs de la plateforme de BI. Mappez le nom d'hôte de l'ordinateur serveur ou le nom de domaine complet sur son adresse IP externe.
4. Enregistrez le fichier `hosts`.

8.17.2 Débogage d'un déploiement équipé d'un pare-feu

Si un ou plusieurs serveurs de la plateforme de BI ne fonctionnent pas lorsque votre pare-feu est activé et cela même lorsque les ports attendus sont ouverts sur le pare-feu, vous pouvez utiliser les journaux d'événements pour déterminer quels serveurs tentent d'écouter sur quels ports ou quelles adresses IP. Vous pouvez alors soit ouvrir ces ports sur votre pare-feu, soit utiliser la CMC (Central Management Console) pour modifier les numéros de port ou les adresses IP sur lesquels ces serveurs tentent d'écouter.

A chaque démarrage d'un serveur de la plateforme de BI, celui-ci consigne les informations suivantes dans le journal d'événements pour chaque port de requête avec lequel il tente d'entrer en liaison.

- *Serveur* - Nom du serveur et si son lancement a réussi.
- *Adresses publiées* - Liste de combinaisons d'adresses IP et de ports enregistrées dans le service de noms que vont utiliser les autres serveurs pour communiquer avec ce serveur.

Si le serveur parvient à établir une liaison avec un port, le fichier journal affiche également *Ecoute sur les ports* (adresse IP et port sur lesquels écoute le serveur). Si le serveur ne parvient pas à établir de liaison avec le

port, le fichier journal affiche *Echec de l'écoute sur les ports* (adresse IP et port sur lesquels le serveur tente d'écouter et échoue).

Au démarrage d'un serveur Central Management Server, il consigne également les informations Adresses publiées, Ecoute sur les ports et Echec de l'écoute sur les ports pour le port du service des noms associé au serveur.

> **Remarque**
>
> Si le serveur est configuré pour utiliser un port affecté automatiquement ainsi qu'un nom d'hôte ou une adresse IP non valide, le journal d'événements indique que le serveur a échoué dans sa tentative d'écoute sur (nom d'hôte ou adresse IP et port « 0 »). Si un nom d'hôte ou une adresse IP spécifié(e) n'est pas valide, le serveur échoue avant que le système d'exploitation hôte ne lui attribue de port.

Exemple

L'exemple suivant indique l'entrée d'un Central Management Server qui écoute avec succès sur deux ports de requêtes et un port du service de noms.

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

8.17.2.1 Débogage d'un déploiement équipé d'un pare-feu

1. Lisez le journal d'événements pour déterminer si le serveur réussit à établir la liaison avec le port que vous avez spécifié.

   Si le serveur n'a pas pu établir de liaison avec un port, il y a probablement conflit de port entre le serveur et un autre processus en cours d'exécution sur la même machine. L'entrée *Echec de l'écoute sur* indique le port sur lequel porte la tentative d'écoute du serveur. Exécutez un utilitaire de type netstat pour déterminer le processus suivi par le port, puis configurez soit l'autre processus, soit un autre port d'écoute pour le serveur.
2. Si le serveur a réussi à établir une liaison avec un port, l'entrée *Ecoute sur* indique le port sur lequel le serveur écoute. Si un serveur écoute un port et ne fonctionne toujours pas correctement, vérifiez que ce port est ouvert dans le pare-feu ou configurez le serveur de manière à ce qu'il écoute sur un port ouvert.

Si tous les Central Management Servers de votre déploiement tentent d'écouter sur des ports ou des adresses IP indisponibles, les CMS ne démarrent pas et vous ne pouvez pas vous connecter à la CMC. Si vous souhaitez modifier le numéro de port ou l'adresse IP sur lesquels le CMS tente d'écouter, vous devez utiliser le Central Configuration Manager (CCM) pour spécifier un numéro de port ou une adresse IP valide.

Informations associées

Configuration des numéros de port [page 477]

8.18 Exemples de scénarios classiques de pare-feu

Cette section fournit des exemples de scénarios de déploiement de pare-feu classiques.

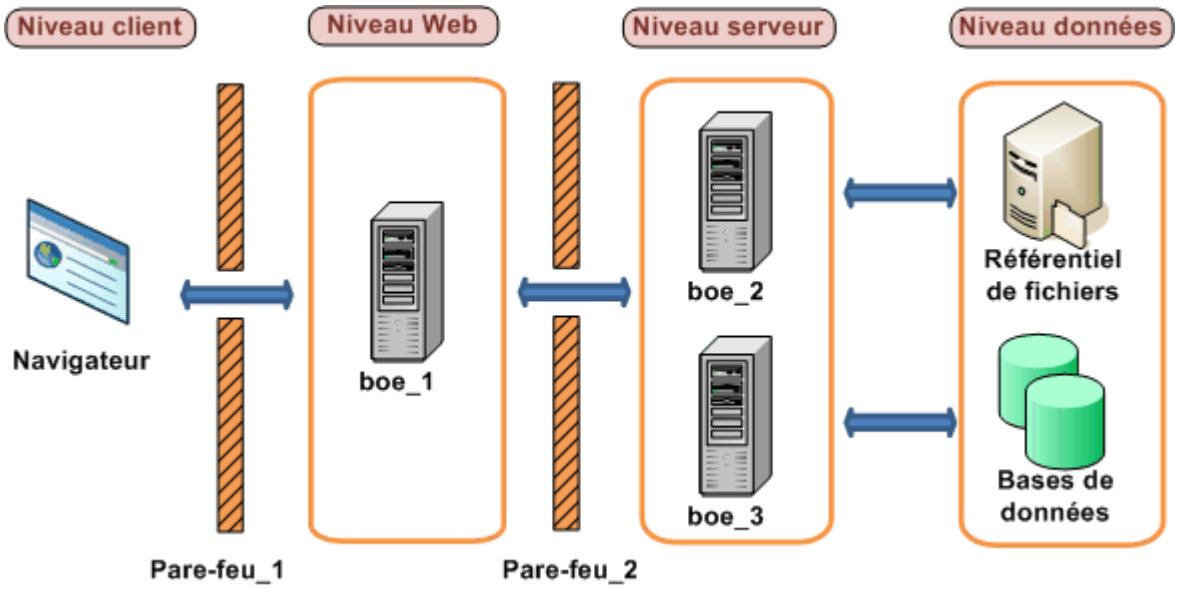
8.18.1 Exemple - Niveau application déployé sur un réseau distinct

Cet exemple explique comment configurer un pare-feu et la plateforme de BI afin qu'ils puissent fonctionner ensemble dans un déploiement où le pare-feu sépare le serveur d'applications Web des autres serveurs de la plateforme de BI.

Dans cet exemple, les composants de la plateforme de BI sont déployés sur les ordinateurs suivants :

- L'ordinateur boe_1 héberge le serveur d'applications Web et le SDK.
- L'ordinateur boe_2 héberge les serveurs de niveau Intelligence, notamment le Central Management Server, l'Input File Repository Server, l'Output File Repository Server, et l'Event Server.
- L'ordinateur boe_3 héberge les serveurs de niveau Traitement, notamment l'Adaptative Job Server, le serveur de traitement Web Intelligence, le Report Application Server, le Crystal Reports Cache Server et le serveur de traitement Crystal Reports.

Niveau application déployé sur un réseau distinct



8.18.1.1 Pour configurer un niveau application déployé sur un réseau distinct

Les étapes suivantes expliquent comment configurer cet exemple.

1. Cette configuration s'applique à l'exemple suivant :
   - Le serveur d'applications Web qui héberge le SDK doit pouvoir communiquer avec le CMS sur ses deux ports.
   - Le serveur d'applications Web qui héberge le SDK doit pouvoir communiquer avec chaque serveur de la plateforme de BI.
   - Le navigateur doit pouvoir accéder au port de requêtes HTTP ou HTTPS sur le serveur d'applications Web.
2. Le serveur d'applications Web doit pouvoir communiquer avec tous les serveurs sur les ordinateurs `boe_2` et `boe_3`. Configurez les numéros de port de chaque serveur sur ces ordinateurs. Notez que vous pouvez utiliser n'importe quel port disponible compris entre 1025 et 65535.
   Les numéros de port choisis pour cet exemple sont indiqués dans le tableau ci-dessous.

Serveur	Numéro de port
Central Management Server	6400
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event Server	6425
Adaptative Job Server	6435
Crystal Reports Cache Server	6440
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Configurez les pare-feu `Pare-feu_1` et `Pare-feu_2` de façon à permettre la communication avec les ports fixes des serveurs et du serveur d'applications Web que vous avez configuré à l'étape précédente.

   Dans cet exemple, nous ouvrons le port HTTP pour le serveur d'applications Tomcat.

   Configuration de Pare-feu_1

Port	Ordinateur de destination	Port	Action
N'importe lequel	boe_1	8080	Autoriser

   Configuration de Pare-feu_2

Ordinateur source	Port	Ordinateur de destination	Port	Action
boe_1	N'importe lequel	boe_2	6400	Autoriser
boe_1	N'importe lequel	boe_2	6411	Autoriser

Ordinateur source	Port	Ordinateur de destination	Port	Action
boe_1	N'importe lequel	boe_2	6415	Autoriser
boe_1	N'importe lequel	boe_2	6420	Autoriser
boe_1	N'importe lequel	boe_2	6425	Autoriser
boe_1	N'importe lequel	boe_3	6435	Autoriser
boe_1	N'importe lequel	boe_3	6440	Autoriser
boe_1	N'importe lequel	boe_3	6460	Autoriser
boe_1	N'importe lequel	boe_3	6465	Autoriser
boe_1	N'importe lequel	boe_3	6470	Autoriser

4. Ce pare-feu n'étant pas configuré NAT, il n'est pas nécessaire de configurer le fichier `hosts`.

Informations associées

Configuration des numéros de port [page 477]
Description de la communication entre les composants de la plateforme de BI [page 197]

8.18.2 Exemple : Client lourd et niveau base de données séparés des serveurs de la plateforme de BI par un pare-feu

Cet exemple montre comment configurer un pare-feu et la plateforme de BI afin qu'ils puissent fonctionner ensemble dans un scénario de déploiement dans lequel :

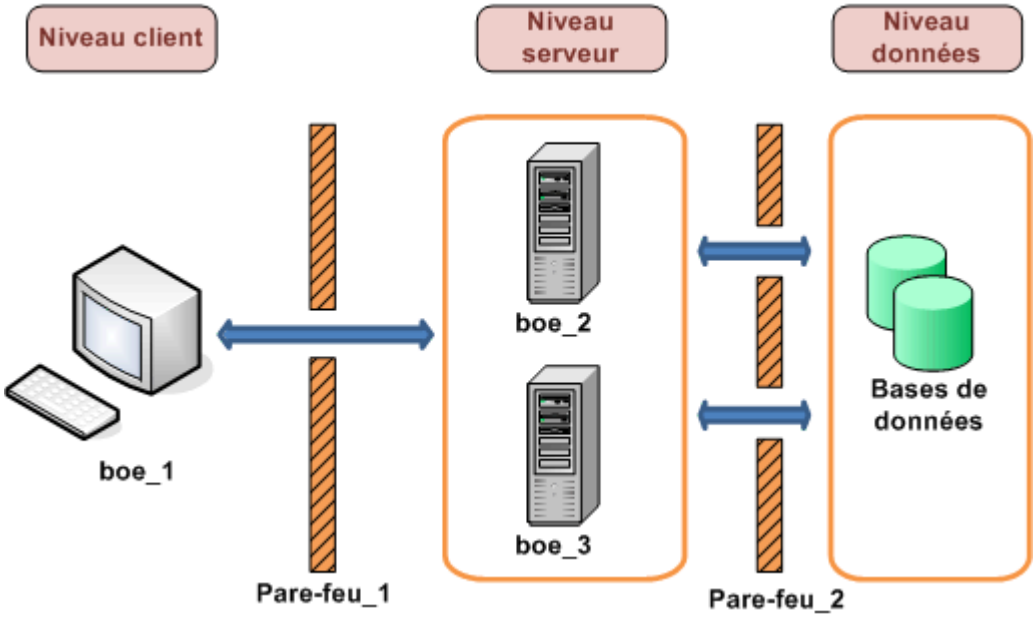
- un pare-feu sépare un client lourd des serveurs de la plateforme de BI ;
- un pare-feu sépare les serveurs de la plateforme de BI du niveau base de données.

Dans cet exemple, les composants de la plateforme de BI sont déployés sur les ordinateurs suivants :

- L'ordinateur `boe_1` héberge l'Assistant de publication. L'Assistant de publication est un client lourd de la plateforme de BI.
- L'ordinateur `boe_2` héberge les serveurs de niveau Intelligence, notamment le CMS (Central Management Server), l'Input File Repository Server, l'Output File Repository Server, et l'Event Server.
- L'ordinateur `boe_3` héberge les serveurs de niveau Traitement, notamment l'Adaptative Job Server, le serveur de traitement Web Intelligence, le Report Application Server, le serveur de traitement Crystal Reports et le Crystal Reports Cache Server.
- L'ordinateur `Bases de données` héberge les bases de données d'audit et système du CMS, ainsi que la base de données de reporting. Notez que vous avez la possibilité de déployer les deux bases de données sur le même serveur de base de données ou de déployer chaque base de données sur son propre serveur

de base de données. Dans cet exemple, toutes les bases de données du CMS et la base de données de reporting sont déployées sur le même serveur de base de données.

Rich Client et niveau base de données déployés sur des réseaux distincts



8.18.2.1 Pour configurer des niveaux séparés des serveurs de la plateforme de BI par un pare-feu

Les étapes suivantes expliquent comment configurer cet exemple.

1. Appliquez la configuration suivante à cet exemple :
   - L'Assistant de publication doit pouvoir établir la communication avec le CMS™ sur ses deux ports.
   - L'Assistant de publication doit pouvoir établir la communication avec l'Input File Repository Server et l'Output File Repository Server.
   - Le serveur de connexion, tous les processus enfant du Job Server et tous les serveurs de traitement doivent avoir accès au port d'écoute sur le serveur de base de données de reporting.
   - Le CMS™ doit pouvoir accéder au port d'écoute de la base de données sur le serveur de base de données du CMS™.
2. Configurez un port spécifique pour le CMS™, l'Input FRS et l'Output FRS. Notez que vous pouvez utiliser n'importe quel port disponible compris entre 1025 et 65535.
   Les numéros de port choisis pour cet exemple sont indiqués dans le tableau ci-dessous.

Serveur	Numéro de port
Central Management Server ™	6411
Input File Repository Server	6415
Output File Repository Server	6416

3. Il n'est pas nécessaire de configurer une plage de ports pour les enfants du Job Server dans la mesure où le pare-feu entre les Job Servers et les serveurs de base de données seront configurés de façon à permettre à n'importe quel port d'établir la communication.
4. Configurez `<Pare-feu_1>` de façon à permettre la communication avec les ports fixes des serveurs de la plateforme configurés à l'étape précédente. Le port 6400 est le port de serveur de noms par défaut du CMS™ et n'a pas eu besoin d'être configuré explicitement à l'étape précédente.

Port	Ordinateur de destination	Port	Action
N'importe lequel	boe_2	6400	Autoriser
N'importe lequel	boe_2	6411	Autoriser
N'importe lequel	boe_2	6415	Autoriser
N'importe lequel	boe_2	6416	Autoriser

Configurez `<Pare-feu_2 >`de façon à permettre la communication avec le port d'écoute du serveur de base de données. Le CMS™ (sur *boe_2*) doit pouvoir accéder à la base de données système et d'audit du CMS™ et les Job Servers (sur *boe_3*) doivent pouvoir accéder aux bases de données système et d'audit. Notez qu'il n'a pas été nécessaire de configurer une plage de ports pour les processus enfants du Job Server, car leur communication avec le CMS n'est pas protégée par un pare-feu.

Ordinateur source	Port	Ordinateur de destination	Port	Action
boe_2	N'importe lequel	Databases	3306	Autoriser
boe_3	N'importe lequel	Databases	3306	Autoriser

5. Ce pare-feu n'étant pas configuré NAT, il n'est pas nécessaire de configurer le fichier `hosts`.

Informations associées

Description de la communication entre les composants de la plateforme de BI [page 197]
Configuration de la plateforme de BI pour les pare-feu [page 211]

8.19 Paramètres de pare-feu pour les environnements intégrés

Cette section détaille les critères et paramètres de port spécifiques pour les déploiements de la plateforme de BI s'intégrant aux environnements ERP suivants.

- SAP
- Oracle EBS
- Siebel
- JD Edwards

- PeopleSoft

Parmi les composants de la plateforme de BI figurent les clients navigateur, les clients enrichis, les serveurs et le SDK hébergé sur le serveur d'applications Web. Les composants système peuvent être installés sur plusieurs ordinateurs. Il est utile de comprendre les principes de base de la communication entre la plateforme de BI et les composants ERP avant de configurer le système en vue d'une utilisation avec des pare-feu.

Ports requis pour les serveurs de la plateforme de BI

Vous trouverez ci-dessous la liste des ports requis pour chaque serveur de la plateforme de BI :

Spécifications requises pour le port du serveur
• Port du serveur de noms du Central Management Server • Port de requêtes du Central Management Server • Port de requêtes de l'Input FRS • Port de requêtes de l'Output FRS • Port de requêtes du Report Application Server • Port de requêtes du Crystal Reports Cache Server • Port de requêtes du Page Server Crystal Reports • Port de requêtes du serveur de traitement Crystal Reports

8.19.1 Instructions propres au pare-feu pour l'intégration SAP

Votre déploiement de la plateforme de BI doit observer les règles de communication suivantes :

- Le CMS doit être en mesure d'établir la communication avec le système SAP via le port de passerelle du système SAP.
- L'Adaptive Job Server et le serveur de traitement Crystal Reports (ainsi que les composants d'accès aux données) doivent être en mesure d'établir la communication avec le système SAP via le port de passerelle du système SAP.
- Le composant BW Publisher doit être en mesure d'établir la communication avec le système SAP via le port de passerelle du système SAP.
- Les composants de la plateforme de BI déployés au niveau du portail SAP Enterprise (par exemple, iViews et KMC) doivent être en mesure d'établir la communication avec les applications Web de la plateforme de BI via les ports HTTP/HTTPS.
- Le serveur d'applications Web doit être en mesure d'établir la communication au niveau du service de passerelle du système SAP.
- Crystal Reports doit être en mesure d'établir la communication avec l'hôte SAP via le port de passerelle du système SAP et le port de répartiteur du système SAP.

Le port de réception du service de passerelle SAP est celui spécifié lors de l'installation.

> **Remarque**
>
> Si un composant requiert un routeur SAP pour se connecter à un système SAP, vous pouvez configurer le composant à l'aide de la chaîne de routeur SAP. Par exemple, lorsque vous configurez un système d'autorisation SAP pour importer des rôles et des utilisateurs, la chaîne de routeur SAP peut remplacer le nom du serveur d'applications. Cela garantit que le CMS communiquera avec le système SAP par le biais du routeur SAP.

Informations associées

Installation d'une passerelle SAP locale [page 1036]

8.19.1.1 Spécifications détaillées requises pour le port

Ports requis pour SAP

La plateforme de BI utilise le Connecteur Java SAP (SAP JCO) pour communiquer avec SAP NetWeaver. Vous devez configurer les ports suivants et vous assurer de leur disponibilité :

- Port d'écoute du service de passerelle SAP (par exemple, 3300).
- Port d'écoute du service de répartiteur SAP (par exemple, 3200).

Le tableau suivant répertorie les configurations de port spécifiques dont vous avez besoin.

Ordinateur source	Port	Ordinateur de destination	Port	Action
SAP	N'importe laquelle	Serveur d'applications Web de la plateforme de BI	Port HTTP/HTTPS du service Web	Autoriser
SAP	N'importe laquelle	CMS	Port du serveur de noms du CMS	Autoriser
SAP	N'importe laquelle	CMS	Port du CMS requis	Autoriser
Serveur d'applications Web	N'importe laquelle	SAP	Port du service de passerelle du système SAP	Autoriser
Central Management Server (CMS)	N'importe laquelle	SAP	Port du service de passerelle du système SAP	Autoriser
Crystal Reports™	N'importe laquelle	SAP	Port du service de passerelle du système SAP et port du répartiteur du système SAP	Autoriser

8.19.2 Configuration du pare-feu pour l'intégration JD Edwards EnterpriseOne

Les déploiements de la plateforme de BI qui communiqueront avec le logiciel JD Edwards doivent être conformes à ces règles de communication générales :

- Les applications Web de la Central Management Console doivent être en mesure d'établir la communication avec JD Edwards EnterpriseOne par le biais du port JDENET et d'un port sélectionné de manière aléatoire.
- Crystal Reports avec le composant côté client Connectivité des données doit être en mesure d'établir la communication avec JD Edwards EnterpriseOne par le biais du port JDNET. Pour l'extraction de données, le côté JD Edwards EnterpriseOne doit être en mesure de communiquer avec le pilote via un port aléatoire qui ne peut pas être contrôlé.
- Le CMS (Central Management Server) doit être en mesure d'établir la communication avec JD Edwards EnterpriseOne par le biais du port JDENET et d'un port sélectionné de manière aléatoire.
- Le numéro du port JDENET se trouve dans le fichier de configuration du serveur d'applications JD Edwards EnterpriseOne (`JDE.INI`) dans la section JDENET.

Ports requis pour les serveurs de la plateforme de BI

Produit	Spécifications requises pour le port du serveur
SAP BusinessObjects Business Intelligence	Port du serveur de connexion de la plateforme de BI

Exigences en matière de ports pour JD Edwards EnterpriseOne

Produit	Configuration de port	Description
JD Edwards EnterpriseOne	Port JDENET et un port sélectionné de manière aléatoire	Utilisé pour la communication établie entre la plateforme de BI et le serveur d'applications JD Edwards EnterpriseOne.

Configuration du serveur d'applications Web pour communiquer avec JD Edwards

Cette section explique comment configurer un pare-feu et la plateforme de BI afin qu'ils puissent fonctionner ensemble dans un scénario de déploiement dans lequel le pare-feu sépare le serveur d'applications Web des autres serveurs de la plateforme.

Pour obtenir des informations sur la configuration du pare-feu avec les clients et les serveurs de la plateforme de BI, voir la section *Configuration requise pour les ports de la plateforme de Business Intelligence* de ce guide.

Outre la configuration standard des pare-feu, la communication avec les serveurs JD Edwards réclame d'ouvrir des ports supplémentaires.

Pour JD Edwards EnterpriseOne Enterprise

Ordinateur source	Port	Ordinateur de destination	Port	Action
CMS avec fonction Connectivité de la sécurité pour JD Edwards EnterpriseOne	N'importe laquelle	JD Edwards EnterpriseOne	N'importe laquelle	Autoriser
Serveurs de la plateforme de BI avec connectivité des données pour JD Edwards EnterpriseOne	N'importe laquelle	JD Edwards EnterpriseOne	N'importe laquelle	Autoriser
Crystal Reports avec connectivité des données côté client pour JD Edwards EnterpriseOne	N'importe laquelle	JD Edwards EnterpriseOne	N'importe laquelle	Autoriser
Serveur d'applications Web	N'importe laquelle	JD Edwards EnterpriseOne	N'importe laquelle	Autoriser

8.19.3 Instructions propres au pare-feu pour Oracle EBS

Votre déploiement de la plateforme de BI doit permettre aux composants suivants d'établir la communication avec le port d'écoute de la base de données Oracle :

- Composants Web de la plateforme de BI
- CMS (particulièrement le plug-in de sécurité Oracle EBS)
- Serveurs principaux de la plateforme de BI (particulièrement le composant d'accès aux données EBS)
- Crystal Reports (particulièrement le composant d'accès aux données EBS)

> **Remarque**
>
> Dans tous les cas cités ci-dessus, la valeur par défaut du port d'écoute de la base de données Oracle est 1521.

8.19.3.1 Spécifications détaillées requises pour le port

Outre la configuration de pare-feu standard pour la plateforme de BI, certains ports supplémentaires doivent être ouverts pour fonctionner dans un environnement Oracle EBS intégré :

Ordinateur source	Port	Ordinateur de destination	Port	Action
Serveur d'applications Web	N'importe lequel	Oracle EBS	Port de base de données Oracle	Autoriser

Ordinateur source	Port	Ordinateur de destination	Port	Action
CMS avec fonction Connectivité de la sécurité pour Oracle EBS	Quelconque	Oracle EBS	Port de base de données Oracle	Autoriser
Serveurs de la plateforme de BI avec la fonction côté serveur Connectivité de données pour Oracle EBS	N'importe lequel	Oracle EBS	Port de base de données Oracle	Autoriser
Crystal Reports avec la fonction côté client Connectivité de données pour Oracle EBS	N'importe lequel	Oracle EBS	Port de base de données Oracle	Autoriser

8.19.4 Configuration du pare-feu pour l'intégration PeopleSoft Enterprise

Les déploiements de la plateforme de BI qui communiqueront avec PeopleSoft Enterprise doivent être conformes aux règles de communication générales suivantes :

- Le CMS (Central Management Server) ayant le composant Connectivité de sécurité doit être en mesure d'initier une communication avec le service Web PeopleSoft Query Access (QAS).
- Les serveurs de la plateforme de BI ayant le composant Connectivité de données doivent être en mesure d'initier une communication avec le service Web PeopleSoft QAS.
- Les rapports Crystal ayant le composant côté client Connectivité de données doivent être en mesure d'initier une communication avec le service Web PeopleSoft QAS.
- La passerelle Enterprise Management (EPM) doit être en mesure de communiquer avec le CMS et Input File Repository Server.
- La passerelle EPM doit être en mesure de communiquer avec la base de données PeopleSoft via une connexion ODBC.

Le numéro de port du service Web doit être celui spécifié dans le nom de domaine PeopleSoft Enterprise.

Ports requis pour les serveurs de la plateforme de BI

Produit	Spécifications requises pour le port du serveur
Plateforme SAP BI	Port du serveur de connexion de la plateforme de BI

Configuration de port requise pour PeopleSoft

Produit	Configuration de port	Description
PeopleSoft Enterprise : People Tools 8.46 ou version ultérieure	Port HTTP/HTTPS du service Web	Ce port est requis lors de l'utilisation de la connexion SOAP pour PeopleSoft Enterprise for PeopleTools 8.46 et versions ultérieures

Configuration de la plateforme de BI et de PeopleSoft pour les pare-feu

Cette section explique comment configurer la plateforme de BI et PeopleSoft Enterprise afin qu'ils puissent fonctionner ensemble dans un scénario de déploiement dans lequel le pare-feu sépare le serveur d'applications Web des autres serveurs de la plateforme de BI.

Pour une configuration de pare-feu avec serveurs et clients de la plateforme de BI, voir le *Guide d'administration de la plateforme de Business Intelligence*.

Outre la configuration des pare-feu avec la plateforme de BI, vous devrez procédez à une configuration supplémentaire.

For PeopleSoft Enterprise : PeopleTools 8.46 ou version ultérieure

Ordinateur source	Port	Ordinateur de destination	Port	Action
CMS avec fonction Connectivité de la sécurité pour PeopleSoft	N'importe laquelle	PeopleSoft	Port HTTP /HTTPS du service Web PeopleSoft	Autoriser
Serveurs de la plateforme de BI avec la fonction Connectivité de données pour PeopleSoft	N'importe laquelle	PeopleSoft	Port HTTP /HTTPS du service Web PeopleSoft	Autoriser
Crystal Reports avec la fonction Connectivité de données côté client pour PeopleSoft	N'importe laquelle	PeopleSoft	Port HTTP /HTTPS du service Web PeopleSoft	Autoriser
Passerelle EPM	N'importe laquelle	CMS	Port du serveur de nom CMS	Autoriser
Passerelle EPM	N'importe laquelle	CMS	Port du CMS requis	Autoriser
Passerelle EPM	N'importe laquelle	Input File Repository Server	Port de l'Input FRS	Autoriser
Passerelle EPM	N'importe laquelle	PeopleSoft	Port de la base de données PeopleSoft	Autoriser

8.19.5 Configuration du pare-feu pour l'intégration Siebel

Cette section présente les ports spécifiques utilisés pour la communication entre les systèmes de la plateforme de BI et Siebel eBusiness Application lorsqu'ils sont séparés par des pare-feu.

- L'application Web doit être en mesure d'initier une communication avec le serveur de connexion de la plateforme de BI pour Siebel. Le serveur de connexion BusinessObjects Enterprise pour Siebel requiert trois ports :
  1. Le port Echo (TCP) 7 qui vérifie l'accès au serveur de connexion.
  2. Le port du serveur de connexion Enterprise pour Siebel (8448 par défaut) qui sert de port d'écoute CORBA IOR.
  3. Un port POA aléatoire de communication CORBA qui ne peut pas être contrôlé, donc tous les ports doivent être ouverts.
- Le CMS doit être en mesure d'initier une communication avec le serveur de connexion de la plateforme de BI pour Siebel. Un port d'écoute CORBA IOR configuré pour chaque serveur de connexion (par exemple 8448). Vous devrez également ouvrir un numéro de port POA aléatoire qui ne sera pas connu tant que vous n'aurez pas installé la plateforme de BI.
- Le serveur de connexion de la plateforme de BI pour Siebel doit être en mesure d'établir la communication avec le port SCBroker (Siebel connection broker), par exemple 2321.
- Les serveurs principaux de la plateforme de BI (composant Siebel Data Access) doivent être en mesure d'établir la communication avec le port SCBroker (Siebel connection broker), par exemple 2321.
- Crystal Reports (composant Siebel Data Access) doit être en mesure d'établir la communication avec le port SCBroker (Siebel connection broker), par exemple 2321.

Description détaillée des ports

Cette section répertorie les ports utilisés par la plateforme de BI. Si vous déployez la plateforme de BI avec des pare-feu, ces informations vous permettront d'ouvrir le nombre minimal de ports requis dans ces pare-feu spécifiquement pour l'intégration à Siebel.

Ports requis pour les serveurs de la plateforme de BI

Produit	Spécifications requises pour le port du serveur
Plateforme SAP BI	Port du serveur de connexion de la plateforme de BI

Configuration de port pour Siebel

Produit	Configuration de port	Description
Application Siebel eBusiness	2321	Port SCBroker (service Broker pour les connexions Siebel) par défaut

Configuration des pare-feu de la plateforme de BI pour l'intégration à Siebel

Cette section explique comment configurer les pare-feu pour Siebel et la plateforme de BI afin qu'ils puissent fonctionner ensemble dans un scénario de déploiement dans lequel le pare-feu sépare le serveur d'applications Web des autres serveurs de la plateforme.

Ordinateur source	Port	Ordinateur de destination	Port	Action
Serveur d'applications Web	N'importe laquelle	Serveur de connexion de la plateforme de BI pour Siebel	N'importe laquelle	Autoriser
CMS	N'importe laquelle	Serveur de connexion de la plateforme de BI pour Siebel	N'importe laquelle	Autoriser
Serveur de connexion de la plateforme de BI pour Siebel	N'importe laquelle	Siebel	Port SCBroker	Autoriser
Serveurs de la plateforme de BI avec connectivité de données côté serveur pour Siebel	N'importe laquelle	Siebel	Port SCBroker	Autoriser
Crystal Reports avec connectivité de données côté client pour Siebel	N'importe laquelle	Siebel	Port SCBroker	Autoriser

8.20 Plateforme de BI et serveurs proxy inverses

La plateforme de BI peut être déployée dans un environnement comportant un ou plusieurs serveurs proxy inverses. Les serveurs proxy inverses sont généralement déployés devant les serveurs d'applications Web afin de les masquer derrière une adresse IP unique. Cette configuration permet d'acheminer tout le trafic Internet adressé aux serveurs d'applications Web privés via le serveur proxy inverse, masquant ainsi les adresses IP privées.

Dans la mesure où le serveur proxy inverse traduit les URL publiques en URL internes, il doit être configuré avec les URL des applications Web de la plateforme de BI déployées sur le réseau interne.

8.20.1 Description du déploiement des applications Web

Les applications Web de la plateforme de BI sont déployées sur un serveur d'applications Web. Les applications sont déployées automatiquement durant l'installation par le biais de l'outil Wdeploy. L'outil peut également être utilisé pour déployer manuellement les applications après le déploiement de la plateforme de BI. Les applications Web se trouvent dans le répertoire suivant dans une installation Windows par défaut :

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps
```

WDeploy est utilisé pour déployer les fichiers WAR suivants :

- `BOE` : inclut la CMC (Central Management Console), la zone de lancement BI et OpenDocument
- `dswsbobje` : contient l'application de services Web.

Si le serveur d'applications Web se trouve derrière un serveur proxy inverse, ce dernier doit être configuré avec les chemins de contexte des fichiers WAR corrects. Pour exposer toutes les fonctionnalités de la plateforme de BI, configurez un chemin de contexte pour chaque fichier WAR de la plateforme de BI déployé.

8.21 Configuration des serveurs proxy inverses pour les applications Web de la plateforme de Business Intelligence

Le serveur proxy inverse doit être configuré de façon à mapper les demandes d'URL entrantes à l'application Web correcte dans les déploiements dans lesquels les applications Web de la plateforme de BI se trouvent derrière un serveur proxy inverse.

Cette section contient des exemples de configuration spécifiques s'appliquant à certains serveurs proxy inverses pris en charge. Pour en savoir plus, voir la documentation fournie avec le serveur proxy inverse.

8.21.1 Instructions détaillées relatives à la configuration des serveurs proxy inverses

Configurer les fichiers WAR

Les applications Web de la plateforme de BI sont déployées sous forme de fichiers WAR situés sur un serveur d'applications Web. Veillez à configurer une directive sur le serveur proxy inverse pour le fichier WAR requis par le déploiement. Vous pouvez utiliser WDeploy pour déployer les fichiers WAR `BOE` ou `dswbobje`. Pour en savoir plus sur WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme de BI*.

Spécifier les propriétés BOE dans le répertoire de configuration

Les fichiers `BOE.war` contiennent les propriétés générales et propres à l'application. Si vous devez modifier les propriétés, utilisez le répertoire de configuration personnalisé. Par défaut, le répertoire se trouve à l'emplacement `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> ⚠ Attention
>
> Pour éviter d'écraser les fichiers du répertoire par défaut, ne modifiez pas les propriétés dans le répertoire `config\default`. Les utilisateurs doivent utiliser le répertoire `personnalisé`.

> **Remarque**
>
> Sur certains serveurs d'applications Web comme la version Tomcat fournie avec la plateforme de BI, vous pouvez accéder directement au fichier `BOE.war`. Dans ce type de scénario, vous pouvez définir directement des paramètres personnalisés, sans annuler le déploiement du fichier WAR. Lorsque vous ne pouvez pas accéder au fichier `BOE.war`, vous devez annuler le déploiement du fichier, le personnaliser, puis le redéployer.

Utilisation cohérente des barres obliques (/)

Définissez les chemins de contexte dans le serveur proxy inverse de la même façon que dans une URL de navigateur. Par exemple, si la directive contient un caractère barre oblique (/) à la fin du chemin miroir sur le serveur proxy inverse, saisissez-en un à la fin de l'URL du navigateur.

Veillez à ce que le caractère « / » soit utilisé de façon cohérente dans l'URL source et l'URL de destination dans la directive du serveur proxy inverse. Si le caractère « / » est ajouté à la fin de l'URL source, il doit être placé au même endroit dans l'URL de destination.

8.21.2 Pour configurer le serveur proxy inverse

Les étapes indiquées ci-dessous sont requises pour que les applications Web de la plateforme de BI fonctionnent derrière un serveur proxy inverse pris en charge.

1. Assurez-vous que le serveur proxy inverse est correctement installé, selon les instructions du fournisseur et la topologie réseau du déploiement.
2. Indiquez quel fichier WAR de la plateforme de BI est nécessaire.
3. Configurez le serveur proxy inverse pour chaque fichier WAR de la plateforme de BI. Notez que les règles sont spécifiées différemment sur chaque type de serveur proxy inverse.
4. Effectuez les éventuelles configurations spéciales requises. Certaines applications Web requièrent une configuration spéciale lorsqu'elles sont déployées sur certains serveurs d'applications Web.

8.21.3 Pour configurer le serveur proxy inverse Apache 2.2 pour la plateforme de BI

Cette section fournit un workflow permettant de configurer la plateforme de BI et Apache 2.2 afin qu'ils puissent fonctionner ensemble.

1. Assurez-vous que la plateforme de BI et Apache 2.2 sont installés sur des ordinateurs distincts.
2. Assurez-vous qu'Apache 2.2 est installé et configuré en tant que serveur proxy inverse, tel que décrit dans la documentation du fournisseur.
3. Configurez le `ProxyPass` pour chaque fichier WAR déployé derrière le serveur proxy inverse.
4. Ouvrez le fichier *httpd.conf* situé dans le dossier d'installation du proxy inverse Apache.

5. Configurez le `ProxyPassReverseCookiePath` pour chaque application Web déployée derrière le serveur proxy inverse. Par exemple :

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.21.4 Pour configurer le serveur proxy inverse WebSEAL 6.0 pour la plateforme de BI

Cette section explique comment configurer la plateforme de BI et WebSEAL 6.0 afin qu'ils puissent fonctionner ensemble.

La méthode de configuration recommandée consiste à créer une jonction standard unique qui mappe toutes les applications Web de la plateforme de BI hébergées sur un serveur d'applications Web interne ou un serveur Web à un point de montage unique.

1. Assurez-vous que la plateforme de BI et WebSEAL 6.0 sont installés sur des ordinateurs distincts.

   Il est possible mais déconseillé de déployer la plateforme de BI et WebSEAL 6.0 sur le même ordinateur. Pour obtenir les instructions de configuration de ce scénario de déploiement, consultez la documentation fournie avec WebSEAL 6.0.
2. Assurez-vous que WebSEAL 6.0 est installé et configuré conformément à la documentation du fournisseur.
3. Lancez l'utilitaire de ligne de commande *pdadmin* de WebSeal. Connectez-vous à un domaine sécurisé tel que *sec_master* en tant qu'utilisateur doté des droits d'administration.
4. A l'invite de commande *pdadmin sec_master*, saisissez la commande suivante :

   ```
   server task <instance_name-webseald-host_name> create -t
   <type> -h <host_name> -p <port> <junction_point>
   ```

   Où :

   - `<nom_instance-nom_hôte-webseald>` désigne le nom de serveur complet de l'instance WebSEAL installée. Utilisez le même format pour ce nom de serveur complet que celui affiché dans la sortie de la commande `server list`.
   - `<type>` désigne le type de jonction. Utilisez `tcp` si la jonction mappe un port HTTP interne. Utilisez `ssl` si la jonction mappe un port HTTPS interne.
   - `<nom_hôte>` désigne le nom d'hôte DNS ou l'adresse IP du serveur interne qui reçoit les demandes.
   - `<port>` désigne le port TCP du serveur interne qui reçoit les demandes.
   - `<point_jointure>` désigne le répertoire de l'espace d'objets protégé WebSEAL dans lequel l'espace de documents du serveur interne est monté.

Exemple

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.21.5 Pour configurer Microsoft ISA 2006 pour la plateforme de BI

Cette section explique comment configurer la plateforme de BI et ISA 2006 afin qu'ils puissent fonctionner ensemble.

La méthode de configuration recommandée consiste à créer une jonction standard unique qui mappe tous les fichiers WAR de la plateforme de BI hébergés sur un serveur d'applications Web interne ou un serveur Web à un point de montage unique. Selon votre serveur d'applications Web, vous devez procéder à des configurations supplémentaires sur le serveur d'applications pour qu'il fonctionne avec ISA 2006.

1. Assurez-vous que la plateforme de BI et ISA 2006 sont installés sur des ordinateurs distincts.

   Il est possible mais déconseillé de déployer la plateforme de BI et ISA 2006 sur le même ordinateur. Pour obtenir les instructions de configuration de ce scénario de déploiement, consultez la documentation fournie avec ISA 2006.
2. Assurez-vous qu'ISA 2006 est installé et configuré selon la documentation du fournisseur.
3. Lancer l'utilitaire Gestion ISA Server.
4. Utilisez le panneau de navigation pour lancer une nouvelle règle de publication
   a. Accédez à

      Arrays > *MachineName* > *Firewall Policy* > *New* > *Web Site Publishing Rule* (Tableaux > NomOrdinateur > Stratégie de pare-feu> Nouvelle > Règle de publication Web)

      > **→ N'oubliez pas**
      >
      > Remplacez `MachineName` (nom de l'ordinateur) par le nom de l'ordinateur sur lequel est installé ISA 2006.

   b. Saisissez un nom de règle dans *Nom de la règle de publication Web* et cliquez sur *Suivant*.
   c. Sélectionnez *Autoriser* comme action de règle et cliquez sur *Suivant*.
   d. Sélectionnez *Publier un seul site Web ou un équilibreur de charge* et cliquez sur *Suivant*.
   e. Sélectionnez un type de connexion entre le ISA Server et le site Web publié, puis cliquez sur *Suivant*.

      Par exemple, sélectionnez *Utiliser une connexion non sécurisée pour la connexion au serveur Web publié ou à la batterie de serveurs*.
   f. Saisissez le nom interne du site Web que vous publiez (par exemple, le nom de l'ordinateur hébergeant la plateforme de BI) dans *Nom du site interne* et cliquez sur *Suivant*.

      > **ⓘ Remarque**
      >
      > Si l'ordinateur hébergeant ISA 2006 ne peut pas se connecter au serveur cible, sélectionnez *Utiliser un nom d'ordinateur ou une adresse IP pour établir la connexion avec le serveur publié* et saisissez le nom ou l'adresse IP dans le champ prévu à cet effet.

g. Dans *Informations sur les noms publics*, sélectionnez le nom de domaine (*N'importe quel nom de domaine*, par exemple) et spécifiez toutes les informations de publication interne (`/*`, par exemple). Cliquez sur *Suivant*.
Vous devez à présent créer un port d'écoute Web pour surveiller les requêtes Web entrantes.

5. Cliquez sur *Nouveau* pour lancer l'Assistant Nouveau port d'écoute Web.
   a. Saisissez un nom dans *Nom du port d'écoute Web* et cliquez sur *Suivant*.
   b. Sélectionnez un type de connexion entre ISA Server et le site Web publié, puis cliquez sur *Suivant*.

      Par exemple, sélectionnez *Do not require SSL secured connections with clients* (pas de connexions SSL sécurisées obligatoires avec les client).
   c. Dans la section *Adresses IP des ports d'écoute*, procédez aux sélections suivantes et cliquez sur *Suivant*.
      - Interne
      - Externe
      - Hôte local
      - Tous les réseaux

      ISA Server est à présent configuré pour publier uniquement via HTTP.
   d. Sélectionnez une option *Paramètre d'authentification*, cliquez sur *Suivant*, puis sur *Terminer*.
      Le nouveau port d'écoute est à présent configuré pour la règle de publication Web.
6. Cliquez sur *Suivant* dans *Ensembles d'utilisateurs*, puis cliquez sur *Terminer.*
7. Cliquez sur *Appliquer* pour enregistrer tous les paramètres de la règle de publication Web et actualiser la configuration d'ISA 2006.
   Vous devez maintenant actualiser les propriétés de la règle de publication Web pour mapper les chemins d'accès des applications Web.
8. Dans le panneau de navigation, cliquez avec le bouton droit de la souris sur la stratégie de pare-feu que vous avez configurée et sélectionnez *Propriétés*.
9. Dans l'onglet *Chemins*, cliquez sur *Ajouter* pour mapper les chemins d'accès aux applications Web SAP BusinessObjects.
10. Dans l'onglet *Nom public*, sélectionnez *Demande pour les sites Web suivants* et cliquez sur *Ajouter*.
11. Dans la boîte de dialogue *Nom public*, saisissez le nom de votre serveur ISA 2006 et cliquez sur *OK*.
12. Cliquez sur *Appliquer* pour enregistrer tous les paramètres de la règle de publication Web et actualiser la configuration d'ISA 2006.
13. Vérifiez la connexion en accédant à l'URL suivante :

    ```
    http://<Nom d'hôte ISA Server>:<numéro du port d'écoute Web>/<Chemin d'accès externe de l'application>
    ```

    Par exemple : `http://myISAserver:80/Product/BOE/CMC`

    > **Remarque**
    >
    > Vous devrez peut-être actualiser plusieurs fois le navigateur.

Pour être sûr que vous pourrez vous connecter à la CMC, vous devez modifier la stratégie HTTP de la règle que vous venez de créer. Cliquez avec le bouton droit de la souris sur la règle que vous avez créée dans l'utilitaire Gestion ISA Server, et sélectionnez *Configurer HTTP*. Désélectionnez à présent *Vérifier la normalisation* dans la zone *Protection des URL*.

Pour accéder à distance à la plateforme de BI, vous devez créer une règle d'accès.

8.22 Configuration spéciale de la plateforme de BI dans les déploiements de serveurs proxy inverses

Afin de pouvoir fonctionner correctement dans les déploiements de serveurs proxy inverses, certains produits de la plateforme de BI nécessitent une configuration supplémentaire. Cette section explique comment effectuer cette configuration supplémentaire.

8.22.1 Activation du proxy inverse pour les services Web

Cette section décrit les procédures requises pour activer les proxys inverses pour les services Web.

8.22.1.1 Pour activer le proxy inverse sur Tomcat

Pour activer le proxy inverse sur le serveur d'applications Web Tomcat, vous devez modifier le fichier `server.xml`. Les modifications requises comprennent l'affectation du port d'écoute du serveur proxy inverse au paramètre `proxyPort` et l'ajout d'un nouvel attribut `proxyName`. Cette section explique la procédure à suivre.

1. Arrêtez Tomcat.
2. Ouvrez le fichier `server.xml` pour Tomcat.

   Sous Windows, le fichier `server.xml` se trouve à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   Sous UNIX, le fichier `server.xml` se trouve dans le dossier `<RACINE_CATALINA>/conf`. La valeur par défaut de `<RACINE_CATALINA>` est `<REP_INSTALL>/sap_bobj/tomcat`.
3. Recherchez la section suivante dans le fichier server.xml :

```
<!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

4. Annulez la mise en commentaire de l'élément Connector en supprimant `<!--` et `-->`.
5. Remplacez la valeur de `proxyPort` par le port d'écoute du serveur proxy inverse.
6. Ajoutez un nouvel attribut `proxyName` à la liste des attributs de Connector. La valeur de `proxyName` doit être le nom du serveur proxy dont Tomcat doit déterminer l'adresse IP correcte.

Par exemple :

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
                <!--See proxy documentation for more information about using
                  this.-->
                <Connector port="8082"
                maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                enableLookups="false"
                acceptCount="100" debug="0"
connectionTimeout="20000"

proxyName="my_reverse_proxy_server.domain.com"
                proxyPort="ReverseProxyServerPort"
                disableUploadTimeout="true" />
```

Où `my_reverse_proxy_server.domain.com` et `ReverseProxyServerPort` doivent être remplacés par le nom de serveur et par le port d'écoute du proxy inverse.

7. Enregistrez et fermez le fichier `server.xml`.
8. Redémarrez Tomcat.
9. Vérifiez que le chemin virtuel du serveur proxy inverse est mappé au port du connecteur Tomcat adéquat. Dans l'exemple ci-dessus, il s'agit du port 8082.

   L'exemple suivant présente un exemple de configuration d'Apache HTTP Server 2.2 utilisé pour inverser le proxy des services Web SAP BusinessObjects™ déployés sur Tomcat :

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/
dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Pour activer les services Web, le nom de proxy et le numéro de port doivent être identifiés pour le connecteur.

8.22.1.2 Activation du proxy inverse pour les services Web sur des serveurs d'applications Web autres que Tomcat

La procédure suivante nécessite de configurer correctement les applications Web de la plateforme de BI en fonction du serveur d'applications Web choisi. Notez que les valeurs `wsresources` respectent la casse.

1. Arrêtez le serveur d'applications Web.
2. Indiquez l'URL externe des services Web dans le fichier `dsws.properties`.

   Ce fichier se trouve dans l'application Web `dswsbobje`. Par exemple, si votre URL externe est `http://mon_serveur_proxy_inverse.domaine.com/dswsbobje/`, mettez à jour les propriétés dans le fichier dsws.properties :

   - `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine`
   - `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
   - `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish`

- `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService`
- `wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform`
- `wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice`

3. Enregistrez le fichier `dsws.properties` et fermez-le.
4. Redémarrez le serveur d'applications Web.
5. Vérifiez que le chemin virtuel du serveur proxy inverse est mappé au port de connecteur du serveur d'applications Web adéquat. L'exemple suivant illustre une configuration d'Apache HTTP Server 2.2 utilisé pour inverser les proxys des services Web de la plateforme de BI déployés sur le serveur d'applications Web de votre choix :

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<port d'écoute> /dswsbobje
   ```

   ```
   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   Où `<port d'écoute>` correspond au port d'écoute de votre serveur d'applications Web.

8.22.2 Activation du chemin racine des cookies de session pour ISA 2006

Cette section décrit le mode de configuration des serveurs d'applications Web spécifiques pour activer le chemin racine des cookies de session pour assurer la compatibilité avec ISA 2006 comme serveur proxy inverse.

8.22.2.1 Configuration d'Apache Tomcat

Pour configurer le chemin racine de façon à ce que les cookies de session fonctionnent avec ISA 2006 comme serveur proxy inverse, ajoutez la chaîne suivante à l'élément `<Connector>` dans le fichier `server.xml` :

```
emptySessionPath="true"
```

1. Arrêtez Tomcat.
2. Ouvrez le fichier server.xml situé dans :

   `<CATALINA_HOME>\conf`
3. Localisez la section suivante dans le fichier server.xml :

   ```
   <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
   <!-- See proxy documentation for more information about using this -->
   <!--
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxS
   pareThreads="75" enableLookups="false"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyPort="80" disableUploadTimeout="true" />
   -->
   ```

4. Annulez la mise en commentaire de l'élément Connector en supprimant `<!--` et `-->`.
5. Pour configurer le chemin racine de façon à ce que les cookies de session fonctionnent avec ISA 2006 comme serveur proxy inverse, ajoutez la chaîne suivante à l'élément `<Connector>` dans le fichier `server.xml` :

```
emptySessionPath="true"
```

6. Remplacez la valeur de `proxyPort` par le port d'écoute du serveur proxy inverse.
7. Ajoutez un nouvel attribut `proxyName` à la liste des attributs de Connector. La valeur doit être le nom du serveur de proxy dont Tomcat doit déterminer l'adresse IP correcte.

   Par exemple :

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about using
this -->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. Enregistrez et fermez le fichier `server.xml`.
9. Redémarrez Tomcat.

Vérifiez que le chemin virtuel du serveur proxy inverse est mappé au port du connecteur Tomcat adéquat. Dans l'exemple ci-dessus, il s'agit du port 8082.

8.22.2.2 Pour configurer Sun Java 8.2

Vous devez modifier le fichier `sun-web.xml` pour chaque application Web de la plateforme de BI.

1. Accédez à `<<SUN_WEBAPP_DOMAIN>>`\generated\xml\j2ee-modules\webapps\BOE\WEB-INF
2. Ouvrez le fichier `sun-web.xml`.
3. Après le conteneur `<context-root>`, ajoutez les chaînes suivantes :

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
        </session-config>
   <property name="reuseSessionID" value="true"/>
```

4. Enregistrez et fermez le fichier `sun-web.xml`.
5. Répétez les étapes de 1 à 4 pour chaque application Web.

8.22.2.3 Pour configurer Oracle Application Server 10gR3

Vous devez modifier le fichier `global-web-application.xml` ou `orion-web.xml` pour chaque répertoire de déploiement de l'application Web de la plateforme de BI.

1. Accédez à `<ORACLE_HOME>>\j2ee\home\config\`
2. Ouvrez le fichier `global-web-application.xml` ou `orion-web.xml`.
3. Ajoutez la ligne suivante au conteneur `<orion-web-app>` :

```
<session-tracking cookie-path="/" />
```

4. Enregistrez le fichier de configuration et fermez-le.
5. Connectez-vous à Oracle Admin Console :
   a. Accédez à *OC4J:home* > *Administration* > *Server Properties* (Propriétés du serveur).
   b. Sélectionnez *Options* sous *Command Line Options* (Options de ligne de commande).
   c. Cliquez sur *Add another Row* (Ajouter une ligne) et saisissez la chaîne suivante :

```
Doracle.useSessionIDFromCookie=true
```

6. Redémarrez le serveur Oracle.

8.22.2.4 Pour configurer WebSphere Community Edition 2.0

1. Ouvrez WebSphere Community Edition 2.0 Admin Console.
2. Dans le panneau de navigation de gauche, recherchez *Server* (Serveur) et sélectionnez *Web Server* (Serveur Web).
3. Sélectionnez les connecteurs et cliquez sur *Modifier*.
4. Sélectionnez la case à cocher *emptySessionPath* et cliquez sur *Save* (Enregistrer).
5. Saisissez le nom de votre serveur ISA dans *ProxyName*.
6. Saisissez le numéro du port d'écoute ISA dans *ProxyPort*.
7. Arrêtez et redémarrez le connecteur.

8.22.3 Activation du proxy inverse pour SAP BusinessObjects Live Office

Pour activer la fonction Afficher l'objet dans le navigateur Web de SAP BusinessObjects Live Office pour les proxys inverses, modifiez l'URL du visualiseur par défaut. Pour ce faire, utilisez la Central Management Console (CMC) ou les options de Live Office.

> **Remarque**
>
> Cette section part du principe que vous avez activé des proxys inverses pour la zone de lancement BI et que les services Web de la plateforme de BI ont été activés avec succès.

8.22.3.1 Modification de l'URL du visualiseur par défaut dans la CMC

1. Connectez-vous à la CMC
2. Dans la page *Applications*, cliquez sur *Central Management Console*.
3. Sélectionnez *Actions* > *Paramètres de traitement*.
4. Dans le champ *URL*, sélectionnez l'URL du visualiseur par défaut approprié et cliquez sur *Enregistrer et fermer*.
   Par exemple :

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   `ReverseProxyServer` et `ReverseProxyServerPort` correspondent au nom du serveur proxy inverse et à son port d'écoute.

9 Authentification

9.1 Options d'authentification dans la plateforme de BI

L'authentification est un processus consistant à vérifier l'identité d'un utilisateur qui tente d'accéder au système, alors que la gestion des droits est un processus consistant à vérifier que des droits suffisants ont été octroyés à l'utilisateur pour exécuter l'action demandée sur l'objet spécifié.

Les plug-ins de sécurité développent et personnalisent la manière dont la plateforme de BI authentifie les utilisateurs. Ils facilitent la création et la gestion des comptes en permettant de mapper des comptes et des groupes d'utilisateurs de systèmes tiers dans la plateforme. Vous pouvez mapper des comptes ou des groupes d'utilisateurs tiers à des comptes ou des groupes d'utilisateurs de la plateforme de BI existants, ou créer de nouveaux comptes ou groupes d'utilisateurs Enterprise qui correspondent à chaque entrée mappée dans le système externe.

La version actuelle prend en charge les méthodes d'authentification suivantes :

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

La plateforme de BI étant entièrement personnalisable, l'authentification et les processus peuvent varier d'un système à l'autre.

9.1.1 Authentification primaire

L'authentification primaire intervient lorsqu'un utilisateur tente d'accéder pour la première fois au système. Les deux choses suivantes peuvent l'une ou l'autre se produire pendant une authentification primaire :

- Si la connexion unique n'est pas configurée, l'utilisateur fournit ses références de connexion, telles que son nom d'utilisateur, son mot de passe et le type d'authentification.
  Ces détails sont saisis par les utilisateurs sur l'écran de connexion.

  > **Remarque**
  >
  > Par défaut, seul le paramètre de mot de passe pour l'utilisation de caractères à casse mixte est activé, sauf si l'administrateur le modifie. Le mot de passe doit contenir au moins un caractère en majuscule et un caractère en minuscule. L'administrateur peut activer d'autres paramètres de mot de passe, si nécessaire.

- Si une méthode de connexion unique est configurée, les références de connexion des utilisateurs sont transmises de manière silencieuse.
  Ces détails sont extraits en utilisant d'autres méthodes, telles que Kerberos ou SiteMinder.

Il peut s'agir de l'authentification Enterprise, LDAP Windows AD, SAP Oracle EBS, Siebel, JD Edwards EntrepriseOne ou PeopleSoft Enterprise, selon le type d'authentification activé et configuré dans la zone de gestion Authentification de la CMC (Central Management Console). Le navigateur Web de l'utilisateur envoie les informations vers votre serveur Web via le protocole HTTP, qui les achemine à son tour vers le CMS ou le serveur de la plateforme approprié.

Le serveur d'applications Web transmet les informations sur l'utilisateur via un script côté serveur. En interne, ce script communique avec le SDK et, finalement, le plug-in de sécurité approprié pour authentifier l'utilisateur en fonction de la base de données utilisateur.

Par exemple, si l'utilisateur se connecte à la zone de lancement BI et spécifie l'authentification Enterprise, le SDK s'assure que le plug-in de sécurité de la plateforme de BI procède à l'authentification. Le CMS (Central Management Server) utilise le plug-in de sécurité pour vérifier le nom d'utilisateur et le mot de passe en fonction de la base de données système. Sinon, si l'utilisateur spécifie une méthode d'authentification différente, le SDK utilise le plug-in de sécurité correspondant pour authentifier l'utilisateur.

Si le plug-in de sécurité reconnaît les références de connexion, le CMS accorde à l'utilisateur une identité active sur le système, et les actions suivantes sont effectuées :

- Le CMS crée une session Enterprise pour l'utilisateur. Une fois active, cette session nécessite une licence utilisateur sur le système.
- Le CMS génère et code un jeton de connexion qu'il envoie au serveur d'applications Web.
- Le serveur d'applications Web stocke les informations de l'utilisateur en mémoire dans une variable de session. Une fois active, cette session stocke les informations qui permettent à la plateforme de BI de répondre aux requêtes de l'utilisateur.

  > ⓘ Remarque
  >
  > La variable de session ne contient pas le mot de passe de l'utilisateur.

- Le serveur d'applications Web conserve le jeton de connexion dans un cookie sur le navigateur du client. Ce cookie est uniquement utilisé à des fins de basculement, par exemple lorsque vous avez un CMS en cluster ou lorsque la zone de lancement BI est mise en cluster pour l'affinité de la session.

  > ⓘ Remarque
  >
  > Il est possible de désactiver le jeton de connexion. Néanmoins, si vous le faites, vous désactivez aussi le basculement.

9.1.2 Plug-ins de sécurité

Les plug-ins de sécurité développent et personnalisent la manière dont la plateforme de BI authentifie les utilisateurs. La plateforme de BI comprend actuellement les plug-ins suivants :

- Enterprise
- LDAP
- Windows AD

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Les plug-ins de sécurité facilitent la création et la gestion des comptes en permettant de mapper des comptes et des groupes d'utilisateurs de systèmes tiers à la plateforme de BI. Vous pouvez mapper des comptes ou des groupes d'utilisateurs tiers à des comptes ou des groupes d'utilisateurs de la plateforme de BI existants, ou créer de nouveaux comptes ou groupes d'utilisateurs Enterprise qui correspondent à chaque entrée mappée dans le système externe.

Les plug-ins de sécurité mettent dynamiquement à jour les listes d'utilisateurs et de groupes tiers. Ainsi, une fois que vous avez mappé un groupe externe à la plateforme de BI, tous les utilisateurs appartenant à ce groupe peuvent se connecter avec succès à la plateforme de BI. Lorsque vous apportez des modifications ultérieures à l'appartenance d'un groupe tiers, vous n'avez pas besoin d'actualiser la liste sur la plateforme de BI. Par exemple, si vous mappez un groupe LDAP à la plateforme de BI, puis que vous ajoutez un nouvel utilisateur au groupe, le plug-in de sécurité crée dynamiquement un alias pour ce nouvel utilisateur lorsque ce dernier se connecte pour la première fois à la plateforme de BI avec des références de connexion LDAP valides.

Par ailleurs, les plug-ins de sécurité vous permettent d'attribuer des droits aux utilisateurs et aux groupes de manière cohérente, car les utilisateurs et les groupes mappés sont considérés comme des comptes Enterprise. Par exemple, vous pouvez mapper des comptes et des groupes d'utilisateurs de Windows AD, et des comptes et des groupes d'utilisateurs d'un serveur de répertoires LDAP. Ensuite, lorsque vous devez attribuer des droits ou créer des groupes personnalisés sur la plateforme de BI, vous définissez tous vos paramètres dans la CMC.

Chaque plug-in de sécurité se comporte comme un fournisseur d'authentifications qui vérifie les références de connexion de l'utilisateur par rapport à la base de données utilisateur appropriée. Lorsque les utilisateurs se connectent à la plateforme de BI, ils choisissent parmi les types d'authentification disponibles que vous avez activés et configurés dans la zone de gestion Authentification de la CMC.

> ⓘ Remarque
>
> Le plug-in de sécurité Windows AD ne peut pas authentifier les utilisateurs si les composants du serveur de la plateforme de BI sont exécutés sous UNIX.

9.1.3 Connexion unique à la plateforme de BI

La connexion unique à la plateforme de BI signifie qu'une fois les utilisateurs connectés au système d'exploitation, ils peuvent accéder aux applications qui prennent en charge la connexion unique sans avoir à fournir de nouveau leurs références de connexion. Lorsqu'un utilisateur se connecte, un contexte de sécurité est créé pour cet utilisateur. Ce contexte peut être propagé à la plateforme de BI afin d'établir une connexion unique.

Le terme « connexion unique anonyme » désigne également la connexion unique à la plateforme de BI, mais il fait plus particulièrement référence à la fonction de connexion unique pour le compte utilisateur Guest. Lorsque le compte utilisateur Guest est activé par défaut, n'importe qui peut se connecter à la plateforme de BI en tant que Guest et obtient ainsi l'accès au système.

9.1.3.1 Prise en charge de la connexion unique

Le terme de connexion unique est utilisé pour décrire différents scénarios. Au sens le plus général, ce terme fait référence à une situation où l'utilisateur peut accéder à au moins deux applications ou systèmes tout en ne fournissant qu'une seule fois ses références de connexion, ce qui facilite l'interaction avec le système.

La connexion unique à la zone de lancement BI peut être fournie par la plateforme de BI ou par différents outils d'authentification en fonction du type de serveur d'applications et du système d'exploitation.

Ces méthodes de connexion unique sont disponibles si vous utilisez un serveur d'applications Java sous Windows :

- Windows AD avec Kerberos
- Windows AD avec SiteMinder

Ces méthodes de connexion unique sont disponibles si vous utilisez IIS sous Windows :

- Windows AD avec Kerberos
- Windows AD avec NTLM
- Windows AD avec SiteMinder

Ces méthodes de connexion unique sont disponibles sous Windows ou UNIX, quel que soit le serveur d'applications Web pris en charge par la plateforme.

- LDAP avec SiteMinder
- Authentification sécurisée
- Windows AD avec Kerberos
- LDAP via Kerberos sur SUSE 11
- Connexion unique SAP NetWeaver via l'authentification sécurisée

> **Remarque**
>
> Windows AD avec Kerberos est pris en charge si l'application Java se trouve sous UNIX. Cependant, les services de la plateforme de BI doivent s'exécuter sur un serveur Windows.

Le tableau suivant décrit les méthodes disponibles de prise en charge de la connexion unique pour la zone de lancement BI.

Mode d'authentification	Serveur CMS	Options	Remarques
Windows AD	Windows uniquement	Windows AD avec Kerberos uniquement	L'authentification Windows AD pour la zone de lancement BI et la CMC est prête à l'emploi.
LDAP	Toute plateforme prise en charge	Serveurs de répertoires LDAP pris en charge, avec SiteMinder uniquement	L'authentification LDAP pour la zone de lancement BI et la CMC est prête à l'emploi. La connexion unique à la zone de lancement BI et à la CMC nécessite SiteMinder.
Enterprise	Toute plateforme prise en charge	Authentification sécurisée	L'authentification Enterprise pour la zone de lancement BI et la CMC est

Mode d'authentification	Serveur CMS	Options	Remarques
			prête à l'emploi. La connexion unique avec l'authentification Enterprise à la zone de lancement BI et à la CMC requiert l'authentification sécurisée.

9.1.3.1.1 Activation de la connexion unique pour la CMC

Pour configurer la connexion unique sur la CMC, suivez les étapes mentionnées ci-dessous :

Du côté client, le cache doit être vidé avant la configuration initiale de la CMC. Sinon, la méthode d'authentification Enterprise sera mise en cache.

Sur le serveur Tomcat, suivez la procédure ci-dessous :

1. Sur un système où la connexion unique est déjà configurée pour BILP, accédez à `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom`.
2. Créez un fichier CmcApp.properties et mentionnez
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   dans ce fichier.
3. Redémarrez Tomcat.

   La connexion unique est activée pour la CMC.

> **Remarque**
>
> Après une expiration de session de la zone de lancement BI ou de la CMC, si la connexion unique est activée dans les deux cas, l'utilisateur est invité à se connecter. Lors de l'actualisation de la page, l'utilisateur est reconnecté sans avoir à fournir un mot de passe. Le ping ne doit pas être désactivé pendant le processus.

9.1.3.2 Connexion unique à la base de données

Une fois les utilisateurs connectés à la plateforme de BI, la connexion unique à la base de données leur permet d'effectuer des actions nécessitant un accès à la base de données, en particulier, l'affichage et l'actualisation de rapports, sans devoir fournir à nouveau leurs références de connexion. La connexion unique à la base de données peut être combinée à la connexion unique à la plateforme de BI pour permettre aux utilisateurs d'accéder encore plus facilement aux ressources dont ils ont besoin.

9.1.3.3 Connexion unique de bout en bout

La connexion unique de bout en bout fait référence à une configuration dans laquelle les utilisateurs disposent à la fois de la connexion unique à la plateforme de BI au niveau interface client et de la connexion unique aux bases de données. Ainsi, les utilisateurs ne doivent fournir leurs références de connexion qu'une seule fois, lorsqu'ils se connectent au système d'exploitation, pour accéder à la plateforme de BI et effectuer des actions requérant un accès à la base de données, telles que l'affichage de rapports.

Sur la plateforme de BI, la connexion unique de bout en bout est prise en charge par l'intermédiaire de Windows AD et de Kerberos.

9.2 Authentification Enterprise

9.2.1 Présentation de l'authentification Enterprise

L'authentification Enterprise est la méthode d'authentification par défaut de la plateforme de BI. Elle est automatiquement activée lorsque vous installez pour la première fois le système (elle ne peut pas être désactivée). Lorsque vous ajoutez et gérez des utilisateurs et des groupes, la plateforme de BI conserve des informations relatives à l'utilisateur et au groupe au sein de sa base de données.

> → Conseil
>
> Utilisez l'authentification système par défaut Enterprise si vous préférez créer des comptes et des groupes distincts à utiliser avec la plateforme de BI ou si vous n'avez pas encore configuré de hiérarchie d'utilisateurs et de groupes dans un serveur de répertoires tiers.
>
> Vous n'avez pas à configurer ni à activer l'authentification Enterprise. Vous pouvez cependant modifier les paramètres de l'authentification Enterprise pour répondre aux besoins de sécurité particuliers de votre organisation. Les paramètres d'authentification Enterprise peuvent être modifiés via la CMC (Central Management Console).

9.2.2 Paramètres d'authentification Enterprise

Paramètres	Options	Description
Restrictions relatives aux mots de passe	*Appliquer des mots de passe à casse mixte*	Cette option permet de s'assurer que les mots de passe contiennent au moins un caractère en majuscule et un caractère en minuscule.

Paramètres	Options	Description
		Remarque Par défaut, cette option est cochée. Au besoin, elle peut être décochée par l'administrateur.
	Appliquer les chiffres dans les mots de passe	Cette option permet de vérifier que les mots de passe comportent au moins un caractère numérique.
	Appliquer les caractères spéciaux dans les mots de passe	Cette option permet de vérifier que les mots de passe comportent au moins un caractère spécial.
	Doit contenir au moins N caractères où N est	Cette option permet de s'assurer que les mots de passe comportent au moins N caractères.
	Ne doit pas dépasser N caractères où N est	Cette option garantit que les mots de passe ne dépassent pas N caractères.
	Ne doit pas contenir les séquences de caractères suivantes :	Cette option garantit que le mot de passe ne doit pas contenir de séquences de caractères restreintes. La valeur par défaut est la suivante : Mot de passe 12345678 administrateur.
Restrictions relatives aux utilisateurs	*Doit changer de mot de passe tous les N jours*	Cette option permet que les mots de passe ne deviennent pas un problème et qu'ils soient actualisés régulièrement.
	Les N derniers mots de passe ne peuvent pas être réutilisés	Cette option permet que les mots de passe ne soient pas répétés par habitude.
	Le mot de passe peut être modifié après N minute(s)	Cette option permet que les nouveaux mots de passe ne puissent pas être modifiés immédiatement après leur saisie dans le système.
	Doit changer de mot de passe après N jour(s) d'inactivité	Cette option garantit que le mot de passe doit changer après N jour(s) d'inactivité.
	Doit changer le mot de passe initial après N jour(s) :	Cette option garantit que le mot de passe initial doit changer après N jour(s).
Restrictions relatives aux connexions	*Désactiver le compte après N échecs de connexion*	Cette option de sécurité spécifie le nombre de tentatives de connexion autorisées pour un utilisateur avant que son compte ne soit désactivé.
	Réinitialiser le nombre d'échecs de connexion après N minute(s)	Cette option spécifie un intervalle de temps avant la réinitialisation du compteur de tentatives de connexion.

Paramètres	Options	Description
	Réactiver le compte après N minute(s)	Cette option spécifie la durée pour laquelle un compte est suspendu après N échecs de tentative de connexion.
Synchroniser les références de connexion à la source de données lors de la connexion.	*Activer et mettre à jour les références de connexion à la source de données de l'utilisateur au moment de la connexion*	Cette option active les références de connexion aux sources de données après que l'utilisateur se soit connecté.
Authentification sécurisée	*L'authentification sécurisée est activée*	Fournit les paramètres de configuration de l'authentification sécurisée.
Authentification OpenID Connect	*L'authentification OpenID Connect est activée*	Pour activer l'*Authentification OpenID Connect*, cochez la case *L'authentification OpenID Connect est activée*. Lors de l'authentification via OpenID Connect, une session Enterprise interne est créée sur la plateforme de BI.

9.2.3 Modification des paramètres d'Enterprise

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Enterprise*.
   La boîte de dialogue *Enterprise* s'affiche.
3. Modifiez les paramètres.

   > → Conseil
   >
   > Pour remplacer tous les paramètres par les valeurs par défaut, cliquez sur *Réinitialiser*.

4. Cliquez sur *Mettre à jour* pour enregistrer vos modifications.

9.2.3.1 Pour modifier les paramètres généraux de mot de passe

> ⓘ Remarque
>
> Les comptes non utilisés pendant une longue période ne sont pas désactivés automatiquement. Les administrateurs doivent supprimer manuellement les comptes inactifs.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Enterprise*.
   La boîte de dialogue *Enterprise* s'affiche.
3. Activez la case à cocher pour chaque paramètre de mot de passe à utiliser et renseignez-la si nécessaire.

Le tableau suivant identifie les valeurs minimales et maximales pour chacun des paramètres concernant le mot de passe que vous pouvez configurer.

Paramètre de mot de passe	Par défaut	Valeur minimale	Valeur maximale recommandée
Ne doit pas contenir les séquences de caractères suivantes :	Mot de passe 12345678 administrateur	1 caractère	25 550 caractères
Doit comprendre N caractères au minimum	8 caractère	6 caractères	255 caractères
Ne doit pas dépasser N caractères	255 caractères	13 caractères	255 caractères
Doit changer de mot de passe tous les N jours	30 jours	2 jours	100 jours
Les N derniers mots de passe ne peuvent être réutilisés	3 mots de passe	1 mot de passe	100 mots de passe
Le mot de passe peut être modifié après N minute(s)	0 minutes	0 minutes	100 minutes
Doit modifier le mot de passe après N jour(s) d'inactivité :	20 jours	2 jours	365 jours
Doit changer le mot de passe initial après N jour(s)	7 jours	2 jours	15 jours
Désactiver le compte après N échecs de connexion	10 échec	1 échec	100 échecs
Réinitialiser le nombre d'échecs de connexion après N minute(s)	5 minutes	1 minute	100 minutes
Réactiver le compte après N minute(s)	5 minute	0 minute	100 minutes

4. Cliquez sur *Mettre à jour*.

9.2.4 Authentification SAML 2.0

9.2.4.1 Pour activer la connexion unique via SAML 2.0

Pour garantir la connexion unique, la plateforme de Business Intelligence peut maintenant être intégrée dans le portail ou l'application SAML de votre choix, sous forme de mécanisme d'authentification. Vous pouvez

ainsi vous connecter à une application Cloud telle qu'Analytics Hub ou SAP Analytics Cloud afin d'accéder aux ressources des applications BI telles que la zone de lancement BI façon Fiori et Open Document pendant la même session de connexion.

Vous devez configurer votre serveur d'applications pour bénéficier d'une connexion unique via SAML 2.0.

> **Remarque**
>
> Configurez les conditions préalables suivantes pour utiliser la fonctionnalité d'authentification SAML pour la connexion via une adresse électronique :
>
> - Utilisateurs tiers
> Utilisez le paramètre de ligne de commande `"-importtpemailduringsync"` pour importer des adresses électroniques à partir d'un système tiers :
> 1. Ajoutez le paramètre `"-importtpemailduringsync"` à *CMS* > *Propriétés* > *Paramètres de ligne de commande*.
> 2. Redémarrez le CMS.
> 3. Effectuez la mise à jour de l'authentification tierce du tiers dont vous souhaitez utiliser l'adresse électronique pour la connexion.
> Les types d'authentifications tierces pris en charge pour cette fonctionnalité sont SAP, LDAP et WinAD.
> - Utilisateurs Enterprise
> Voir la note SAP 2642247.

9.2.4.2 Configuration de la plateforme de BI comme fournisseur de services SAML

Pour utiliser la plateforme de BI comme fournisseur de services SAML, vous devez la configurer pour l'authentification SAML 2.0.

Dans cette version, les étapes de configuration d'un serveur d'applications comme fournisseur de services SAML ont été simplifiées. Dans le cadre de cette simplification, les étapes suivantes ont été supprimées :

- Copie des fichiers JAR SAML dans le répertoire d'installation de la plateforme de BI
- Modification du fichier securitycontext.xml
- Modification du fichier web.xml

Cela signifie que les fichiers JAR SAML, les balises XML pour chaque application Web dans le fichier securitycontext.xml et les filtres dans le fichier web.xml sont disponibles par défaut. Par conséquent, après avoir exécuté les étapes ci-dessous, vous pouvez activer ou désactiver l'authentification SAML 2.0 pour chaque application Web via le fichier de propriétés de chaque application Web.

> **Remarque**
>
> Utilisez un fournisseur d'identités SAP Cloud Identity comme fournisseur d'identités par défaut.

> **Remarque**
>
> Vous pouvez utiliser les serveurs d'applications Tomcat, WebSphere et JBoss comme fournisseur de services SAML.

1. Suivez la procédure expliquée dans Configuration de l'authentification sécurisée avec des sessions Web [page 252].
2. Si vous utilisez un fournisseur d'identités SAP Cloud Platform, exportez tous les utilisateurs, puis importez-les dans la plateforme de BI. Reportez-vous à How to import users in bulk from Central Management Console (Méthode d'importation en bloc d'utilisateurs à partir de la CMC).

   Pour exporter les utilisateurs SAP Cloud Platform dans un fichier CSV, reportez-vous à Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service (Exportation des utilisateurs existants d'un client du service SAP Cloud Platform Identity Authentication).
3. Modifiez le fichier de propriétés en modifiant `logon.webssoauthnetication.framework=None` par `logon.webssoauthnetication.framework=SAML`.
   - Pour la zone de lancement BI façon Fiori, accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` et modifiez le fichier `fioriBI.properties`.
   - Pour OpenDocument, accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` et modifiez le fichier `OpenDocument.properties`.
   - Pour la CMC, accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` et modifiez le fichier `CMCApp.properties`.

   > **Remarque**
   >
   > En plus d'ajouter `saml.enabled=true`, définissez la propriété `sso.supported.types = trustedSession` dans les fichiers de propriétés `CMC\FioriBI\OpenDocument`.
4. Pour mettre à jour les métadonnées du fournisseur d'identités SAML (IdP) dans SP, téléchargez d'abord les métadonnées de l'IdP à partir des fournisseurs de services IdP respectifs, puis copiez le fichier des métadonnées sur `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF` et renommez-le en `idp-meta-downloaded.xml`.

   Pour en savoir plus sur le téléchargement des métadonnées IdP, reportez-vous à Configuration du client SAML 2.0.

   > **Remarque**
   >
   > Si la plateforme de BI est déployée sur un ordinateur utilisant un système d'exploitation autre que Windows, vous devez modifier les séparateurs de chemin dans le chemin d'accès aux métadonnées de l'IdP sous le bean **FilesystemMetadataProvider** dans le fichier `securityContext.xml` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
   >
   > Par exemple, modifiez `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` en `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

   Si vous souhaitez générer un fichier de stockage des clés pour l'activation de SAML 2.0, reportez-vous à Génération d'un fichier de stockage des clés pour SAML 2.0 [page 253].
5. (Facultatif) Vous pouvez utiliser l'adresse électronique comme attribut d'assertion SAML. Pour en savoir plus, voir la rubrique Pour utiliser l'adresse électronique comme attribut d'assertion SAML [page 254].

6. (Facultatif) Si vous utilisez un équilibreur de charge ou un serveur proxy inverse, reportez-vous à 2621904 pour en savoir plus.
7. Créez le fichier WAR à l'aide de l'outil WDeploy.
   a. Accédez au chemin `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Utilisez la commande deploy appropriée pour créer le fichier war pour des versions spécifiques à l'application.

   - Pour Windows : `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`
   - Pour UNIX : `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

   > **Remarque**
   >
   > Vous devez remplacer <App_Server><Version_Name> par le type de serveur d'applications et sa version. Par exemple, vous pouvez utiliser tomcat8 pour le serveur d'applications Tomcat v8.0. De même, vous pouvez utiliser jboss7 pour le serveur d'applications JBoss v7.0 et websphere9 pour le serveur d'applications WebSphere v9.0.

8. Une fois que le fichier WAR est créé, copiez-le et déployez-le sur votre serveur d'applications.
9. Générez et chargez les métadonnées du fournisseur de services.

   > **Remarque**
   >
   > Vous pouvez définir l'URL de la base d'entité de la propriété dans le fichier securitycontext.xml pour générer les métadonnées du fournisseur de services avec votre URL du point de terminaison. Par défaut, le nom d'hôte et le numéro de port que vous fournissez dans l'URL sont pris en compte pour le téléchargement des métadonnées du fournisseur de services.

   a. Accédez à `http(s)://host:port/BOE/saml/metadata`.

      Le fichier XML est automatiquement téléchargé.
   b. Chargez le fichier XML vers le fournisseur d'identités. Si vous utilisez Microsoft Active Directory Federation Services comme fournisseur d'identités, consultez Création d'une approbation de partie de confiance [page 255] pour en savoir plus.

   > **Remarque**
   >
   > Vous pouvez utiliser le fichier de métadonnées du fournisseur de services par défaut `spring_saml_metadata.xml` qui se trouve sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` au lieu de le générer manuellement. Vous devez remplacer la balise XML`<replace_withip>` par l'adresse IP ou le nom d'hôte de l'ordinateur de votre réseau, et `<replace_withport>` par le numéro de port du serveur d'applications. Remplacez HTTP par HTTPS si vous avez activé HTTPS sur le serveur d'applications.

10. Si vous utilisez SAP Cloud Identity pour créer une application SAML dans l'IdP et charger le fichier `metadata.xml` de SP dans l'IdP pour configurer la connexion unique SAML sur la plateforme de BI, reportez-vous à Configure a Trusted Service Provider (Configuration d'un fournisseur de services de confiance).

    > **Remarque**
    >
    > Vous devez générer les métadonnées du fournisseur de services les plus récentes une fois que le fichier de stockage des clés a été modifié.

> → Conseil
>
> Pour vérifier si l'intégration SAML est réussie, vous allez être redirigé vers le fournisseur d'identités SAML après avoir lancé l'application SAML (zone de lancement BI, zone de lancement BI façon Fiori ou OpenDocument).

9.2.4.2.1 Configuration de l'authentification sécurisée avec des sessions Web

Vous devez configurer l'authentification sécurisée avec des sessions Web dans le cadre de la configuration d'un serveur d'applications comme fournisseur de services SAML.

> ⓘ Remarque
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

1. Créez le fichier `global.properties` dans le dossier personnalisé `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.
2. Saisissez ce qui suit comme contenu du fichier `global.properties` :

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```

   > ⓘ Remarque
   >
   > Assurez-vous de gérer les mêmes valeurs pour les paramètres `trusted.auth.user.param` et `trusted.auth.shared.secret` que dans le fichier *custom.jsp*.

3. Accédez à *CMC* > *Authentification* > *Entreprise*.
4. Définissez une valeur comprise entre 0 et 365 (*jours*) pour la *Validité*.
5. Cliquez sur *Nouveau secret partagé*.
6. Pour télécharger le secret partagé généré, sélectionnez *Télécharger le secret partagé*.

   Le fichier `TrustedPrincipal.conf` est téléchargé.
7. Copiez et collez le fichier `TrustedPrincipal.conf` dans `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` et dans `\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Accédez à *CMC* > *Authentification* > *Entreprise* et sélectionnez *Mettre à jour*.
9. Mettez le fichier custom.jsp à jour avec la valeur de la clé de secret partagé pour la zone de lancement BI classique et la zone de lancement BI façon Fiori. Pour en savoir plus, voir Modification du fichier custom.jsp [page 413].

> **Remarque**
>
> Vous devez mettre à jour le fichier custom.jsp si vous utilisez Microsoft ADFS et Microsoft Azure comme fournisseurs d'identités.

9.2.4.2.2 Génération d'un fichier de stockage des clés pour SAML 2.0

Pour utiliser votre propre fichier de stockage des clés pour SAML 2.0, vous devez le générer.

Les échanges SAML utilisent la cryptographie pour signer et chiffrer les données. Un exemple de fichier de stockage des clés auto-signé (`sampletestKeystore.jks`) est fourni avec le produit. Il est valide jusqu'au 18 octobre 2019. Le nom d'alias de `sampletestKeystore.jks` est **Testkey** et son mot de passe est **Password1**.

Vous pouvez maintenant générer un fichier de stockage des clés auto-signé à l'aide de l'utilitaire keytool de Java.

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Exécutez la commande : `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Commande	Description
-alias	Saisissez le nom d'alias du certificat.
-keypass	Saisissez le mot de passe du certificat.
-keystore	Nom du fichier de stockage des clés
-validity	Validité du certificat
numberofdays	Durée, en jours, de validité du certificat auto-signé.

Répondez aux questions suivantes après avoir exécuté la commande :

- Saisissez le mot de passe du fichier de stockage de clés : `*****`
- Confirmer le nouveau mot de passe : `*****`
- Quel est votre prénom et votre nom ? : **`MON_PRÉNOM_ET_NOM`**
- Quel est le nom de votre entité organisationnelle ? : **`MON_ENTITÉ_ORGANISATIONNELLE`**
- Quel est le nom de votre organisation ? : **`MON_ORGANISATION`**
- Quel est le nom de votre ville ? : **`MA_VILLE`**
- Quel est le nom de votre état ou de votre province ? : **`MON_ÉTAT`**
- Quel est le code-pays à deux lettres correspondant à cette entité ? : **`CODE_PAYS`**

Le fichier de stockage des clés est généré sous `INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.

3. Déplacez le fichier de stockage des clés dans `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
4. Modifiez le fichier `securityContext.xml` situé sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` en saisissant les nouveaux nom d'alias, mot de passe et nom de fichier de stockage des clés.

   Reportez-vous au code XML ci-dessous :

   Exemple de code

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

   Reportez-vous au tableau ci-dessous pour comprendre la commande :

Balise XML	Description
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Localise le fichier de stockage des clés
`<constructor-arg type="java.lang.String" value="Password1"/>`	Mot de passe du fichier de stockage des clés
`<entry key="aliasname" value="password"/>`	Mot de passe de l'alias
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Alias du certificat par défaut

9.2.4.2.3 Pour utiliser l'adresse électronique comme attribut d'assertion SAML

Vous pouvez activer l'authentification par adresse électronique sur SAML pour la zone de lancement BI façon Fiori, OpenDocument et la CMC (Central Management Console).

1. En fonction de l'application que vous utilisez, modifiez le fichier des propriétés en ajoutant les deux lignes suivantes :

```
saml.enabled=true
saml.isUseEmailAddress=true
```

```
saml.authType=secEnterprise
```

> **Remarque**
>
> `saml.isUseEmailAddress` utilise des valeurs booléennes, et `saml.authType` correspond au type d'authentification des détails de l'utilisateur/alias avec lesquels la connexion doit être exécutée. La fonctionnalité d'adresse électronique peut être gérée séparément pour chacune des applications mentionnées ci-dessus. Si `saml.isUseEmailAddress` est défini sur `false`, la connexion est exécutée sur la base du paramètre du nom. Si elle est définie sur `true`, la connexion est exécutée selon le paramètre d'adresse électronique. `saml.authType` contrôle les doublons potentiels et s'assure que deux alias avec le même type d'authentification ne peuvent pas avoir la même adresse électronique.

- Pour la zone de lancement BI façon Fiori, `fioriBI.properties` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Pour Opendocument, `OpenDocument.properties` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Pour la CMC, `CMCApp.properties` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

> **Remarque**
>
> Pour la CMC, assurez-vous de définir la propriété `sso.supported.types = trustedSession` dans le fichier `CMCApp.properties`.

2. Configurez le fournisseur d'identités pour la prise en charge des adresses électroniques. Vous pouvez également vous référer au Guide du service SAP Cloud Platform Identity Authentication pour en savoir plus si vous utilisez un fournisseur d'identités SAP Cloud Identity.
   a. Accédez à l'URL de la console d'administration du client pour le service SAP Cloud Platform Identity Authentication.

   > **Remarque**
   >
   > L'URL ressemble à : `https://<tenant ID>.accounts.ondemand.com/admin`. L'ID client est généré automatiquement par le système. Le premier administrateur créé pour le client reçoit un courrier électronique d'activation avec une URL contenant l'ID client.

   b. Sélectionnez *Applications*.
   c. Sélectionnez une application.
   d. Dans l'onglet *Confiance*, sous la section *SAML 2.0*, cliquez sur *Attribut d'ID de nom*.
   e. Sélectionnez *Courrier électronique*.
   f. Cliquez sur *Enregistrer*.

9.2.4.2.4 Création d'une approbation de partie de confiance

Vous devez créer une approbation de partie de confiance et une règle de revendication dans l'outil de gestion Microsoft ADFS pour mettre à jour les métadonnées du fournisseur de services.

1. Lancez le *Gestionnaire de serveur*.

2. Accédez à *Outils* > *Gestion AD FS*.
3. Développez *Relations d'approbation*.
4. Cliquez avec le bouton droit sur *Approbation de partie de confiance* et sélectionnez *Ajouter une approbation de partie de confiance*.
5. Dans l'assistant *Ajout d'approbation de partie de confiance*, sélectionnez *Démarrer*.
6. Sélectionnez *Importer les données concernant la partie de confiance à partir d'un fichier* et sélectionnez *Parcourir*.
7. Naviguez jusqu'au fichier des métadonnées du fournisseur de services téléchargé et sélectionnez-le.
8. Sélectionnez *Suivant*.
9. Saisissez le *Nom d'affichage* et sélectionnez *Suivant*.
10. À l'étape *Configurer l'authentification multifacteur maintenant ?*, sélectionnez *Suivant*.
11. Sélectionnez *Autoriser l'accès de tous les utilisateurs à cette partie de confiance* et sélectionnez *Suivant*.
12. Contrôlez les informations dans l'écran *Prêt à ajouter l'approbation* et sélectionnez *Suivant*.
13. Sélectionnez *Terminer*.
    La boîte de dialogue *Modifier les règles de revendication* apparaît. Vous pouvez créer des règles de revendication avec le nom d'utilisateur ou l'adresse électronique comme attribut.

Vous avez maintenant créé une approbation de partie de confiance.

9.2.4.2.4.1 Création d'une règle de revendication avec un nom d'utilisateur comme attribut

Vous pouvez créer une règle de revendication avec un nom d'utilisateur comme attribut d'assertion SAML

Une approbation de partie de confiance doit être disponible.

1. Dans la boîte de dialogue *Modifier les règles de revendication*, sélectionnez *Ajouter une règle*.
2. Dans l'*Assistant Ajout de règle de revendication de transformation*, sélectionnez *Envoyer les attributs LDAP en tant que revendications* et sélectionnez *Suivant*.
3. Saisissez le *nom de la règle de revendication*, puis sélectionnez *Active Directory* comme *Magasin d'attributs*.
4. Sous *Attribut LDAP*, sélectionnez *Nom de compte SAM*.
5. Sous *Type de revendication sortante*, sélectionnez *ID de nom*.
6. Sélectionnez *Terminer*.

La règle de revendication est créée avec le nom d'utilisateur comme attribut.

9.2.4.2.4.2 Création d'une règle de revendication avec une adresse électronique comme attribut

Vous devez créer deux règles de revendication pour utiliser l'adresse électronique comme attribut d'assertion SAML.

1. Dans la boîte de dialogue *Modifier les règles de revendication*, sélectionnez *Ajouter une règle*.

2. Dans l'*Assistant Ajout de règle de revendication de transformation*, sélectionnez *Envoyer les attributs LDAP en tant que revendications* et sélectionnez *Suivant*.
3. Saisissez le *nom de la règle de revendication*, puis sélectionnez *Active Directory* comme *Magasin d'attributs*.
4. Sous *Attribut LDAP*, sélectionnez *Adresses de messagerie* puis, sous *Type de revendication sortante*, sélectionnez *Adresse électronique*.
5. Dans la deuxième entrée, sous *Attribut LDAP*, sélectionnez *Prénom* puis, sous *Type de revendication sortante*, saisissez *Prénom*.
6. Sélectionnez *Terminer*.

   Vous avez créé la première règle. Suivez les étapes ci-dessous pour créer la deuxième règle de revendication.
7. Dans la boîte de dialogue *Modifier les règles de revendication*, sélectionnez *Ajouter une règle*.
8. Dans l'*Assistant Ajout de règle de revendication de transformation*, sélectionnez *Transférer une revendication entrante* et sélectionnez *Suivant*.
9. Saisissez le *nom de la règle de revendication*, sélectionnez *Adresse de messagerie* comme *Type de revendication entrante*, *ID de nom* comme *Type de revendication sortante*, et *Adresse de messagerie* comme *Format du nom sortant*.
10. Sélectionnez *Terminer*.

9.2.4.3 Pour utiliser le serveur d'applications WebSphere comme fournisseur de services SAML

Cette rubrique contient des instructions relatives à la configuration du serveur d'applications WebSphere pour l'authentification SAML 2.0.

> **Remarque**
>
> Les étapes mentionnées ci-après utilisent un fournisseur d'identités SAP Cloud Identity.

Suivez la procédure ci-dessous :

1. Copiez les fichiers JAR SAML présents sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\SAMLJARS` dans `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\lib`.
2. Pour configurer l'authentification sécurisée avec une session Web, procédez comme suit :
   1. Ajoutez le fichier global.properties dans le dossier personnalisé `<WebSphere_InstallDir>\WebSphere\\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom`. Voici le contenu du fichier global.properties :
      ```
      sso.enabled=true
      trusted.auth.user.retrieval=WEB_SESSION
      trusted.auth.user.param=UserName
      ```
   2. Accédez à *CMC* > *Authentification* > *Entreprise*.
   3. Activez l'option *Authentification sécurisée*.

4. Définissez la *Validité*.
5. Cliquez sur *Nouveau secret partagé*.
6. Pour télécharger le secret partagé généré, sélectionnez *Télécharger le secret partagé*.
   Le fichier `TrustedPrincipal.conf` est téléchargé.
7. Collez le fichier TrustedPrincipal.conf dans `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` et `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Accédez à *CMC* > *Authentification* > *Entreprise* et sélectionnez *Mettre à jour*.
9. Redémarrez le serveur d'applications WebSphere.

3. Si vous utilisez un fournisseur d'identités SAP Cloud Platform, exportez tous les utilisateurs, puis importez-les dans la plateforme de BI. Reportez-vous à la section Méthode d'importation en bloc d'utilisateurs à partir de la CMC.

   Pour exporter les utilisateurs SAP Cloud Platform dans un fichier CSV, consultez la section Exportation des utilisateurs existants d'un client du service SAP Cloud Platform Identity Authentication.

4. Modifiez le fichier de propriétés en ajoutant la ligne `saml.enabled=true`. Reportez-vous aux noms de fichier et aux emplacements ci-dessous :
   1. Pour la zone de lancement BI façon Fiori, accédez à `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` et modifiez le fichier *fioriBI.properties*.
   2. Pour OpenDocument, accédez à `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` et modifiez le fichier *OpenDocument.properties*.
   3. Pour la CMC, accédez à `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF\config\custom` et modifiez le fichier *CMCApp.properties*.

   > **Remarque**
   >
   > Pour la CMC, vous devez définir une autre propriété `sso.supported.types = trustedSession` dans le fichier *CMCApp.properties*.

   > **Remarque**
   >
   > Si l'application ne contient aucun fichier de propriétés personnalisé, créez-en un.

5. Pour mettre à jour les métadonnées IDP dans SP, téléchargez les métadonnées IDP à partir des fournisseurs de services IDP respectifs. Copiez le fichier de métadonnées dans `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF` et renommez-le en **idp-meta-downloaded.xml**. Pour de plus amples informations sur le téléchargement des métadonnées IDP, reportez-vous à la section Configuration du client SAML 2.0.

   > **Remarque**
   >
   > Un nouvel algorithme SHA-256 est maintenant pris en charge pour l'intégration SAML.

6. Redémarrez le serveur d'applications WebSphere.

> **Remarque**
>
> Si BOE est déployé sur n'importe quel ordinateur Windows, les séparateurs du chemin d'accès aux métadonnées de l'IDP sous le bean **FilesystemMetadataProvider** doivent être modifiés en `securityContext.xml` sous `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Nom>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF`.
>
> Par exemple, `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` doit être remplacé par `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

Pour générer un fichier de stockage des clés en vue de l'activation de SAML 2.0 (facultatif)

Cette étape s'applique uniquement si vous souhaitez utiliser votre propre fichier de stockage des clés.

Les échanges SAML impliquent l'utilisation d'une fonction de cryptographie pour la signature et le cryptage des données. Un exemple de fichier de stockage des clés auto-signé `sampletestKeystore.jks` est fourni avec le produit ; il est valide jusqu'au 18 octobre 2019. `sampletestKeystore.jks` inclut un nom d'alias `Testkey` et un mot de passe `Password1`. Vous pouvez maintenant générer un fichier de stockage des clés auto-signé à l'aide de l'utilitaire keytool de Java. Suivez les étapes ci-dessous pour générer un fichier de stockage des clés :

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Exécutez la commande : `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Commande	Description
-alias	Saisissez le nom d'alias du certificat.
-keypass	Saisissez le mot de passe du certificat.
-keystore	Nom du fichier de stockage des clés
-validity	Validité du certificat
numberofdays	Durée, en jours, de validité du certificat auto-signé.

Les invites et les questions suivantes s'affichent après l'exécution de la commande :

- Saisissez le mot de passe du fichier de stockage de clés : *****
- Confirmer le nouveau mot de passe : *****
- Quel est votre prénom et votre nom ? : <Prénom et nom>
- Quel est le nom de votre entité organisationnelle ? : <Nom du service>
- Quel est le nom de votre organisation ? : <Nom de l'entreprise>
- Quel est le nom de votre ville ? : <Nom de la ville>
- Quel est le nom de votre état et de votre province ? : <Nom de l'état ou de la province>

- Quel est le code-pays à deux lettres correspondant à cette entité ? : <Nom du pays ou code ISO>

3. Arrêtez le serveur d'applications WebSphere.
   Le fichier de stockage des clés est généré sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
4. Déplacez le fichier de stockage des clés vers `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF`
5. Modifiez le fichier `securityContext.xml` situé sous `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\WEB-INF` en saisissant les nouveaux nom d'alias, mot de passe et nom de fichier de stockage des clés. Reportez-vous au code XML ci-dessous :

   Exemple de code

   ```
   <bean id="keyManager"
   class="org.springframework.security.saml.key.JKSKeyManager">
   <constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
   <constructor-arg type="java.lang.String" value="Password1"/>
   <constructor-arg>
   <map>
   <entry key="aliasname" value="password"/>
   </map>
   </constructor-arg>
   <constructor-arg type="java.lang.String" value="Testkey"/>
   </bean>
   ```

   Reportez-vous au tableau ci-dessous pour comprendre les arguments :

Balise XML	Description
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Localise le fichier de stockage des clés.
`<constructor-arg type="java.lang.String" value="Password1"/>`	Mot de passe du fichier de stockage des clés.
`<entry key="aliasname" value="password"/>`	Mot de passe de l'alias
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Alias du certificat par défaut

7. Générez et chargez les métadonnées du fournisseur de services.
   1. Accédez à http(s)://host:port/BOE/saml/metadata. Le fichier XML est automatiquement téléchargé lorsque vous accédez à l'URL ci-dessus.
   2. Téléchargez le fichier XML vers le fournisseur d'identités.

> **Remarque**
>
> Vous pouvez utiliser le fichier de métadonnées du fournisseur de services par défaut `spring_saml_metadata.xml` situé à l'emplacement `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Profile_Name>\installedApps\<Node_Name>\BOE.ear\BOE.war\biprws\WEB-INF` au lieu de le générer manuellement. Vous devez remplacer la balise XML `<replace_withip>` par l'adresse IP ou le nom d'hôte de l'ordinateur de votre réseau, et `<replace_withport>` par le numéro de port du serveur d'applications WebSphere. Remplacez HTTP par HTTPS si vous avez activé les communications HTTPS sur le serveur WebSphere.

8. Si vous utilisez SAP Cloud Identity, pour créer une application SAML dans l'IDP et télécharger le fichier `metadata.xml` de SP dans l'IDP en vue de la configuration de la fonction de connexion unique SAML dans la plateforme de BI, reportez-vous à la rubrique Configuration d'un fournisseur de services approuvé.
9. Redémarrez le serveur d'applications WebSphere.

> **Remarque**
>
> Les métadonnées du fournisseur de services les plus récentes doivent être générées après la modification du fichier de stockage des clés.

> **→ Conseil**
>
> Pour vérifier si l'intégration SAML est réussie, après avoir lancé l'application SAML (zone de lancement BI, zone de lancement BI façon Fiori ou OpenDocument), vous êtes redirigé vers l'IDP.

9.2.5 Pour établir une authentification sécurisée entre SAP NetWeaver Java Application Server et la plateforme de BI

- SAP NetWeaver Java Application Server est configuré comme fournisseur de services pour l'authentification SAML 2.0.
- Un utilisateur doit exister dans SAP NetWeaver Java Application Server.
- Les certificats SAML 2.0 du fournisseur de services et du fournisseur d'identités sont échangés afin de configurer une communication sécurisée entre eux.
  Le même utilisateur doit être importé en tant qu'utilisateur Enterprise dans la plateforme de BI.

Pour établir une authentification sécurisée entre SAP NetWeaver Java Application Server et la plateforme de BI, procédez comme suit :

> **Remarque**
>
> - Vous devez utiliser la méthode `USER_PRINCIPAL` pour récupérer l'utilisateur lorsque vous activez l'authentification sécurisée pour les applications Web.
> - L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité,

les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

1. Générez une application Web BI à l'aide de l'outil WDeploy.
   a. Accédez à l'emplacement `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Exécutez la commande pour générer le fichier `BOE.sca` : `wdeploy.bat sapappsvr73 -DAPP=BOE predeploy`

      Le fichier `BOE.sca` est généré sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application`.
2. Activez l'authentification sécurisée en modifiant le fichier `web.xml`.
   a. Extrayez le fichier `BOE.sca` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application` à l'aide d'un outil tel que WinRAR ou WinZip.
   b. Copiez le fichier `BOE.sca` avant d'apporter des modifications. Dans le fichier `BOE.sca`, accédez à *DEPLOYARCHIVES* > *BOE.ear* > *BOE.war* > *WEB-INF*.
   c. Modifiez le fichier `web.xml` en ajoutant les balises XML ci-dessous avant `</web-app>`.

> **Remarque**
>
> Veillez à ajouter les rôles (mentionnés dans le code XML ci-dessous) dans SAP NetWeaver Java Application Server et à les affecter à un groupe d'utilisateurs ou à un utilisateur :
>
> - j2ee-admin
> - j2ee-guest
> - j2ee-special

Exemple de code

```
<security-constraint>
<web-resource-collection>
 <web-resource-name>InfoView</web-resource-name>
<url-pattern>*</url-pattern>
<http-method>DELETE</http-method>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>PUT</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>j2ee-admin</role-name>
<role-name>j2ee-guest</role-name>
<role-name>j2ee-special</role-name>
</auth-constraint>
<user-data-constraint>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
<realm-name>InfoView</realm-name>
</login-config>
<security-role>
<description>Assigned to the SAP J2EE Engine System Administrators</
description>
<role-name>j2ee-admin</role-name>
</security-role>
<security-role>
<description>Assigned to all users</description>
```

```
<role-name>j2ee-guest</role-name>
</security-role>
<security-role>
<description>Assigned to a special group of users</description>
<role-name>j2ee-special</role-name>
</security-role>
```

d. Créez un nouveau fichier XML `web-j2ee-engine.xml` avec les balises XML ci-dessous et enregistrez-le sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\WEB-INF`.

Exemple de code

```
<?xml version="1.0" encoding="UTF-8"?>
<web-j2ee-engine xsi:noNamespaceSchemaLocation="web-j2ee-engine.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<security-role-map>
    <role-name>j2ee-admin</role-name>
    <server-role-name>administrators</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-guest</role-name>
      <server-role-name>guests</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-special</role-name>
      <server-role-name>all</server-role-name>
</security-role-map>
 <login-module-configuration>
      <security-policy-domain>/irj</security-policy-domain>
 </login-module-configuration>
</web-j2ee-engine>
```

e. Enregistrez le fichier `web-j2ee-engine.xml`.

f. Faites glisser le fichier dans le dossier `WEB-INF` de l'archive `BOE.war`.

Activation de la connexion unique dans le fichier `Trustedprincipal.conf` de la plateforme de BI via la méthode USER_PRINCIPAL et un secret partagé

La méthode USER_PRINCIPAL permet d'activer la connexion unique en vue du transfert du nom d'utilisateur NW et du fichier `Trustedprincipal.conf` pour la transmission du secret partagé.

Pour activer l'authentification sécurisée et générer un secret partagé, procédez comme suit :

1. Accédez à *CMC* > *Authentification* > *Entreprise*.
2. Activez l'option *Authentification sécurisée*.
3. Cliquez sur *Créer un nouveau secret partagé*.
4. Sélectionnez *Télécharger le secret partagé* et enregistrez-le sur votre ordinateur BOE.
5. Sélectionnez *Mettre à jour*.
6. Sous `BOE.war/web-inf/config/default/folder`, extrayez le fichier suivant vers `BOE.war/web-inf/config/custom/folder` :
   - `global.properties`
7. Ajoutez le texte suivant dans le fichier `global.properties` :
   - `sso.enabled=true`
   - `trusted.auth.user.retrieval=USER_PRINCIPAL`
   - `trusted.auth.user.namespace.enabled=true`

- `trusted.auth.shared.secret=MySecret`

> **Remarque**
>
> Vous venez d'activer l'authentification sécurisée (trusted.auth.user.namespace.enabled=true).

Lors de la première tentative, vous devez recevoir le message d'erreur suivant : Connexion refusée : L'utilisateur "secExternal:samltest" est introuvable (FWB 00007). Une fonctionnalité de liaison automatique mappe `secExternal: samltest` en tant qu'alias à un utilisateur BOE. Connectez-vous normalement via le formulaire de connexion InfoView. Les informations d'identification BOE que vous utilisez incluent un alias `secExternal: samltest` créé spécialement Par exemple, si vous utilisez le compte utilisateur samltest, dans les propriétés utilisateur, vous pouvez constater que `secExternal: samltest` est affecté sous forme d'alias.

8. Accédez au fichier `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\WEB-INF\Eclipse\plugins\webpath.InfoView\web\custom.jsp`.
9. Ajoutez les balises XML ci-dessous au fichier `custom.jsp`.
   Bloc de code :

> **Exemple de code**
>
> ```
> <%@ page language="java" contentType="text/html;charset=utf-8"%>
> <%@ page
> import="com.businessobjects.bip.core.web.appcontext.RequestInfo"%>
> <%
>  request.getSession().setAttribute("MySecret","Your generated shared
> secret content");
> %>
>  <html>
> <head>
>     <title></title>
>  </head>
>     <body>
>    <script     type="text/javascript"     src="noCacheCustomResources/
> custom.js"></script>
>    <script     type="text/javascript">
>    window.location = "logon.faces";
>    </script>
>    </body>
> </html>
> ```

10. Enregistrez le fichier.

3. Mettez à jour le fichier d'archive et fermez-le.
4. Après avoir exécuté la procédure ci-dessus dans le fichier `BOE.sca`, déployez le fichier dans NetWeaver.
5. Une fois que vous avez déployé le fichier BOE.sca, lancez-le pour vérifier que son contenu est correct (http://<hostname>:<port_number>/nwa).
6. Lorsque l'authentification de base est déclarée dans le fichier `web.xml`, une fenêtre contextuelle d'authentification s'affiche.

   Vous venez d'établir une authentification sécurisée entre SAP NetWeaver Java Application Server et la plateforme de BI.

> **Remarque**
>
> Si une fenêtre contextuelle de navigateur s'affiche pour l'authentification, procédez comme suit :
>
> 1. Connectez-vous à SAP NetWeaver Java Application Server à l'adresse http://<hostname>:<port_number>/nwa.
> 2. Accédez à *Configuration* > *Sécurité* > *Authentification* > *Connexion unique* >.
> 3. Recherchez la configuration des règles de sécurité de l'application BI.
> 4. Basculez vers le mode *Édition*.
> 5. Dans l'onglet *Pile d'authentification*, laissez le champ *Modèle utilisé* vide et ajoutez *SAML2LoginModule* à la pile supérieure avec l'indicateur *SUFFISANT*.
> 6. Enregistrez vos modifications et fermez le fichier.

9.2.6 Pour utiliser l'authentification SAML 2.0 avec SAP NetWeaver Java Application Server

Pour autoriser les utilisateurs SAP NetWeaver Java Application Server à accéder au contenu de la plateforme SAP Business Intelligence via une connexion unique, un mécanisme permettant d'autoriser l'accès à ces applications doit être mis en place. Les étapes ci-dessous illustrent la procédure à suivre pour mettre en œuvre une authentification sécurisée entre SAP NetWeaver Java Application Server et Business Intelligence.

Portée : la portée de ces étapes n'inclut pas la configuration de l'authentification SAML, étant donné que l'IDP peut varier d'un fournisseur à l'autre. Reportez-vous aux documents spécifiques au fournisseur pour configurer l'authentification SAML.

La configuration inclut les étapes suivantes :

1. Configuration de l'authentification SAML dans SAP NetWeaver Java Application Server
2. Configuration de l'authentification sécurisée pour la plateforme de BI

Pour de plus amples informations sur l'activation de l'authentification SAML dans SAP NetWeaver Java Application Server, consultez la section Utilisation de SAML 2.0.

9.2.7 Activation de l'authentification sécurisée

L'authentification sécurisée d'Enterprise est utilisée pour effectuer une connexion unique en s'appuyant sur le serveur d'applications Web pour vérifier l'identité d'un utilisateur. Cette méthode d'authentification implique l'établissement d'une sécurité entre le CMS (Central Management Server) et le serveur d'applications Web hébergeant l'application Web de la plateforme de BI. Lorsque la sécurité est établie, le système abandonne la vérification de l'identité d'un utilisateur au serveur d'applications Web. L'authentification sécurisée peut être utilisée pour prendre en charge des méthodes d'authentification telles que SAML, x.509 et d'autres méthodes ne disposant pas d'un plug-in d'authentification propre.

Les utilisateurs préfèrent se connecter une fois au système et ne pas avoir à entrer leurs mots de passe plusieurs fois pendant une session. L'authentification sécurisée constitue une solution de connexion unique Java pour intégrer la solution d'authentification de votre plateforme de BI aux solutions d'authentification tierces. Les applications qui possèdent une sécurité établie avec le Central Management Server (CMS) peuvent

utiliser l'authentification sécurisée pour permettre aux utilisateurs de se connecter sans entrer leurs mots de passe.

Pour activer l'authentification sécurisée, vous devez configurer un secret partagé sur le serveur via les paramètres d'authentification d'Enterprise, alors que le client est configuré via les propriétés spécifiées pour le fichier WAR `BOE`.

> **Remarque**
>
> - Pour pouvoir utiliser l'authentification sécurisée, vous devez au préalable avoir créé des utilisateurs Enterprise ou mappé les utilisateurs tiers que vous utilisez pour établir la connexion à la plateforme de BI.
> - L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

Informations associées

Pour configurer le serveur de manière à utiliser l'authentification sécurisée [page 267]
Pour configurer l'authentification sécurisée pour l'application Web [page 272]

9.2.7.1 Authentification sécurisée pour les services Web RESTful sur le serveur Web

Cette rubrique fournit des instructions relatives à l'activation de l'authentification sécurisée pour les services Web RESTful sur le serveur Web.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

Suivez les étapes ci-après pour activer l'authentification sécurisée :

1. Générez une clé de secret partagé. Pour en savoir plus, voir Génération de la valeur d'un secret partagé [page 417].
2. Sous Windows, enregistrez la clé de secret partagé sur `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`.
3. Ouvrez la clé de secret partagé dans un éditeur de texte.

4. Copiez la clé de secret partagé.
5. 5. Copiez le fichier biprws.properties depuis `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps` et collez-le dans `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom`.
6. Ouvrez le fichier *biprws.properties* dans un éditeur de texte.
7. Collez la clé de secret partagé sur la valeur *Trusted_Auth_Shared_Secret=*.
8. Ajoutez la *Méthode d'extraction* et le *Paramètre du nom d'utilisateur*. Reportez-vous au tableau ci-dessous pour ajouter la méthode d'extraction et le paramètre du nom d'utilisateur.

   Service Web RESTful - propriétés de la configuration de l'authentification sécurisée

Propriété	Description	Valeur par défaut
Méthode d'extraction	Il s'agit d'un menu qui définit la méthode de requête qui doit être utilisée pour extraire les jetons de connexion à l'authentification sécurisée lors de l'utilisation de l'API du service Web RESTful `/logon/trusted`. • *HTTP_HEADER* est utilisé pour les requêtes GET avec l'en-tête de requête accept=application/xml (ou application/json). • *QUERY_STRING* est utilisé pour ajouter un nom de connexion à la fin d'une requête URL à l'aide de l'API du service Web RESTful, par exemple /logon/trusted/?user=johndoe. • *COOKIE* est utilisé lorsque le nom de connexion est extrait d'un cookie d'un navigateur Web. Le domaine, le nom, la valeur et le chemin doivent être stockés dans le cookie.	**HTTP_HEADER**
Paramètre du nom d'utilisateur	Il s'agit de l'étiquette utilisée pour identifier l'utilisateur sécurisé pour extraire un jeton de connexion.	**X-SAP-TRUSTED-USER**

9. Enregistrez le fichier *biprws.properties*.
10. Redémarrez le serveur Web.

9.2.7.2 Pour configurer le serveur de manière à utiliser l'authentification sécurisée

Pour pouvoir configurer l'authentification sécurisée, vous devez avoir créé des utilisateurs Enterprise ou mappé des utilisateurs tiers qui doivent se connecter à la plateforme de BI.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

1. Connectez-vous à la CMC
2. Accédez à la zone de gestion *Authentification*.

3. Cliquez sur l'option *Enterprise*.
   La boîte de dialogue *Enterprise* s'affiche.
4. Sous *Authentification sécurisée* :
   a. Cliquez sur *L'authentification sécurisée est activée*.
   b. Cliquez sur *Nouveau secret partagé*.
      Le message `La clé du secret partagé est générée et prête au téléchargement` s'affiche.
   c. Cliquez sur *Télécharger le secret partagé*.

      Le secret partagé est utilisé par le client et le CMS pour établir la fiabilité. Commencez par configurer le serveur, puis le client, pour l'authentification sécurisée.

      La boîte de dialogue de *téléchargement de fichier* s'affiche.
   d. Cliquez sur *Enregistrer* et enregistrez le fichier `TrustedPrincipal.conf` dans l'un des répertoires suivants :

      > ⚠ Attention
      >
      > Ne définissez pas l'expiration sur **`0`** (zéro). Une valeur **`0`** signifie que le décalage possible entre les deux horloges est illimité, ce qui peut augmenter la vulnérabilité aux attaques répétées.

   e. Dans le champ *Période de validité du secret partagé*, saisissez le nombre de jours de validité du secret partagé.
   f. Spécifiez la durée maximale, en millisecondes, de décalage entre l'horloge du client et l'horloge du CMS pour les demandes d'authentification sécurisée.
   g. Si vous comptez partager le secret via le fichier TrustedPrincipal.conf au lieu de la session Web, copiez-le sur l'un des répertoires suivants :

      - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
      - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
5. Cliquez sur *Mettre à jour* pour activer le secret partagé.

La plateforme de BI n'effectue pas d'audit sur toutes les modifications des paramètres de l'authentification sécurisée. Vous devez sauvegarder manuellement les informations de l'authentification sécurisée.

Le secret partagé est utilisé par le client et le CMS pour établir la fiabilité. L'étape suivante consiste à configurer le client pour l'authentification sécurisée.

9.2.8 Configuration de l'authentification sécurisée pour l'application Web

Pour configurer l'authentification sécurisée pour le client, vous devez modifier les propriétés globales du fichier `BOE.war` ainsi que les propriétés spécifiques de la zone de lancement BI et des applications OpenDocument.

Utilisez une des méthodes suivantes pour transmettre le secret partagé au client :

- Option `WEB_SESSION`
- Fichier `TrustedPrincipal.conf`

Employez une des méthodes suivantes pour transmettre le nom d'utilisateur au client :

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Quelle que soit le mode de transmission du secret partagé, la méthode utilisée doit être personnalisée dans les propriétés globales de `Trusted.auth.user.retrieval` pour le fichier `BOE.war`.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

9.2.8.1 Utilisation de l'authentification sécurisée pour la connexion unique SAML

Le SAML (Security Assertion Markup Language) est un standard XML pour la communication d'informations d'identité. Le SAML fournit une connexion sécurisée où l'identité et l'approbation sont communiquées par activation d'un mécanisme de connexion unique qui élimine les connexions supplémentaires pour les utilisateurs sécurisés tentant d'accéder à la plateforme de BI.

Activation de l'authentification SAML

Si votre serveur d'applications peut fonctionner comme fournisseur de service SAML, vous pouvez utiliser l'authentification sécurisée pour fournir la connexion unique SAML à la plateforme de BI.

Pour ce faire, vous devez d'abord configurer le serveur d'applications Web pour l'authentification SAML.

Vous devez aussi utiliser l'une de ces méthodes pour transmettre le nom d'utilisateur au client :

- `REMOTE_USER`
- `USER_PRINCIPAL`

Voici un exemple de fichier web.xml configuré pour l'authentification SAML :

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
```

```
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```

Veuillez vous référer à la documentation du serveur d'applications pour davantage d'instructions sur la manière de procéder car cela varie en fonction du serveur d'applications.

Utilisation de l'authentification sécurisée

Une fois configuré votre serveur d'applications pour fonctionner comme fournisseur de service SAML, vous pouvez utiliser l'authentification sécurisée pour fournir la connexion unique SAML.

La création dynamique d'alias est utilisée pour activer la connexion unique. Lorsqu'un utilisateur accède pour la première fois à la page de connexion via SAML, il est invité à se connecter manuellement à l'aide de ses références de compte existantes de la plateforme de BI. Une fois les références de connexion de l'utilisateur vérifiées, le système crée un alias entre l'identité SAML de l'utilisateur et son compte de plateforme de BI. Les tentatives ultérieures de connexion de l'utilisateur seront réalisées à l'aide de la connexion unique car le système aura fait correspondre dynamiquement l'alias d'identité de l'utilisateur avec un compte existant.

> **Remarque**
>
> Les utilisateurs doivent être importés sur la plateforme de BI ou disposer de comptes Enterprise.

> **Remarque**
>
> Une propriété spécifique pour le fichier BOE war (`trusted.auth.user.namespace.enabled`) doit être activée pour que ce mécanisme fonctionne.

9.2.8.2 Propriétés d'authentification sécurisée pour les applications Web

Le tableau suivant répertorie les paramètres d'authentification sécurisée dans les `global.properties` par défaut pour le fichier `BOE.war`. Pour remplacer les paramètres, créez un fichier dans `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

Propriété	Valeur par défaut	Description
`sso.enabled=true`	`sso.enabled=false`	Active et désactive la connexion unique (SSO) à la plateforme de BI. Définissez sur `true` pour activer l'authentification sécurisée.
`trusted.auth.shared.secret`	Aucune	Nom de variable de session utilisé pour extraire le secret pour l'authentification sécurisée. Uniquement d'application si la session Web est utilisée pour transmettre le secret partagé.
`trusted.auth.user.param`	Aucune	Spécifie la variable utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée.
`trusted.auth.user.retrieval`	Aucune	Spécifie la méthode utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée : • `REMOTE_USER` • `HTTP_HEADER` • `COOKIE` • `QUERY_STRING` • `WEB_SESSION` • `USER_PRINCIPAL` Ne définissez aucune valeur pour désactiver l'authentification sécurisée.
`trusted.auth.user.namespace.enabled`	Aucune	Active et désactive la liaison dynamique des alias aux comptes utilisateur existants. Si le paramètre est défini sur `true`, l'authentification sécurisée utilise la liaison d'alias pour authentifier les utilisateurs sur

Propriété	Valeur par défaut	Description
		plateforme de BI. Avec la liaison d'alias, votre serveur d'applications peut fonctionner comme un fournisseur de service SAML, en activant l'authentification sécurisée pour fournir une connexion unique SAML au système. Si le paramètre est vide, l'authentification sécurisée utilisera la correspondance de noms lors de l'authentification des utilisateurs.

9.2.8.3 Pour configurer l'authentification sécurisée pour l'application Web

Si vous avez l'intention de stocker le secret partagé dans le fichier `TrustedPrincipal.conf`, assurez-vous de stocker le fichier dans le répertoire de plateforme approprié :

Plateforme	Emplacement du fichier TrustedPrincipal.conf
Windows, installation par défaut	• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86`

Il existe plusieurs mécanismes remplissant la variable de nom d'utilisateur utilisée pour configurer l'authentification sécurisée pour le client hébergeant des applications Web. Configurez votre serveur d'applications Web de façon à ce que les noms d'utilisateur soient exposés avant d'utiliser les méthodes d'extraction du nom d'utilisateur. Pour en savoir plus, voir http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html .

Pour configurer l'authentification sécurisée pour le client, vous devez accéder au fichier `BOE.war` et en modifier les propriétés globales, y compris les propriétés générales et spécifiques de la zone de lancement BI et des applications Web OpenDocument.

> **Remarque**
>
> En fonction de la méthode que vous comptez utiliser pour extraire le nom d'utilisateur ou le secret partagé, il peut exister des étapes supplémentaires.

1. Accédez au dossier "custom" du fichier `BOE.war` sur l'ordinateur hébergeant les applications Web :

   `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Vous devez ensuite redéployer le fichier `BOE.war` modifié.
2. Créez un fichier à l'aide de Notepad ou d'un autre éditeur de texte.
3. Entrez les propriétés d'authentification sécurisée suivantes :

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
trusted.auth.shared.secret=<Secret Variable>
```

   Pour la propriété `trusted.auth.user.retrieval`, sélectionnez l'une des options suivantes pour l'extraction du nom d'utilisateur :

Option	Mode d'extraction du nom d'utilisateur
`HTTP_HEADER`	Le nom d'utilisateur est extrait du contenu d'un en-tête HTTP. Vous spécifiez l'en-tête HTTP à utiliser dans la propriété `trusted.auth.user.param`.
`QUERY_STRING`	Le nom d'utilisateur est extrait d'un paramètre de l'URL de la requête. Vous spécifiez la chaîne de requête à utiliser dans la propriété `trusted.auth.user.param`.
`COOKIE`	Le nom d'utilisateur est extrait d'un cookie défini. Vous spécifiez le cookie à utiliser dans la propriété `trusted.auth.user.param`.
`WEB_SESSION`	Le nom d'utilisateur est extrait du contenu d'une variable de session définie. Vous spécifiez la variable de session Web à utiliser dans la propriété `trusted.auth.user.param` du fichier `global.properties`.
`REMOTE_USER`	Le nom d'utilisateur est extrait d'un appel à `HttpServletRequest.getRemoteUser()`.
`USER_PRINCIPAL`	Le nom d'utilisateur est extrait d'un appel à `getUserPrincipal().getName()` sur l'objet `HttpServletRequest` pour la requête en cours dans un servlet ou un fichier JSP.

> → Recommandation
>
> Lorsque vous utilisez la connexion unique basée sur HTTP_HEADER ou sur QUERY_STRING, assurez-vous que les utilisateurs finaux (navigateurs) n'accèdent pas directement à BOE pour s'authentifier. Au lieu de cela, SAP recommande que les utilisateurs finaux (navigateurs) accèdent à BOE via le portail ou l'application personnalisée.

> **Remarque**
>
> Certains serveurs d'applications Web nécessitent que la variable d'environnement `REMOTE_USER` soit définie sur `true` sur le serveur. Pour déterminer si cela est nécessaire, consultez la documentation de votre serveur d'applications Web. Si cela est nécessaire, confirmez que la variable d'environnement est définie sur `true`.

> **Remarque**
>
> Si vous utilisez `USER_PRINCIPAL` ou `REMOTE_USER` pour transmettre le nom d'utilisateur, laissez vide le paramètre `trusted.auth.user.param`.

4. Enregistrez le fichier sous le nom `global.properties`.
5. Redémarrez le serveur d'applications Web.

Les nouvelles propriétés s'appliquent uniquement lorsque l'application Web BOE est redéployée sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

9.2.8.3.1 Exemples de configuration

9.2.8.3.1.1 Pour transmettre le secret partagé par le biais du fichier TrustedPrincipal.conf

Les informations utilisateur sont stockées et transmises par le biais de la session Web, le secret partagé est transmis via le fichier `TrustedPrincipal.conf`, qui se trouve par défaut dans le répertoire `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. La version fournie de Tomcat constitue le serveur d'applications Web.

1. Dans le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`, créez un fichier avec Notepad ou tout autre éditeur de texte.
2. Pour spécifier les paramètres de l'authentification sécurisée, saisissez les valeurs suivantes :

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
```

3. Enregistrez le fichier sous le nom **`global.properties`**.
4. Localisez le fichier `custom.jsp` dans le dossier `web` du fichier `com.businessobjects.webpath.InfoView.jar` à l'emplacement `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
5. Insérez le code Java personnalisé dans le fichier `custom.jsp` dans le fichier `com.businessobjects.webpath.InfoView.jar` :

```
<%
```

```
//custom Java code
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> **Remarque**
>
> Dans l'extrait de code ci-dessus, la variable <Nom d'utilisateur> doit être un utilisateur Entreprise valide sur la plateforme de BI.

6. Redémarrez le serveur d'applications Web.
7. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web.

   Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

Pour vérifier si vous avez correctement configuré l'authentification sécurisée, utilisez l'URL suivante pour accéder à la zone de lancement BI : `http://<[nom_cms]>:8080/BOE/BI/custom.jsp` où `<[nom_cms]>` désigne le nom de l'ordinateur hébergeant le CMS. Vous êtes invité à saisir votre nom d'utilisateur et votre mot de passe la première fois. Une fois l'authentification réussie, vous êtes automatiquement redirigé vers la zone de lancement BI.

9.2.8.3.1.2 Pour transmettre le secret partagé par le biais de la variable de session Web

Les informations utilisateur et le secret partagé seront stockés et transmis via une variable de session Web. Ouvrez le fichier TrustedPrincipal.conf qui a précédemment été enregistré et notez le contenu du fichier. Dans cet exemple de configuration, il est supposé que le secret partagé est le suivant :

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

La version fournie de Tomcat constitue le serveur d'applications Web.

1. Accédez au répertoire suivant :

   `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Créez un fichier dans un éditeur de texte.
3. Spécifiez les propriétés de l'authentification sécurisée en saisissant les éléments suivants :

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```
4. Enregistrez le fichier sous le nom suivant :

   `global.properties`
5. Accédez au fichier suivant :

   Zone de lancement BI classique : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`

   Zone de lancement BI façon Fiori : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.FioriBI\web\custom.jsp`

6. Modifiez le contenu du fichier pour inclure les éléments suivants :

```
<%
//custom Java code
request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
6a3f1345285b55a0a7");
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> **Remarque**
>
> Dans l'extrait de code ci-dessus, la variable <Nom d'utilisateur> doit être un utilisateur Entreprise valide sur la plateforme de BI.

7. Redémarrez le serveur d'applications Web.
8. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web.

   Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

Pour vérifier si vous avez correctement configuré l'authentification sécurisée, utilisez l'URL suivante pour accéder à l'application de zone de lancement BI : `http://[nom_cms]:8080/BOE/BI/custom.jsp` où [nom_cms] est le nom de l'ordinateur hébergeant le CMS. Vous êtes invité à saisir votre nom d'utilisateur et votre mot de passe la première fois. Une fois l'authentification réussie, vous êtes automatiquement redirigé vers la zone de lancement BI.

9.2.8.3.1.3 Pour transmettre le nom d'utilisateur par le biais de l'utilisateur principal

L'exemple de configuration suivant suppose qu'un utilisateur nommé « JohnDoe » a été créé sur la plateforme de BI.

Les informations utilisateur sont stockées et transmises par le biais de l'option Utilisateur principal, le secret partagé est transmis via le fichier `TrustedPrincipal.conf`, qui se trouve par défaut dans le répertoire `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` . La version fournie de Tomcat constitue le serveur d'applications Web.

1. Arrêtez le serveur Tomcat.
2. Ouvrez le fichier `server.xml` pour Tomcat, situé par défaut dans le répertoire `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
3. Recherchez l'entrée `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>`, et remplacez-la par la valeur suivante :

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. Ouvrez le fichier `tomcat-users.xml`, situé par défaut dans le répertoire `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
5. Cherchez la balise `<tomcat-users>` et modifiez la valeur suivante :

   ```
   <user name=« JohnDoe » password=« password »
   ```

```
roles=« onjavauser »/>
```

6. Ouvrez le fichier `web.xml` dans le répertoire `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
7. Avant la balise `</web-app>`, ajoutez les valeurs suivantes :

```
<security-constraint>
    <web-resource-collection>
         <web-resource-name>OnJavaApplication</web-resource-name>
         <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
         <role-name>onjavauser</role-name>
    </auth-constraint>
</security-constraint>
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>OnJava Application</realm-name>
</login-config>
```

   Saisissez une page spécifique pour le paramètre `<url-pattern></url-pattern>`. Habituellement, cette page n'est pas l'URL par défaut de la zone de lancement BI ni d'aucune autre application Web.
8. Dans le fichier personnalisé `global.properties`, saisissez les valeurs suivantes :

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

   > **Remarque**
   >
   > La configuration de `trusted.auth.user.namespace.enabled=true` est facultative. Ajoutez le paramètre lorsque vous voulez mapper un nom d'utilisateur externe à un nom d'utilisateur de la plateforme de BI différent.
9. Redémarrez le serveur d'applications Web.
10. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web.

    Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

Les configurations sur le serveur d'applications Web sont les mêmes que si vous utilisiez la méthode Utilisateur distant.

Pour vérifier si vous avez correctement configuré l'authentification sécurisée, utilisez l'URL suivante pour accéder à la zone de lancement BI : `http://<[nom_cms]>:8080/BOE/BI` où `<[nom_cms]>` désigne le nom de l'ordinateur hébergeant le CMS. Après un moment, une boîte de dialogue de connexion s'affiche.

9.3 Authentification LDAP

9.3.1 Utilisation de l'authentification LDAP

Cette section fournit une description générale du fonctionnement de l'authentification LDAP avec la plateforme de BI. Elle présente ensuite les outils d'administration qui vous permettent de gérer et de configurer les comptes LDAP sur la plateforme.

Lorsque vous installez la plateforme de BI, le plug-in d'authentification LDAP est installé automatiquement, mais n'est pas activé par défaut. Vous devez tout d'abord vérifier que votre répertoire LDAP est configuré afin d'utiliser l'authentification LDAP. Pour obtenir davantage d'informations sur LDAP, reportez-vous à la documentation relative à LDAP.

Le protocole LDAP (Lightweight Directory Access Protocol), un répertoire commun indépendant de toute application, permet aux utilisateurs de partager des informations entre plusieurs applications. Basé sur un standard ouvert, LDAP fournit un moyen d'accéder et de mettre à jour des informations dans un répertoire.

LDAP est basé sur le standard X.500, qui utilise un protocole d'accès aux répertoires (DAP) pour communiquer entre un client répertoire et un serveur d'annuaire. LDAP est une alternative à DAP car il utilise moins de ressources, simplifie et omet certaines opérations et fonctions X.500.

La structure de répertoires dans LDAP se compose d'entrées organisées selon un schéma spécifique. Chaque entrée est identifiée par un nom distinctif correspondant (DN) ou un nom commun (CN). Les autres attributs communs incluent le nom d'unité de l'organisation (OU) et le nom de l'organisation (O). Par exemple, un groupe de membres peut se trouver dans une arborescence de répertoires comme suit : cn=Utilisateurs de la plateforme de BI, ou=Utilisateurs Enterprise A, o=Recherche. Consultez votre documentation LDAP pour plus d'informations.

LDAP étant indépendant de toute application, tout client disposant des privilèges appropriés peut accéder à ses répertoires. LDAP offre la possibilité de configurer des utilisateurs pour se connecter à la plateforme de BI par le biais de l'authentification LDAP. Il fournit aux utilisateurs des droits d'accès aux objets du système. Tant que vous disposez d'un serveur (ou de serveurs) LDAP en cours d'exécution, et que vous utilisez LDAP dans vos systèmes existants reliés en réseau, vous pouvez utiliser l'authentification LDAP (en même temps que les authentifications Enterprise et Windows AD).

Si vous le souhaitez, le plug-in de sécurité LDAP fourni avec la plateforme de BI peut communiquer avec votre serveur LDAP via une connexion SSL établie à l'aide d'une authentification serveur ou d'une authentification mutuelle. Dans le cadre d'une authentification serveur, le serveur LDAP possède un certificat de sécurité que la plateforme de BI utilise pour vérifier si elle approuve le serveur, tandis que le serveur LDAP autorise les connexions depuis des clients anonymes. Dans le cadre d'une authentification mutuelle, le serveur LDAP et la plateforme de BI disposent de certificats de sécurité et le serveur LDAP doit également vérifier le certificat client pour qu'une connexion puisse être établie.

Le plug-in de sécurité LDAP fourni avec la plateforme de BI peut être configuré de manière à communiquer avec votre serveur LDAP via SSL, mais il effectue toujours une authentification de base lors de la vérification des références de connexion des utilisateurs. Avant de déployer l'authentification LDAP conjointement avec la plateforme de BI, assurez-vous que vous êtes familiarisé avec les différences entre ces types d'authentification LDAP. Pour en savoir plus, voir RFC2251, à présent disponible à l'adresse http://www.faqs.org/rfcs/rfc2251.html .

Informations associées

Configuration de l'authentification LDAP [page 279]
Mappage des groupes LDAP [page 291]

9.3.1.1 Plug-in de sécurité LDAP

Le plug-in de sécurité LDAP vous permet de mapper des comptes et des groupes d'utilisateurs de votre serveur de répertoires LDAP vers la plateforme de BI ; il permet également au système de vérifier toutes les demandes de connexion qui spécifient l'authentification LDAP. Les utilisateurs sont authentifiés par rapport au serveur de répertoire LDAP et leur appartenance à un groupe LDAP mappé est vérifiée avant que le CMS ne leur accorde une session de plateforme de BI active. Les listes d'utilisateurs et les appartenances à des groupes sont mises à jour dynamiquement par le système. Si vous souhaitez renforcer la sécurité, vous pouvez spécifier que la plateforme doit utiliser une connexion SSL (Secure Sockets Layer) pour communiquer avec le serveur d'annuaire LDAP.

L'authentification LDAP pour la plateforme de BI est similaire à l'authentification Windows AD en ce sens que vous pouvez mapper des groupes et configurer l'authentification, les droits d'accès et la création d'alias. En outre, comme dans l'authentification NT ou AD, vous pouvez créer des comptes Enterprise pour les utilisateurs LDAP existants et attribuer des alias LDAP aux utilisateurs existants si les noms d'utilisateur correspondent aux noms d'utilisateur Enterprise. En outre, vous pouvez procéder aux opérations suivantes :

- Mapper les utilisateurs et les groupes depuis le service de répertoire LDAP.
- Mapper LDAP par rapport à AD. Un certain nombre de restrictions s'appliquent si vous configurez LDAP par rapport à AD.
- Spécifier des noms d'hôtes multiples et les ports associés.
- Configurer LDAP avec SiteMinder.

Une fois que vous avez mappé vos utilisateurs et vos groupes LDAP, tous les outils client de la plateforme de BI prennent en charge l'authentification LDAP. Vous pouvez également créer vos propres applications prenant en charge l'authentification LDAP.

Informations associées

Configuration des paramètres SSL pour l'authentification mutuelle ou l'authentification du serveur LDAP [page 284]
Mappage de LDAP par rapport à Windows AD [page 293]
Configuration du plug-in LDAP pour SiteMinder [page 288]

9.3.2 Configuration de l'authentification LDAP

Pour simplifier la gestion, la plateforme de BI prend en charge l'authentification LDAP pour les comptes d'utilisateurs et de groupes. Pour que les utilisateurs puissent utiliser leur nom d'utilisateur et leur mot de passe LDAP afin de se connecter au système, vous devez mapper leur compte LDAP à la plateforme de BI. Lorsque vous mappez un compte LDAP, vous pouvez choisir de créer un compte ou d'établir un lien vers un compte de la plateforme de BI existant.

Avant de configurer et d'activer l'authentification LDAP, vérifiez que le répertoire LDAP est configuré. Pour en savoir plus, reportez-vous à la documentation relative à LDAP.

La configuration de l'authentification LDAP comprend les tâches suivantes :

- Configuration de l'hôte LDAP
- Préparation du serveur LDAP pour SSL (si nécessaire)
- Configuration du plug-in LDAP pour SiteMinder (si nécessaire)

> ⓘ Remarque
>
> Si vous configurez LDAP par rapport à AD, vous pourrez mapper vos utilisateurs, mais vous ne serez pas en mesure de configurer une connexion unique AD ou une connexion unique à la base de données. Cependant, les méthodes de connexion unique LDAP telles que SiteMinder et l'authentification sécurisée seront toujours disponibles.

9.3.2.1 Pour configurer l'hôte LDAP

Il est conseillé d'installer et d'exécuter le serveur LDAP avant de configurer l'hôte LDAP.

1. Dans la liste de navigation, sélectionnez *Authentification* pour accéder à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *LDAP*.
3. Si vous configurez l'authentification LDAP pour la première fois, cliquez sur *Démarrer l'Assistant de configuration LDAP*.
4. Saisissez le nom et le numéro de port de vos hôtes LDAP dans le champ *Ajouter un hôte LDAP (nomhôte:port)* (par exemple, "monserveur:123"), cliquez sur *Ajouter*, puis sur *Suivant*.

   > → Conseil
   >
   > Répétez cette étape pour ajouter d'autres hôtes LDAP appartenant au même type de serveur, qui feront office de serveurs de basculement. Si vous voulez supprimer un hôte, mettez en surbrillance le nom de l'hôte et cliquez sur *Supprimer*.

5. Sélectionnez votre type de serveur dans la liste *Type de serveur LDAP*.

   > ⓘ Remarque
   >
   > Si vous mappez LDAP à AD, sélectionnez le type de serveur *Serveur d'applications Microsoft Active Directory*.

6. Si vous souhaitez afficher ou modifier les mappages des attributs du serveur LDAP ou les attributs de recherche LDAP par défaut, cliquez sur *Afficher les mappages des attributs*.

   Par défaut, les mappages des attributs du serveur et les attributs de recherche de chaque type de serveur pris en charge sont définis.
7. Cliquez sur *Suivant*.
8. Dans le champ *Nom distinctif LDAP de base*, saisissez le nom distinctif (par exemple, o=UneBase) du serveur LDAP, puis cliquez sur *Suivant*.
9. Dans la zone *Références d'administration du serveur LDAP*, indiquez le nom distinctif et le mot de passe d'un compte utilisateur disposant d'un accès en lecture au répertoire.

   Les références d'administrateur ne sont pas requises.

   Si votre serveur LDAP permet la liaison anonyme, ne renseignez pas cette zone. Les serveurs et les clients de la plateforme de BI se connecteront à l'hôte principal via une connexion anonyme.

10. Si vous avez configuré des références sur l'hôte LDAP, saisissez les informations d'authentification dans la zone *Références de connexion LDAP*, puis saisissez le nombre de tronçons de référence dans le champ *Nombre maximal de tronçons de référence*.

    Vous devez configurer la zone *Références LDAP* si tous les critères suivants s'appliquent :

    - L'hôte principal a été configuré pour faire référence à un autre serveur d'annuaire qui traite les requêtes concernant les entrées dans une base spécifiée.
    - L'hôte auquel il est fait référence a été configuré de manière à ne pas autoriser la liaison anonyme.
    - Un groupe de l'hôte auquel il est fait référence sera mappé à la plateforme de BI.

    > **Remarque**
    >
    > Les groupes peuvent être mappés à partir de plusieurs hôtes mais seul un ensemble de références de connexion peut être défini. Par conséquent, si vous disposez de plusieurs hôtes de référence, vous devez créer un compte d'utilisateur sur chaque hôte qui utilise les mêmes nom distinctif et mot de passe.

    > **Remarque**
    >
    > Si le *Nombre maximal de tronçons de référence* est défini sur zéro, aucune référence n'est autorisée.

11. Cliquez sur *Suivant*.
12. Sélectionnez le type d'authentification SSL (Secure Sockets Layer) utilisé :
    - *De base (non SSL)*
    - *Authentification du serveur*
    - *Authentification mutuelle*

    Les informations et prérequis pour l'authentification du serveur et l'authentification mutuelle sont abordés dans une section ultérieure. Pour configurer l'authentification LDAP à l'aide d'un des types de SSL, consultez *Configuration des paramètres SSL pour l'authentification mutuelle ou l'authentification du serveur LDAP* dans ce document avant de poursuivre la procédure.
13. Cliquez sur *Suivant*, puis sélectionnez un mode d'authentification de connexion unique LDAP :
    - *De base (pas de connexion unique)*
    - *SiteMinder*
14. Cliquez sur *Suivant*, puis sélectionnez le mode de mappage des alias et utilisateurs aux comptes de la plateforme de BI.
    a. Dans la zone *Options de nouvel alias*, sélectionnez le mode de mappage des nouveaux alias aux comptes Enterprise :
       - *Affecter à un même compte chaque alias LDAP ajouté*
         Utilisez cette option lorsque vous savez que certains utilisateurs possèdent un compte Enterprise portant le même nom ; cela signifie que les alias LDAP seront affectés aux utilisateurs existants (la création d'alias automatique est activée). Les utilisateurs dépourvus de compte Enterprise, ou ne portant pas le même nom dans leur compte Enterprise et LDAP, sont ajoutés en tant que nouveaux utilisateurs.
       - *Créer un nouveau compte pour chaque alias LDAP ajouté*
         Utilisez cette option pour créer un compte pour chaque utilisateur.

    b. Dans la zone *Options de mise à jour des alias*, sélectionnez le mode de gestion des mises à jour des alias pour les comptes Enterprise :
       - *Créer de nouveaux alias lors de la mise à jour des alias*

Utilisez cette option pour créer automatiquement un nouvel alias pour chaque utilisateur LDAP mappé à la plateforme de BI. De nouveaux comptes LDAP sont ajoutés pour les utilisateurs dépourvus de comptes de la plateforme de BI, ou pour tous les utilisateurs si vous avez sélectionné l'option *Créer un nouveau compte pour chaque alias LDAP ajouté*.

- *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
  Sélectionnez cette option si l'annuaire LDAP que vous mappez contient de nombreux utilisateurs dont seulement quelques-uns utiliseront la plateforme de BI. Le système ne crée pas automatiquement d'alias ni de comptes Enterprise pour tous les utilisateurs. Il crée plutôt des alias (et des comptes, le cas échéant) uniquement pour les utilisateurs qui se connectent à la plateforme de BI.

c. Dans la zone *Options de nouvel utilisateur*, indiquez le nombre d'utilisateurs créés :

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
  Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

  > **Remarque**
  >
  > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
  >
  > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
  Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs à la plateforme, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

15. Suivez cette étape si vous configurez des mappages d'attributs utilisateur ou si vous prévoyez d'importer des adresses électroniques depuis le serveur LDAP. Dans la zone *Options de liaison d'attributs*, spécifiez la priorité de liaison d'attributs pour le plug-in AD :

    a. Cliquez dans la zone *Importer le nom complet, l'adresse électronique et d'autres attributs*.
    Les noms complets et les descriptions des comptes LDAP sont importés et stockés avec les objets utilisateur dans le système.

    b. Spécifiez une option pour *Rendre la liaison d'attributs LDAP prioritaire par rapport aux autres liaisons d'attributs*.

    > **Remarque**
    >
    > Si l'option est définie sur 1, les attributs LDAP sont prioritaires dans les scénarios où LDAP et les autres plug-ins (Windows AD et SAP) sont activés. Si l'option est définie sur 3, les attributs des autres plug-ins sont prioritaires.

16. Cliquez sur *Terminer*.

Informations associées

Configuration des paramètres SSL pour l'authentification mutuelle ou l'authentification du serveur LDAP [page 284]
Configuration du plug-in LDAP pour SiteMinder [page 288]

9.3.2.2 Gestion des hôtes LDAP multiples

Lors de l'utilisation de LDAP et de la plateforme de BI, vous pouvez rendre votre système tolérant aux pannes en ajoutant plusieurs hôtes LDAP. Le système utilise comme hôte LDAP principal le premier hôte que vous ajoutez. Les hôtes suivants sont traités en tant qu'hôtes de basculement.

L'hôte LDAP principal et tous les hôtes de basculement doivent être configurés exactement de la même façon, et chaque hôte LDAP doit faire référence à tous les autres hôtes à partir desquels vous souhaitez mapper des groupes. Pour obtenir davantage d'informations sur les hôtes et les références LDAP, reportez-vous à la documentation relative à LDAP.

Pour ajouter plusieurs hôtes LDAP, saisissez-les lorsque vous configurez LDAP à l'aide de l'Assistant de configuration LDAP (voir pour plus d'informations). Si vous avez déjà configuré LDAP, vous pouvez accéder à la zone de gestion Authentification de la Central Management Console puis cliquer sur l'onglet LDAP. Dans la zone Résumé de la configuration du serveur LDAP, cliquez sur le nom de l'hôte LDAP pour ouvrir la page qui vous permet d'ajouter ou de supprimer des hôtes.

> ⓘ Remarque
>
> Assurez-vous d'ajouter en premier l'hôte principal, suivi des autres hôtes de basculement.

> ⓘ Remarque
>
> Si vous recourez à des hôtes LDAP de basculement, vous ne pouvez pas utiliser le niveau le plus élevé de sécurité SSL (en d'autres termes, vous ne pouvez pas sélectionner l'option "Accepter le certificat du serveur s'il provient d'une autorité de certification fiable et si l'attribut CN du certificat correspond au nom d'hôte DNS du serveur").

Informations associées

Configuration de l'authentification LDAP [page 279]

9.3.2.3 Configuration des paramètres SSL pour l'authentification mutuelle ou l'authentification du serveur LDAP

Cette section contient des informations détaillées sur l'authentification mutuelle ou l'authentification du serveur LDAP par SSL. La configuration d'une authentification par SSL requiert des étapes préliminaires. Cette section fournit aussi des informations spécifiques à la configuration SSL avec l'authentification mutuelle et l'authentification du serveur LDAP dans la CMC. Il est supposé que vous avez configuré l'hôte LDAP et que vous avez sélectionné l'une des options suivantes pour votre authentification SSL.

Pour en savoir plus ou pour obtenir des informations sur la configuration du serveur hôte LDAP, reportez-vous à la documentation de votre fournisseur LDAP.

Pour les systèmes Windows, la communication SSL par défaut utilisent TLS 1.2. Pour les systèmes Linux, veuillez vous référer à la note SAP 2623529.

Informations associées

Pour configurer l'hôte LDAP [page 280]

9.3.2.3.1 Pour configurer l'authentification serveur ou mutuelle LDAP

Ressources	Effectuez les actions suivantes avant de démarrer cette tâche
Certificat CA	Cette action est requise pour l'authentification serveur et mutuelle avec SSL. 1. Obtenez la génération d'un certificat CA par une autorité de certification. 2. Ajoutez le certificat à votre serveur LDAP. Pour en savoir plus, voir la documentation de votre fournisseur de contenus LDAP.
Certificat de serveur	Cette action est requise pour l'authentification serveur et mutuelle avec SSL. 1. Demandez puis générez un certificat de serveur. 2. Autorisez le certificat, puis ajoutez-le au serveur LDAP.
cert7.db ou cert8.db, key3.db	Ces fichiers sont requis pour l'authentification serveur et mutuelle avec SSL. 1. Téléchargez l'application certutil qui génère un fichier `cert7.db` ou `cert8.db` (selon vos besoins) depuis l'adresse : https://developer.mozilla.org/en-US/docs/NSS/tools .

Ressources	Effectuez les actions suivantes avant de démarrer cette tâche

	2. Copiez le certificat CA dans le même répertoire que l'application certutil.
	3. Utilisez la commande suivante pour générer les fichiers `cert7.db` ou `cert8.db`, `key3.db` et `secmod.db` :
	`certutil -N -d .`
	4. Utilisez la commande suivante pour ajouter le certificat CA au fichier `cert7.db` ou `cert8.db` :
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. Stockez les trois fichiers dans un répertoire de l'ordinateur hébergeant la plateforme de BI.

cacerts	Ce fichier est requis pour l'authentification mutuelle avec SSL pour les applications Java, comme la zone de lancement BI. 1. Recherchez le fichier `keytool` dans votre répertoire `bin` Java. 2. Utilisez la commande suivante pour créer le fichier `cacerts` : `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. Stockez le fichier `cacerts` dans le même répertorie que les fichiers `cert7.db` ou `cert8.db` et `key3.db`.
Certificat client	1. Créez des demandes client distinctes pour les fichiers `cert7.db` ou `cert8.db` et `.keystore` : • Pour configurer le plug-in LDAP, utilisez l'application certutil pour générer une demande de certificat client. • Utilisez la commande suivante pour générer la demande de certificat client : `certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .` `<client_dn>` inclut des informations telles que "CN=`<client_name>`, OU=`<org unit>`, O=`<Companyname>`, L=`<city>`, ST=`<province>`, and C=`<country>`. 2. Utilisez le CA pour authentifier la demande de certificat. Utilisez la commande suivante pour

Ressources	Effectuez les actions suivantes avant de démarrer cette tâche

	retrouver le certificat et l'insérer dans le fichier `cert7.db` ou `cert8.db` :
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. Pour faciliter l'authentification Java avec SSL :
	• Utilisez l'utilitaire keytool dans le répertoire Java `bin` pour générer une demande de certificat client.
	• Utilisez la commande suivante pour générer une paire clé :
	`keytool -genkey -keystore .keystore`
	4. Après avoir spécifié les informations sur votre client, utilisez la commande suivante pour générer une demande de certificat client :
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. Une fois la demande de certificat client authentifiée par l'autorité de certification (CA), utilisez la commande suivante pour ajouter le certificat CA au fichier `.keystore` :
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Extrayez la demande de certificat client de l'autorité de certification (CA) et utilisez la commande suivante pour l'ajouter au fichier `.keystore` :
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Stockez le fichier `.keystore` dans le même répertoire que les fichiers `cert7.db` ou `cert8.db` et `cacerts` sur l'ordinateur hébergeant la plateforme de BI.

1. Sélectionnez le niveau de sécurité SSL à utiliser.

   Si vous utilisez l'Assistant de configuration LDAP pour configurer l'authentification LDAP pour la première fois, sélectionnez *Authentification mutuelle* dans la liste *Type d'authentification SSL*, puis cliquez sur *Suivant*. Sinon, si vous reconfigurez la configuration de l'authentification LDAP, accédez à la zone *Authentification* de la CMC, puis cliquez deux fois sur *LDAP*. La page *Résumé de la configuration du serveur LDAP* s'affiche. Cliquez sur la valeur *Type SSL*, puis sélectionnez *Authentification mutuelle* dans la liste *Type d'authentification SSL*.

   - *Toujours accepter le certificat du serveur*

Cette option offre le niveau de sécurité le plus faible. Avant que la plateforme de BI ne puisse établir une connexion SSL avec l'hôte LDAP (pour authentifier les utilisateurs et groupes LDAP), elle doit recevoir et vérifier un certificat de sécurité envoyé par l'hôte LDAP. La plateforme de BI ne vérifie pas le certificat qu'elle reçoit.

- *Accepter le certificat du serveur s'il provient d'une autorité de certification fiable*
  Cette option offre un niveau de sécurité moyen. Avant que la plateforme de BI ne puisse établir une connexion SSL avec l'hôte LDAP (pour authentifier les utilisateurs et groupes LDAP), elle doit recevoir et vérifier un certificat de sécurité envoyé par l'hôte LDAP. Pour vérifier le certificat, le système doit rechercher l'autorité de certification ayant émis le certificat dans sa base de données des certificats.
- *Accepter le certificat du serveur s'il provient d'une autorité de certification fiable et si l'attribut CN du certificat correspond au nom d'hôte DNS du serveur*
  Cette option offre le niveau de sécurité le plus élevé. Avant que la plateforme de BI ne puisse établir une connexion SSL avec l'hôte LDAP (pour authentifier les utilisateurs et groupes LDAP), elle doit recevoir et vérifier un certificat de sécurité envoyé par l'hôte LDAP. Pour vérifier le certificat, la plateforme de BI doit rechercher l'autorité de certification ayant émis le certificat dans sa base de données des certificats et pouvoir confirmer que l'attribut CN du certificat du serveur correspond exactement au nom d'hôte LDAP saisi dans la zone *Ajouter un hôte LDAP* lors de la première étape de l'Assistant, si vous avez entré le nom d'hôte LDAP sous la forme **`ABALONE.rd.crystald.net:389`**. (L'utilisation de **`CN =ABALONE:389`** dans le certificat ne fonctionne pas.) .
  Le nom d'hôte associé au certificat de sécurité du serveur est le nom d'hôte LDAP principal. Si vous sélectionnez cette option, vous ne pouvez pas utiliser un hôte LDAP de basculement.

> **Remarque**
>
> Les applications Java ignorent les premier et dernier paramètres et acceptent le certificat du serveur uniquement si celui-ci provient d'une autorité de certification de confiance.

2. Dans la zone *Hôte SSL*, saisissez le nom d'hôte de chaque ordinateur, puis cliquez sur *Ajouter*.

   Ensuite, vous devez ajouter le nom d'hôte de chaque ordinateur du déploiement de la plateforme BI qui utilise son SDK. (Cela concerne l'ordinateur sur lequel s'exécute le CMS (Central Management Server) et celui sur lequel s'exécute le serveur d'applications Web.)
3. Spécifiez les paramètres SSL pour chaque hôte SSL ajouté à la liste :
   a. Sélectionnez *Par défaut* dans la liste SSL.
   b. Décochez les cases *Utiliser la valeur par défaut*.
   c. Saisissez une valeur dans les zones *Chemin d'accès aux fichiers de certificats et de base de données de clés* et *Mot de passe d'accès à la base de données des clés*.
   d. Si vous spécifiez les paramètres d'une authentification mutuelle, saisissez une valeur dans la zone *Surnom du certificat du client dans la base de données de certificats*.

> **Remarque**
>
> Les paramètres par défaut seront utilisés (pour toute définition) pour n'importe quel hôte où la case *Utiliser la valeur par défaut* est cochée ou pour tout ordinateur dont le nom n'est pas ajouté à la liste des hôtes SSL.

4. Spécifiez les paramètres par défaut de chaque hôte qui n'apparaît pas dans la liste, puis cliquez sur *Suivant*.

   Pour spécifier les paramètres d'un autre hôte, sélectionnez le nom d'hôte dans la liste de gauche, puis saisissez les valeurs dans les zones de droite.

> **Remarque**
>
> Les paramètres par défaut seront utilisés (pour toute définition) pour n'importe quel hôte où la case *Utiliser la valeur par défaut* est cochée ou pour tout ordinateur dont le nom n'est pas ajouté à la liste des hôtes SSL.

5. Sélectionnez *De base (pas de connexion unique)* ou *SiteMinder* comme mode d'authentification de connexion unique LDAP.
6. Choisissez le mode de création de nouveaux utilisateurs et alias LDAP.
7. Cliquez sur *Terminer*.

Informations associées

Configuration du plug-in LDAP pour SiteMinder [page 288]

9.3.2.4 Modification des paramètres de configuration LDAP

Après avoir configuré l'authentification LDAP à l'aide de l'Assistant de configuration LDAP, vous pouvez modifier les paramètres de connexion et les groupes de membres LDAP sur la page *Résumé de la configuration du serveur LDAP*.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *LDAP*.

   Si l'authentification LDAP est configurée, la page *Résumé de la configuration du serveur LDAP* s'affiche. Sur cette page, vous pouvez modifier toutes les zones ou les champs des paramètres de connexion et les options de la zone *Groupes des membres LDAP mappés*.
3. Supprimez les groupes mappés actuellement qui ne seront plus accessibles selon les nouveaux paramètres de connexion, puis cliquez sur *Mettre à jour*.

   Vous pouvez supprimer les groupes mappés en sélectionnant le groupe d'utilisateurs, puis en cliquant sur le bouton *Supprimer* dans la section *Groupes des membres LDAP mappés*.
4. Modifiez les paramètres de connexion, puis cliquez sur *Mettre à jour*.
5. Si nécessaire, modifiez les *Options de nouvel alias*, *Options de mise à jour des alias* et *Options de nouvel utilisateur*, puis cliquez sur *Mettre à jour*.
6. Mappez les nouveaux groupes de membres LDAP, puis cliquez sur *Mettre à jour*.

9.3.2.5 Configuration du plug-in LDAP pour SiteMinder

Cette section explique comment configurer la CMC pour utiliser LDAP avec SiteMinder. SiteMinder est un outil tiers qui permet l'authentification et l'accès des utilisateurs et qui peut être employé avec le plug-in de sécurité LDAP pour créer une connexion unique à la plateforme de BI.

Pour utiliser SiteMinder et LDAP avec la plateforme de BI, vous devez apporter des modifications de configuration à deux endroits :

- Plug-in LDAP via la CMC
- Propriétés du fichier `BOE.war`

> **Remarque**
>
> Vérifiez que l'administrateur SiteMinder a activé la prise en charge des agents 4.x. Cette activation doit être effectuée quelle que soit la version SiteMinder prise en charge que vous utilisez. Pour en savoir plus sur SiteMinder et sur son installation, reportez-vous à sa documentation.

Informations associées

Pour configurer l'hôte LDAP [page 280]

9.3.2.5.1 Pour installer les bibliothèques ETPKI

Vous devez installer les bibliothèques ETPKI pour sécuriser les informations échangées entre le serveur de stratégie de connexion unique CA Single Sign-On et la plateforme de BI.

Avant d'installer les bibliothèques ETPKI, vous devez télécharger et installer le SDK de CA Single Sign-On.

La plateforme de BI prend uniquement en charge CA Single Sign-On 12.x. Si vous disposez d'une version plus ancienne de CA Single Sign-On, anciennement connue sous le nom de CA SiteMinder, vous devez passer à la version 12.x.

1. Accédez à `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install-64` pour les systèmes d'exploitation 64 bits et à `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install` pour les systèmes d'exploitation 32 bits.

   > **Remarque**
   >
   > Si la configuration de CA Single Sign-On n'est pas installée sur l'ordinateur où la plateforme de BI est installée, copiez les bibliothèques ETPKI sur le même ordinateur.

2. Installation des bibliothèques ETPKI dans un environnement Linux :
   a. Connectez-vous avec un accès à la racine et exécutez la commande `./setup install caller=sdk veryverbose`.
      Un message indiquant que l'installation est réussie s'affiche à la fin de l'installation ou de la console.
   b. Exécutez les commandes `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` et `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` pour définir le chemin comme répertoire d'installation avec l'utilisateur de la plateforme de BI.
   c. Redémarrez le *Server Intelligence Agent*.
3. Installation des bibliothèques ETPKI dans un environnement Windows :
   a. Lancez une invite de commande avec des droits d'administrateur depuis l'emplacement de la bibliothèque ETPKI.

b. Exécutez la commande `setup.exe install caller=sdk veryverbose`.
c. Vérifiez le message de réussite de l'installation dans *capki_install.log*, dans *%temp%*.
d. Redémarrez le *Server Intelligence Agent*.

Vous avez correctement installé les bibliothèques ETPKI.

9.3.2.5.2 Pour configurer LDAP pour la connexion unique avec SiteMinder

1. Ouvrez l'écran *Configurez les paramètres SiteMinder* à l'aide d'une des méthodes suivantes :
   - Sélectionnez SiteMinder dans l'écran *Choisissez un mode d'authentification de connexion unique LDAP* de l'Assistant de configuration LDAP.
   - Sélectionnez *Type de connexion unique* dans l'écran d'authentification LDAP, disponible si vous avez déjà configuré LDAP et que vous ajoutez maintenant la connexion unique.
2. Dans la zone *Hôte serveur de règles*, saisissez le nom de chaque serveur de règles, puis cliquez sur *Ajouter*.
3. Pour chaque hôte serveur de règles, indiquez le numéro des ports de *comptabilisation*, d'*Authentification* et d'*autorisation*.
4. Saisissez le *Nom de l'agent* et le *Secret partagé*. Saisissez à nouveau le secret partagé dans la zone *Confirmer le secret partagé*.
5. Cliquez sur *Suivant*.
6. Poursuivez par la configuration des options LDAP.

9.3.2.5.3 Pour activer LDAP et SiteMinder dans le fichier BOE.war

Outre la spécification des paramètres SiteMinder pour le plug-in de sécurité LDAP, les paramètres SiteMinder doivent être spécifiés pour les propriétés du fichier BOE.war.

1. Accédez au répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` de l'installation de la plateforme de BI.
2. Créez un fichier à l'aide de Notepad ou d'un autre éditeur de texte.
3. Entrez l'instruction suivante :

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Fermez le fichier et enregistrez-le sous le nom **`global.properties`**, sans extension de fichier.
5. Créez un autre fichier dans le même répertoire.
6. Entrez l'instruction suivante :

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

Par exemple :

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. Fermez le fichier et enregistrez-le sous le nom `bilaunchpad.properties`.

Les nouvelles propriétés ne prennent effet que lorsque l'application Web BOE modifiée est redéployée sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

9.3.3 Mappage des groupes LDAP

Après avoir configuré l'hôte LDAP à l'aide de l'Assistant de configuration LDAP, vous pouvez mapper les groupes LDAP aux groupes Enterprise.

Après avoir mappé les groupes LDAP, vous pouvez les afficher en cliquant sur les options LDAP dans la zone de gestion *Authentification*. Si l'authentification LDAP est configurée, la zone Groupes des membres LDAP mappés affiche les groupes LDAP mappés à la plateforme de BI.

> ⓘ Remarque
>
> Vous pouvez également mapper les groupes Windows AD pour qu'ils soient authentifiés dans la plateforme de BI via le plug-in de sécurité LDAP.

> ⓘ Remarque
>
> Si vous avez configuré LDAP par rapport à AD, cette procédure mappera vos groupes AD.

9.3.3.1 Pour mapper des groupes LDAP à l'aide de la plateforme de BI.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *LDAP*.

   Si l'authentification LDAP est configurée, la page de résumé LDAP apparaît.
3. Dans la zone *Groupes des membres LDAP mappés*, spécifiez votre groupe LDAP (soit par un nom commun ou un nom distinct) dans le champ *Ajouter un groupe LDAP (par cn ou dn)* et cliquez sur *Ajouter*.

   Répétez cette étape pour chaque groupe LDAP que vous souhaitez ajouter. Pour supprimer un groupe, mettez-le en surbrillance et cliquez sur *Supprimer*.
4. Dans la zone *Options de nouvel alias*, sélectionnez le mode de mappage des alias LDAP aux comptes Enterprise :
   - *Affecter à un même compte chaque alias LDAP ajouté*
     Utilisez cette option lorsque vous savez que certains utilisateurs possèdent un compte Enterprise portant le même nom ; cela signifie que les alias LDAP seront affectés aux utilisateurs existants (la

création d'alias automatique est activée). Les utilisateurs dépourvus de compte Enterprise, ou ne portant pas le même nom dans leur compte Enterprise et LDAP, sont ajoutés en tant que nouveaux utilisateurs LDAP.

- *Créer un nouveau compte pour chaque alias LDAP ajouté*
  Utilisez cette option pour créer un compte pour chaque utilisateur.

5. Dans la zone *Options de mise à jour des alias*, sélectionnez une option pour déterminer si les alias LDAP sont automatiquement créés pour les nouveaux utilisateurs :
   - *Créer de nouveaux alias lors de la mise à jour des alias*
     Utilisez cette option pour créer automatiquement un nouvel alias pour chaque utilisateur LDAP mappé à la plateforme de BI. De nouveaux comptes LDAP sont ajoutés pour les utilisateurs dépourvus de compte de la plateforme de BI, ou pour tous les utilisateurs si vous avez sélectionné l'option *Créer un nouveau compte pour chaque alias LDAP ajouté* et cliqué sur *Mettre à jour*.
   - *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
     Sélectionnez cette option si l'annuaire LDAP que vous mappez contient de nombreux utilisateurs dont seulement quelques-uns utiliseront la plateforme de BI. Le système ne crée pas automatiquement d'alias ni de comptes Enterprise pour tous les utilisateurs. Il crée plutôt des alias (et des comptes, le cas échéant) uniquement pour les utilisateurs qui se connectent à la plateforme de BI.
6. Si votre licence de plateforme de BI est basée sur les rôles utilisateur, sélectionnez une option dans la zone *Options de nouvel utilisateur* pour indiquer les propriétés des nouveaux comptes Enterprise créés à mapper aux comptes LDAP :
   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
     Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

     > **Remarque**
     >
     > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
     >
     > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
     Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs au système, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.
7. Cliquez sur *Mettre à jour*.

9.3.3.2 Pour démapper les groupes LDAP à l'aide de la plateforme de BI

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *LDAP*.

   Si l'authentification LDAP est configurée, la page de résumé LDAP apparaît.
3. Dans la zone "Groupes des membres LDAP mappés", sélectionnez le groupe LDAP que vous voulez supprimer.
4. Cliquez sur *Supprimer*, puis sur *Mettre à jour*.

   Les utilisateurs appartenant à ce groupe ne pourront pas accéder à la plateforme de BI.

   > **Remarque**
   >
   > La seule exception possible se produit lorsqu'un utilisateur dispose d'un alias pour un compte Enterprise. Pour limiter l'accès, désactivez ou supprimez le compte Enterprise de l'utilisateur.

Pour refuser l'authentification LDAP pour tous les groupes, décochez la case "L'authentification LDAP est activée", puis cliquez sur *Mettre à jour*.

9.3.3.3 Mappage de LDAP par rapport à Windows AD

Si vous configurez LDAP par rapport à AD (Windows AD), tenez compte des restrictions suivantes :

- Si vous configurez LDAP par rapport à AD, vous pourrez mapper vos utilisateurs, mais vous ne serez pas en mesure de configurer une connexion unique AD ou une connexion unique à la base de données. Cependant, les méthodes de connexion unique LDAP telles que SiteMinder et l'authentification sécurisée seront toujours disponibles.
- Les utilisateurs qui sont uniquement membres de groupes par défaut d'AD ne pourront pas se connecter. Ils doivent également être membres d'un autre groupe AD créé explicitement et ce groupe doit en plus être mappé. Le groupe "utilisateurs du domaine" est un exemple de ce type de groupe.
- Si un groupe local de domaine mappé contient un utilisateur provenant d'un domaine différent de la forêt, l'utilisateur de ce domaine différent ne sera pas en mesure de se connecter.
- Les utilisateurs d'un groupe universel dont le domaine est différent du contrôleur de domaine spécifié comme hôte LDAP ne pourront pas se connecter.
- Vous ne pouvez pas utiliser le plug-in LDAP pour mapper les utilisateurs et les groupes de forêts AD situés à l'extérieur de la forêt dans laquelle la plateforme de BI est installée.
- Vous ne pouvez pas mapper le groupe Utilisateurs du domaine dans AD.
- Vous ne pouvez pas mapper un groupe local de l'ordinateur.

- Si vous utilisez le contrôleur de domaine de catalogue global, vous devez tenir compte des remarques supplémentaires suivantes lors du mappage de LDAP à AD :

Situation	Remarques
Plusieurs domaines lors du pointage vers le contrôleur de domaine de catalogue global	Vous pouvez effectuer un mappage dans : • les groupes universels d'un domaine enfant, • les groupes du même domaine contenant des groupes universels d'un domaine enfant, et • les groupes universels inter-domaines. Vous ne pouvez pas effectuer de mappage dans : • les groupes globaux d'un domaine enfant, • les groupes locaux d'un domaine enfant, • les groupes du même domaine contenant un groupe global du domaine enfant, et • les groupes globaux inter-domaines. Généralement, si le groupe est un groupe universel, il prendra en charge les utilisateurs inter-domaines et ceux des domaines enfants. Les autres groupes ne seront pas mappés s'ils contiennent des utilisateurs inter-domaines ou de domaines enfants. Dans le domaine vers lequel vous pointez, vous pouvez mapper les groupes locaux, globaux et universels du domaine.
Mappage dans les groupes universels	Pour effectuer un mappage dans les groupes universels, vous devez pointer vers le contrôleur de domaine de catalogue global. Vous devez également utiliser le numéro de port 3268 au lieu du port 389 par défaut.

- Si vous utilisez plusieurs domaines mais que vous ne pointez pas vers le contrôleur de domaine de catalogue global, vous ne pouvez effectuer de mappage dans aucun type de groupe inter-domaines ou de domaines enfant. Vous pouvez effectuer un mappage dans tous les types de groupe du domaine spécifique vers lequel vous pointez uniquement.

9.3.3.4 Utilisation du plug-in LDAP pour configurer la connexion unique à la base de données SAP HANA

Cette section présente aux administrateurs les étapes requises pour définir et configurer la connexion unique (SSO) entre la plateforme de BI s'exécutant sur SUSE Linux 11 et la base de données SAP HANA. L'authentification LDAP à l'aide de Kerberos permet aux utilisateurs AD d'être authentifiés sur une plateforme de BI exécutée sur Linux (spécifiquement SUSE). Ce scénario prend également en charge la connexion unique à SAP HANA comme base de données de reporting.

> **Remarque**
>
> Pour en savoir plus sur la manière de configurer la base de données SAP HANA, voir *Base de données SAP HANA - Guide d'installation et de mise à jour des serveurs*. Pour en savoir plus sur la manière de configurer le composant d'accès aux données de SAP HANA, voir le *Guide d'accès aux données*.

Vue d'ensemble de l'implémentation

Les composants suivants doivent être installés pour que la connexion unique Kerberos fonctionne.

Composant	Configuration requise
Contrôleur de domaine	Hébergé par le même ordinateur qu'Active Directory pour utiliser l'authentification Kerberos.
Central Management Server	Installé et exécuté sur un ordinateur utilisant SUSE Linux Enterprise 11 (SUSE).
Client Kerberos V5	Installé avec les utilitaires et bibliothèques requis sur l'hôte SUSE. **Remarque** Utilise la dernière version du client Kerberos V5. Ajoutez les dossiers `bin` et `lib` aux variables d'environnement `PATH` et `LD_LIBRARY_PATH`.
Plug-in d'authentification LDAP	Activé sur l'hôte SUSE.
Fichier de configuration de connexion Kerberos	Créé sur l'ordinateur hébergeant le serveur d'applications Web.

Workflow d'implémentation

Les tâches suivantes doivent être effectuées pour permettre aux utilisateurs de la plateforme de BI une connexion unique à SAP HANA à l'aide de l'authentification Kerberos via JDBC.

1. Configuration de l'hôte AD.
2. Création des comptes et fichiers keytab pour l'hôte SUSE et la plateforme de BI sur l'hôte AD.
3. Installation des ressources Kerberos sur l'hôte SUSE.
4. Configuration de l'hôte SUSE pour l'authentification Kerberos.
5. Configuration des options de l'authentification Kerberos dans le plug-in d'authentification LDAP.
6. Création d'un fichier de configuration de connexion Kerberos pour l'hôte des applications Web.

9.3.3.4.1 Configuration du contrôleur de domaine

Vous pouvez avoir besoin de configurer une relation sécurisée entre l'hôte SUSE et le contrôleur de domaine. Si l'hôte SUSE est dans le contrôleur de domaine Windows, vous n'avez pas à configurer la relation sécurisée. Cependant, si le déploiement de la plateforme de BI et le contrôleur de domaine sont dans des domaines

différents, vous pouvez avoir besoin de configurer une relation sécurisée entre l'ordinateur Linux SUSE et le contrôleur de domaine. Cette action requiert les éléments suivants :

1. Créez un compte utilisateur pour l'ordinateur SUSE exécutant la plateforme de BI.
2. Créez un nom principal du service (SPN) pour l'hôte.

   > **Remarque**
   >
   > Le SPN doit être mis en forme selon les conventions Windows AD : hôte/`<nom d'hôte>`@`<NOM_DOMAINE_DNS>`. Utilisez un nom de domaine entièrement qualifié, en minuscules, pour /`<nom d'hôte>`. Le `<NOM_DOMAINE_DNS>` doit être spécifié en majuscules.

3. Exécutez la commande de configuration Keytab Kerberos `ktpass` pour associer le SPN au compte utilisateur :

   ```
   c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
   Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
   ```

Les étapes suivantes doivent être effectuées sur l'ordinateur hébergeant le contrôleur de domaine.

1. Créez un compte utilisateur pour le service exécutant la plateforme de BI.
2. Dans la page *Comptes utilisateurs*, cliquez avec le bouton droit sur le nouveau compte de service et sélectionnez *Propriétés* > *Délégation*.
3. Sélectionnez *Approuver cet utilisateur pour la délégation à tous les services (Kerberos uniquement)*.
4. Exécutez la commande de configuration Keytab Kerberos `ktpass` pour créer un compte SPN pour le nouveau compte de service :

   ```
   c:\>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
   <service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
   -out <sianame>.keytab
   ```

   > **Remarque**
   >
   > Le SPN doit être mis en forme selon les conventions Windows AD : nomsia/`<nom_service>`@`<NOM_DOMAINE_DNS>`. Indiquez le `<nom du service>` en minuscules, sinon la plateforme SUSE ne pourra pas le résoudre. Le `<NOM_DOMAINE_DNS>` doit être spécifié en majuscules.

Paramètre	Description
`-princ`	Spécifie le nom principal pour l'authentification Kerberos.
`-out`	Spécifie le nom du fichier `keytab` Kerberos à générer. Il doit correspondre au `<nomsia>` utilisé dans `-princ`.
`-mapuser`	Spécifie le nom du compte utilisateur auquel le SPN est mappé. Le Server Intelligence Agent s'exécute sur ce compte.
`-pass`	Indique le mot de passe utilisé par le compte de service.
`-ptype`	Spécifie le type principal. `-ptype KRB5_NT_PRINCIPAL`

Paramètre	Description
`-crypto`	Spécifie le type de cryptage à utiliser avec le compte de service : `-crypto RC4-HMAC-NT`

Vous avez généré les fichiers keytab requis pour la relation sécurisée entre l'ordinateur SUSE et le contrôleur de domaine.

Vous devez transférer le ou les fichiers keytab sur l'ordinateur SUSE et les stocker dans le répertoire `/etc`.

9.3.3.4.2 Configuration de l'ordinateur SUSE Linux Enterprise 11

Les ressources suivantes sont requises pour configurer Kerberos sur l'ordinateur Linux SUSE exécutant la plateforme de BI :

- Fichiers keytab créés sur le contrôleur de domaine. Le fichier keytab créé pour le service de la palteforme de BI est obligatoire. Le fichier keytab pour l'hôte SUSE est recommandé, en particulier pour les scénarios où l'hôte de la plateforme de BI et le contrôleur de domaine sont dans des domaines différents.
- La dernière bibliothèque Kerberos V5 (y compris le client Kerberos) doit être installée sur l'hôte SUSE. Vous devez ajouter l'emplacement des fichiers binaires aux variables d'environnement `PATH` et `LD_LIBRARY_PATH` . Pour vérifier que le client Kerberos est correctement installé et configuré, assurez-vous que les utilitaires et bibliothèques suivants sont présents sur l'hôte SUSE :
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> → Conseil
>
> Exécutez `rpm -qa | grep krb` pour contrôler la version de ces bibliothèques. Pour en savoir plus sur le dernier client Kerberos, les bibliothèques et la configuration de l'hôte UNIX, voir http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 .

Une fois que toutes les ressources requises sont disponibles sur l'hôte SUSE, suivez les instructions ci-dessous pour configurer l'authentification Kerberos.

> ⓘ Remarque
>
> Pour effectuer ces étapes, vous devez disposer des droits root.

1. Pour fusionner les fichiers keytab, exécutez la commande suivante :

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Modifiez le fichier `/etc/kerb5.conf` pour qu'il fasse référence au contrôleur de domaine (sur la plateforme Windows) comme étant le contrôleur de domaine Kerberos (KDC, Kerberos Domain Controller).

   Utilisez l'exemple ci-dessous :

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

> **Remarque**
>
> Le fichier `krb5.conf` contient les informations de configuration Kerberos, y compris les emplacements des KDC et serveurs des domaines Kerberos importants, les applications Kerberos et les mappages des noms d'hôte dans les domaines Kerberos. Normalement, le fichier `krb5.conf` est installé dans le répertoire `/etc`.

3. Ajoutez le contrôleur de domaine à `/etc/hosts` afin que l'hôte SUSE puisse localiser le KDC.
4. Exécutez le programme `kinit` à partir du répertoire `/usr/local/bin` pour vérifier que Kerberos a été configuré correctement. Vérifiez qu'un compte utilisateur de compte AD peut se connecter à l'ordinateur SUSE.

> **→ Conseil**
>
> Le KDC doit émettre un Ticket Granting Ticket (TGT) pouvant être visualisé dans le cache. Utilisez le programme `klist` pour visualiser le TGT.

Exemple

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>
> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
>klist -k
```

```
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

Utilisez également `kinit` pour tester les SPN.

9.3.3.4.3 Configuration des options d'authentification Kerberos pour LDAP

Avant de configurer l'authentification Kerberos pour LDAP, vous devez activer et configurer le plug-in d'authentification LDAP de la plateforme de BI pour vous connecter au répertoire AD. Pour utiliser l'authentification LDAP, vous devez d'abord vérifier que votre répertoire LDAP respectif est configuré.

> **Remarque**
>
> Lors de l'exécution de l'*Assistant de configuration LDAP*, vous devez spécifier le *serveur d'applications Microsoft Active Directory* et fournir les informations de configuration demandés.

Une fois l'authentification LDAP activée et connectée au serveur d'applications Microsoft Active Directory, la zone *Activer l'authentification Kerberos* s'affiche sur la page Résumé de la configuration du serveur LDAP. Utilisez cette zone pour configurer l'authentification Kerberos, qui est requise pour la connexion unique à la base de données SAP HANA depuis un déploiement de la plateforme de BI sur SUSE.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *LDAP*.

   La page *Résumé de la configuration du serveur LDAP* s'affiche, vous pouvez y modifier n'importe quel paramètre de connexion ou champ.
3. Pour configurer l'authentification Kerberos, suivez ces étapes dans la zone *Activer l'authentification Kerberos* :
   a. Cliquez sur *Activer l'authentification Kerberos*.
   b. Cliquez sur *Contexte de sécurité de la mémoire cache (obligatoire pour une connexion unique à la base de données)*.

      > **Remarque**
      >
      > L'activation du contexte de sécurité du cache est spécialement requise pour la connexion unique à SAP HANA.

   c. Spécifiez le SPN (Service Principal Name) du compte de la plateforme de BI dans *Nom principal du service*.

      Le format pour spécifier le SPN est `<nomsia/service>@<NOM_DOMAINE_DNS>`, où

`<nomsia>`	Nom du Server Intelligence Agent
`<service >`	Nom du compte de service utilisé pour exécuter la plateforme de BI
NOM_DOMAINE_DNS	Nom de domaine du contrôleur de domaine en majuscules

> → Conseil
>
> En spécifiant le SPN, souvenez-vous que `<nomsia/service>` est sensible à la casse.

d. Spécifiez le domaine du contrôleur de domaine dans *Domaine Kerberos par défaut*.
e. Spécifiez `userPrincipalName` dans *Nom principal de l'utilisateur*.

   Cette valeur est utilisée par l'application d'authentification LDAP pour fournir les valeurs d'ID utilisateur requises par Kerberos. La valeur indiquée doit correspondre au nom fourni lors de la création des fichiers keytab.

4. Cliquez sur *Mettre à jour* pour envoyer et enregistrer les modifications.

Vous avez configuré les options d'authentification Kerberos pour faire référence aux comptes utilisateur dans le répertoire AD.

Vous devez créer un fichier de configuration de connexion Kerberos - `bscLogin.conf` - pour activer la connexion Kerberos et la connexion unique.

Informations associées

Configuration de l'authentification LDAP [page 279]

9.3.3.4.4 Création d'un fichier de configuration de connexion Kerberos

Pour activer la connexion Kerberos et la connexion unique, vous devez ajouter un fichier de configuration de connexion sur l'ordinateur hébergeant le serveur d'applications Web de la plateforme de BI.

1. Créez un fichier nommé `bscLogin.conf` et stockez-le dans le répertoire `/etc`.

   > ⓘ Remarque
   >
   > Vous pouvez stocker ce fichier à un emplacement différent. Toutefois, si vous le faites, vous devrez spécifier son emplacement dans vos options Java. Il est conseillé de placer le fichier `bscLogin.conf` et les fichiers keytab Kerberos dans le même répertoire. Dans un déploiement réparti, il faut ajouter un fichier `bscLogin.conf` pour chaque ordinateur hébergeant un serveur d'applications Web.

2. Ajoutez le code suivant au fichier de configuration de connexion `bscLogin.conf` :

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="<nom principal>";
};
```

> **Remarque**
>
> La section suivante est particulièrement requise pour la connexion unique :
>
> ```
> com.businessobjects.security.jgss.accept {
> com.sun.security.auth.module.Krb5LoginModule required
> storeKey=true
> useKeyTab=true
> keyTab="/etc/krb5.keytab"
> principal="<nom principal>";
> };
> ```

3. Enregistrez le fichier et fermez-le.

9.3.3.5 Dépannage des nouveaux comptes LDAP

- Si vous créez un compte utilisateur LDAP qui n'appartient pas à un compte de groupe mappé à la plateforme de BI, mappez le groupe ou ajoutez le nouveau compte utilisateur LDAP à un groupe déjà mappé au système.
- Si vous créez un compte utilisateur LDAP qui appartient à un compte de groupe mappé à la plateforme de BI, actualisez la liste des utilisateurs.

Informations associées

Configuration de l'authentification LDAP [page 279]
Mappage des groupes LDAP [page 291]

9.4 Authentification Windows AD

9.4.1 Utilisation de l'authentification Windows AD

9.4.1.1 Exigences de prise en charge Windows AD et configuration initiale

Cette section vous guide à travers le processus de configuration de l'authentification Windows Active Directory (AD) pour une utilisation sur la plateforme de BI. L'ensemble des workflows de bout en bout requis que vous devez exécuter sont présentés ensemble avec des tests de validation et les vérifications des prérequis.

> **Remarque**
>
> Pour en savoir plus sur la configuration de l'authentification Windows AD, voir l'article KBA 1631734 de la Base de connaissances SAP sur https://service.sap.com/sap/support/notes/1631734.

Exigences de prise en charge

Pour faciliter l'authentification AD sur la plateforme de BI, vous devez tenir compte des exigences de prise en charge suivantes.

- Le CMS doit toujours être installé sur une plateforme Windows prise en charge.
- Certaines applications de la plateforme de BI peuvent uniquement utiliser des méthodes d'authentification spécifiques. Par exemple, des applications telles que la zone de lancement BI et la Central Management Console ne prennent en charge que Kerberos.

Workflow de configuration AD recommandé

Pour configurer initialement l'authentification AD manuelle avec la plateforme de BI, utilisez le workflow suivant :

1. Configurez le contrôleur de domaine.
2. Configurez l'authentification AD dans la CMC.
3. Configurez le compte utilisateur AD sur le Server Intelligence Agent (SIA).
4. Configurez votre serveur d'applications Web pour l'authentification AD avec Kerberos

> **Remarque**
>
> Utilisez ce workflow, que vous ayez besoin ou non de la connexion unique. Le workflow décrit dans les sections suivantes vous permettra d'abord de vous connecter manuellement (à l'aide d'un nom d'utilisateur et d'un mot de passe AD) à la plateforme de BI. Une fois l'authentification AD manuelle correctement configurée, une section détaillée vous guide à travers le processus de configuration de la connexion unique pour l'authentification AD.

9.4.2 Préparation du contrôleur de domaine

9.4.2.1 Configuration d'un compte de service pour l'authentification AD avec Kerberos

Pour configurer la plateforme de BI de sorte à pouvoir utiliser l'authentification Windows AD (Kerberos), vous avez besoin d'un compte de service. Vous pouvez utiliser un compte de domaine existant ou en créer un nouveau. Le compte de service sera utilisé pour exécuter les serveurs de la plateforme de BI. Après avoir configuré le compte, vous devez configurer un SPN pour celui-ci. Ce SPN sert à importer des groupes d'utilisateurs AD sur la plateforme de BI.

> **Remarque**
>
> Pour utiliser AD avec la connexion unique, vous devrez revoir ultérieurement la configuration du compte de service de sorte à lui accorder les droits appropriés et à le configurer pour une restriction de délégation.

9.4.2.1.1 Pour configurer le compte de service sur un domaine Windows 2008

Vous devez configurer un nouveau compte de service pour activer correctement l'authentification Windows AD à l'aide du protocole Kerberos. Ce compte de service sera utilisé principalement pour permettre aux utilisateurs d'un groupe AD précis de se connecter à la zone de lancement BI. La tâche suivante est effectuée sur l'ordinateur du contrôleur de domaine AD.

1. Créez un compte de service avec un mot de passe sur le contrôleur de domaine principal.
2. Utilisez la commande `setspn -s` pour ajouter les noms principaux de service (SPN) au compte de service créé au cours de l'étape 1. Indiquez les noms principaux de service (SPN) du compte de service ainsi que du serveur, du serveur de domaine complet et l'adresse IP de l'ordinateur sur lequel est déployée la zone de lancement BI.
   Par exemple :

   ```
   setspn –s BICMS/service_account_name.domain.com serviceaccountname
   setspn -s HTTP/<servername> <servicename>
   setspn -s HTTP/<servername.domain.com> <servicename>
   setspn -s HTTP/<ip address of server> <servicename>
   ```

   `BICMS` est le nom de l'ordinateur sur lequel s'exécute le SIA, `<nomserveur>` est le nom du serveur sur lequel est déployée la zone de lancement BI, `<domainenomserveur>` est son nom de domaine complet.
3. Exécutez `setspn -l <nomservice>` pour vérifier que les noms de service principaux ont été ajoutés au compte de service.
   Le résultat affiché de la commande doit inclure tous les SPN enregistrés, comme illustré ci-dessous :

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<servername>.@example.com
   HTTP/<servername>
   <servername>/<servicename>@example.com
   ```

   Vous trouverez ci-dessous un exemple de résultat :

   ```
   C:\Users\Admin>setspn -L bossosvcacct
   Registered ServicePrincipalNames for
   CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
           BICMS/bossosvcacct@example.com
           HTTP/Tomcat HTTP/Tomcat@example.com
           HTTP/Load_Balancer.@example.com
   ```

Une fois créé, des droits doivent être affectés au compte de service et celui-ci doit être ajouté au groupe Administrateurs local du serveur. Le SPN servira à importer des groupes AD dans la section suivante.

9.4.3 Configuration de l'authentification AD dans la CMC

9.4.3.1 Plug-in de sécurité Windows AD

Le plug-in de sécurité Windows AD permet de mapper des comptes et des groupes d'utilisateurs de la base de données utilisateur AD 2008 à la plateforme de BI. Il permet également au système de vérifier toutes

les requêtes de connexion qui spécifient l'authentification AD. Les utilisateurs sont authentifiés par rapport à la base de données utilisateur AD et leur appartenance à un groupe AD mappé est vérifiée avant que le CMS (Central Management Server) ne leur accorde une session active. Vous pouvez utiliser le plug-in pour configurer les mises à jour des groupes AD importés.

Le plug-in de sécurité de Windows AD vous permet de procéder à la configuration suivante :

- Authentification Windows AD avec Kerberos
- Authentification Windows AD avec NTLM
- Authentification Windows AD avec SiteMinder pour une connexion unique

Le plug-in de sécurité AD est compatible avec les domaines AD 2008 exécutés en mode natif ou mixte.

Une fois que vous avez mappé vos utilisateurs et groupes AD, ils peuvent accéder aux outils client de la plateforme de BI à l'aide de l'option d'authentification *Windows AD*.

- L'authentification Windows AD fonctionne si le CMS s'exécute sous Windows. Pour que la connexion unique à une base de données fonctionne, les serveurs de reporting doivent également s'exécuter sous Windows. Dans le cas contraire, tous les autres serveurs et services peuvent s'exécuter sur toutes les plateformes prises en charge par la plateforme de BI.

  > **Remarque**
  >
  > La configuration a été effectuée et testée avec SUSE linux Enterprise 11 uniquement.

- Le plug-in Windows AD pour la plateforme de BI prend en charge les domaines dans plusieurs forêts.

9.4.3.2 Pour mapper des utilisateurs et groupes Windows AD

Pour pouvoir importer des groupes d'utilisateurs AD sur la plateforme de BI, vous devez avoir rempli les conditions préalables suivantes :

- Un compte de service a été créé sur le contrôleur de domaine pour la plateforme de BI. Le compte sera utilisé pour exécuter les serveurs de la plateforme de BI.

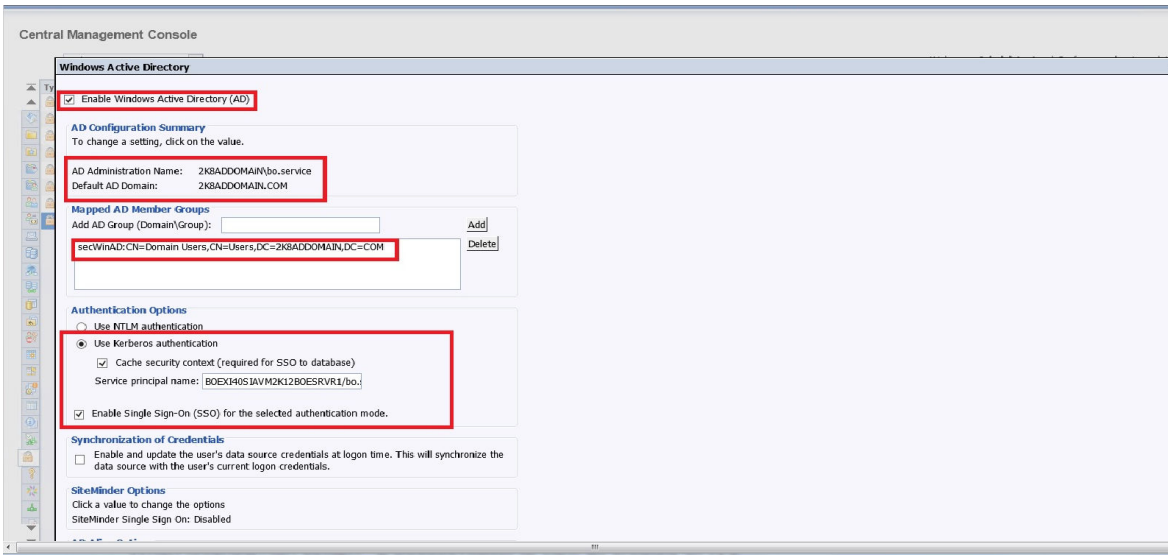
> **ⓘ Remarque**
>
> Pour activer l'authentification AD avec la connexion unique Vintela, vous devez fournir un SPN configuré à cette fin. Les étapes présentées ci-dessous concernent la configuration de l'authentification AD manuelle sur la plateforme de BI. Une fois l'authentification AD manuelle configurée, reportez-vous à la section *Configuration de la connexion unique* de ce chapitre pour savoir comment ajouter la connexion unique à votre configuration d'authentification AD.

- Vous vous êtes assuré que le SPN contenant le nom de l'ordinateur sur lequel s'exécute le SIA a été ajouté au compte de service.

Les étapes 1 à 11 indiquées ci-après sont obligatoires pour importer des groupes AD sur la plateforme de BI.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Windows AD*.
3. Cochez la case *Activer Windows Active Directory (AD)*.
4. Dans la zone *Synthèse de configuration d'AD*, cliquez sur le lien en regard de *Nom d'administration AD*.

> **ⓘ Remarque**
>
> Avant que le plug-in de Windows AD ne soit configuré, ce lien apparaît sous forme de guillemets. Après enregistrement de la configuration, le lien est rempli avec les noms d'administration AD.



5. Saisissez le nom et le mot de passe d'un compte d'utilisateur du domaine activé.

   Les références de connexion d'administration peuvent utiliser l'un des formats suivants :

   - Nom NT (`NomDomaine\NomUtilisateur`)
   - UPN (`utilisateur@nom_domaine_DNS`)

   La plateforme de BI utilise ce compte pour demander des informations à AD. La plateforme ne modifie, n'ajoute ou ne supprime aucun contenu d'AD. Etant donné qu'elle lit uniquement les informations, seuls les droits correspondants sont requis.

> **Remarque**
>
> L'authentification AD sera interrompue si le compte utilisé pour lire l'annuaire AD devient non valide (par exemple, si le mot de passe du compte est modifié ou expire ou si le compte est désactivé).

6. Saisissez le domaine AD dans la zone *Domaine AD par défaut*.

   Le domaine doit être spécifié comme NOM DE DOMAINE COMPLET, TOUT EN MAJUSCULES, ou comme nom de domaine enfant d'où la plupart des utilisateurs se connectent à la plateforme de BI. Cela doit correspondre au domaine par défaut spécifié dans les fichiers de configuration Kerberos utilisés pour configurer le serveur d'applications. Vous pouvez mapper les groupes du domaine par défaut sans spécifier le préfixe du nom de domaine. Si vous saisissez un nom de domaine AD par défaut, les utilisateurs du domaine par défaut n'ont pas à le spécifier lorsqu'ils se connectent à la plateforme de BI à l'aide de l'authentification AD.

7. Dans la zone *Groupes de membres AD mappés*, saisissez le domaine\groupe AD dans la zone *Ajouter un groupe AD (domaine\groupe)* à l'aide d'un des formats suivants pour mapper les groupes :
   - nom de compte du gestionnaire de comptes de sécurité (SAM, Security Account Manager), également appelé nom NT (`NomDomaine\NomGroupe`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   > **Remarque**
   >
   > Si vous souhaitez mapper un groupe local, utilisez uniquement le format de nom NT : `\\<NomServeur>\<NomGroupe>`. AD ne prend pas en charge les utilisateurs locaux ; ceux qui appartiennent à un groupe local mappé ne seront pas mappés à la plateforme de BI. Ils ne peuvent donc pas accéder au système.

   > **→ Conseil**
   >
   > En cas de connexion manuelle à la zone de lancement BI, les utilisateurs issus d'autres domaines doivent faire suivre leur nom d'utilisateur du nom du domaine en majuscules. Par exemple, `CHILD.PARENTDOMAIN.COM` est le domaine dans
   >
   > ```
   > user@CHILD.PARENTDOMAIN.COM
   > ```

8. Cliquez sur *Ajouter*.

   Le groupe est ajouté dans la liste sous *Groupes de membres AD mappés*.

9. Dans la zone *Groupes de membres AD mappés*, saisissez le domaine\groupe AD de votre choix dans le champ *Rechercher un groupe AD (domaine\groupe)*.

   Cette fonction recherche le groupe recherché dans la liste. Vous pouvez également sélectionner *Afficher* pour visualiser la liste complète des groupes AD dans une boîte de dialogue distincte.

10. Sous *Options d'authentification*, sélectionnez *Utiliser l'authentification Kerberos*.
11. Dans la zone *Nom principal du service*, saisissez le SPN mappé au compte de service que vous avez créé pour exécuter les serveurs de la plateforme de BI.

    > **Remarque**
    >
    > Vous devez spécifier le SPN pour le compte de service exécutant le SIA. Par exemple : `BICMS/bossosvcacct.domain.com`.

12. Cliquez sur *Mettre à jour*.

> ⚠ Attention
>
> Ne continuez pas si le mappage des utilisateurs et/ou groupes ne s'effectue pas correctement ! Pour résoudre des problèmes de mappage de groupe AD spécifiques, reportez-vous à la note SAP 1631734.

> ⓘ Remarque
>
> Si vous avez correctement mappé les comptes de groupes AD et ne désirez pas configurer les options d'authentification AD ou les mises à jour de groupes AD, ignorez les étapes 12 à 19. Vous pouvez configurer ces paramètres facultatifs après avoir configuré l'authentification Kerberos AD manuelle.

13. Si votre configuration requiert une connexion unique à la base de données, sélectionnez *Contexte de sécurité de la mémoire cache*.

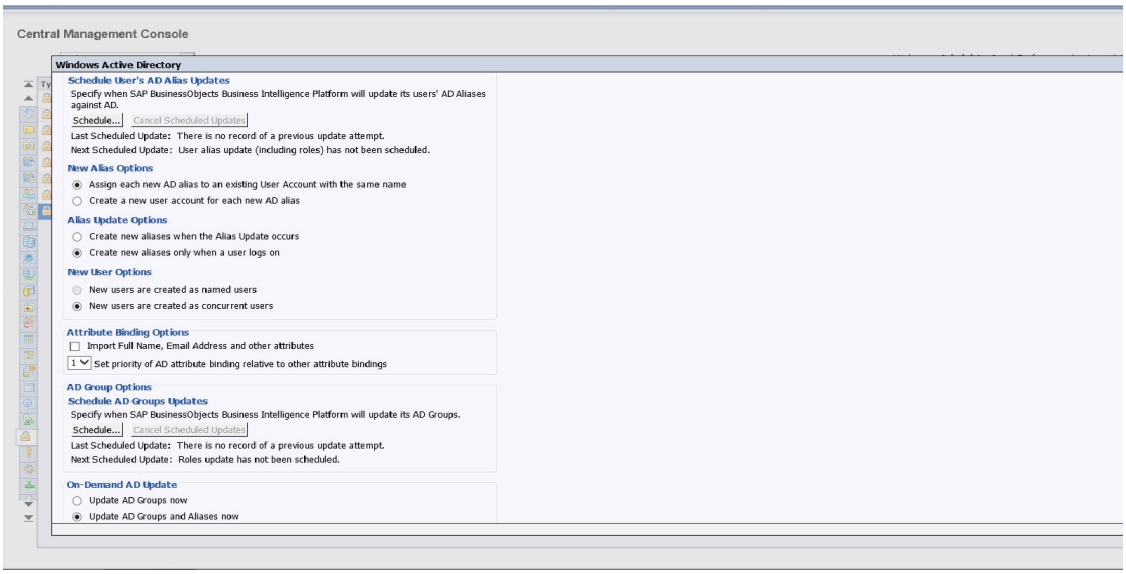
> ⓘ Remarque
>
> S'il s'agit de votre configuration initiale de l'authentification AD, il est recommandé de configurer l'authentification AD manuelle avant d'envisager la configuration supplémentaire requise pour la connexion unique.

14. Sélectionnez *Activez la connexion unique pour le mode d'authentification sélectionné* si vous avez besoin de la connexion unique pour la configuration de l'authentification AD.
15. Dans la zone *Synchronisation des références de connexion*, sélectionnez une option pour activer et mettre à jour les références de connexion à la source de données de l'utilisateur AD.

    Cette option synchronise la source de données avec les références de connexion actuelles de l'utilisateur, permettant ainsi l'exécution de rapports planifiés lorsque l'utilisateur n'est pas connecté à la plateforme de BI et que la connexion unique Kerberos n'est pas disponible.
16. Dans la zone *Options d'alias AD*, indiquez comment les nouveaux alias sont ajoutés et mis à jour sur la plateforme de BI.
    a. Dans la zone *Options de nouvel alias*, sélectionnez le mode de mappage des nouveaux alias aux comptes Enterprise :
       - *Affecter chaque nouvel alias AD à un compte utilisateur existant portant le même nom*
         Sélectionnez cette option si des utilisateurs possèdent un compte Enterprise portant le même nom ; en d'autres termes, les alias AD seront affectés aux utilisateurs existants (la création automatique d'alias est activée). Les utilisateurs dépourvus de compte Enterprise, ou ne portant pas le même nom dans leurs comptes Enterprise et AD, sont ajoutés en tant que nouveaux utilisateurs.
       - *Créer un nouveau compte utilisateur pour chaque nouvel alias AD*
         Sélectionnez cette option pour créer un nouveau compte pour chaque utilisateur.

    b. Dans *Options de mise à jour des alias*, sélectionnez le mode de gestion des mises à jour d'alias pour les comptes Enterprise :
       - *Créer de nouveaux alias lors de la mise à jour des alias*
         Sélectionnez cette option pour créer automatiquement un alias pour chaque utilisateur AD mappé à la plateforme de BI. De nouveaux comptes AD sont ajoutés pour les utilisateurs dépourvus de compte pour la plateforme de BI ou pour tous les utilisateurs si vous avez sélectionné l'option *Créer un nouveau compte utilisateur pour chaque nouvel alias AD* et cliqué sur *Mettre à jour*.
       - *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
         Sélectionnez cette option si l'annuaire AD que vous mappez contient de nombreux utilisateurs dont seulement quelques-uns utiliseront la plateforme de BI. La plateforme ne crée pas

automatiquement d'alias et de comptes Enterprise pour tous les utilisateurs. Il crée plutôt des alias (et des comptes, le cas échéant) uniquement pour les utilisateurs qui se connectent à la plateforme de BI.



c. Dans la zone *Options de nouvel utilisateur*, sélectionnez le mode de création des utilisateurs :

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
  Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers et permettent d'accéder à la plateforme de BI en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

  > **Remarque**
  >
  > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
  >
  > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
  Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences Utilisateur simultané. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs au système, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

17. Pour configurer le mode de planification des mises à jour d'alias AD, cliquez sur *Planifier*.
    a. Dans la boîte de dialogue *Planifier*, sélectionnez une récurrence dans la liste *Exécuter l'objet*.
    b. Définissez les autres options et paramètres de planification selon vos besoins.
    c. Cliquez sur *Planifier*.

Lorsque la mise à jour des alias se produit, les informations sur le groupe sont également mises à jour.

18. Dans la zone *Options de liaison d'attributs*, spécifiez la priorité de liaison d'attributs pour le plug-in AD :
    a. Cochez la case *Importer le nom complet, l'adresse électronique et d'autres attributs*.
    Les noms complets et les descriptions utilisés dans les comptes AD sont importés et stockés avec les objets utilisateur sur la plateforme de BI.
    b. Spécifiez une option pour *Rendre la liaison d'attributs AD prioritaire par rapport aux autres liaisons d'attributs*.

    Si l'option est définie sur 1, les attributs AD sont prioritaires lorsqu'AD et les autres plug-ins (LDAP et SAP) sont activés. Si l'option est définie sur 3, les attributs des autres plug-ins sont prioritaires. Les liaisons doivent être définies sur des valeurs différentes. La définition de plusieurs plug-ins d'authentification sur la même valeur de liaison conduit à des résultats inattendus.
19. Dans la zone *Options du groupe AD*, configurez les mises à jour du groupe AD :
    a. Cliquez sur *Planifier*.
    La boîte de dialogue *Planifier* s'affiche.
    b. Sélectionnez une récurrence dans la liste *Exécuter l'objet*.
    c. Définissez les autres options et paramètres de planification selon vos besoins.
    d. Cliquez sur *Planifier*.

    Le système planifie la mise à jour et l'exécute conformément à la planification que vous avez définie. La prochaine mise à jour planifiée pour les comptes du groupe AD est affichée sous *Options du groupe AD*.
20. Dans la zone *Mise à jour d'AD à la demande*, sélectionnez l'une des options suivantes :
    - *Mettre à jour les groupes AD maintenant*
    Sélectionnez cette option pour démarrer la mise à jour de tous les groupes AD planifiés lorsque vous cliquez sur *Mettre à jour*. La prochaine mise à jour planifiée du groupe AD est répertoriée sous *Options du diagramme de groupe AD*.
    - *Mettre à jour les alias et les groupes AD maintenant*
    Sélectionnez cette option pour démarrer la mise à jour de tous les alias utilisateur et groupes AD planifiés lorsque vous cliquez sur *Mettre à jour*. Les prochaines mises à jour planifiées sont répertoriées sous *Options du groupe AD* et *Options d'alias AD*.
    - *Ne pas mettre à jour les alias et les groupes AD maintenant*
    Aucun alias utilisateur ou groupe AD ne sera mis à jour lorsque vous cliquerez sur *Mettre à jour*.
21. Cliquez sur *Mettre à jour*, puis sur *OK*.

Pour vérifier que vous avez bien importé les comptes utilisateur AD, accédez à *CMC* > *Utilisateurs et groupes* > *Hiérarchie de groupe* et sélectionnez le groupe AD que vous avez mappé pour voir les utilisateurs de ce groupe. Les utilisateurs actuels et imbriqués du groupe AD s'afficheront.

Informations associées

Création d'un fichier de configuration Kerberos [page 315]

9.4.3.3 Planification des mises à jour des groupes Windows AD

La plateforme de BI permet aux administrateurs de planifier des mises à jour pour des groupes et alias d'utilisateurs AD. Cette fonction est disponible pour l'authentification AD avec Kerberos ou NTLM. La CMC vous permet également de visualiser la date et l'heure d'exécution de la dernière mise à jour.

> **Remarque**
>
> Pour que l'authentification AD fonctionne sur la plateforme de BI, vous devez configurer la méthode de mise à jour des groupes et alias AD.

Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous pouvez spécifier l'heure à laquelle l'exécution démarrera, de même que sa date de début et sa date de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les N jours. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Toutes les semaines	La mise à jour s'exécutera toutes les semaines. Elle peut être exécutée une ou plusieurs fois par semaine. Vous pouvez préciser les jours et l'heure auxquels l'exécution doit avoir lieu, ainsi qu'une date de début et une date de fin.
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour sera exécutée aux dates spécifiées dans un calendrier précédemment créé.

Planification des mises à jour de groupe AD

La plateforme de BI s'appuie sur AD pour les informations utilisateur et les informations de groupe. Pour limiter le volume des requêtes envoyées à AD, le plug-in AD met en cache les informations sur les groupes,

leurs relations, et l'appartenance des utilisateurs aux groupes. La mise à jour ne s'effectue pas si aucune planification spécifique n'est définie.

Vous devez utiliser la CMC pour configurer la récurrence de l'actualisation de la mise à jour de groupe. La planification doit refléter la fréquence à laquelle vous voulez modifier les informations d'appartenance aux groupes.

Planification des mises à jour des alias d'utilisateur AD

Les objets utilisateur peuvent avoir un alias dans un compte AD, ce qui permet aux utilisateurs d'utiliser leurs références de connexion AD pour se connecter à la plateforme de BI. Les mises à jour des comptes AD sont répercutées à la plateforme de BI par le plug-in AD. Les comptes créés, supprimés ou désactivés dans AD le seront également dans la plateforme de BI.

Si vous ne planifiez pas les mises à jour des alias AD, elles se produiront uniquement dans les cas suivants :

- Un utilisateur se connecte.
- Un administrateur sélectionne l'option *Mettre à jour les alias et les groupes AD maintenant* dans la zone *Mise à jour d'AD à la demande* de la CMC.

> **Remarque**
>
> Aucun mot de passe AD n'est stocké dans l'alias utilisateur.

9.4.4 Configuration du service de la plateforme de BI pour l'exécution du SIA

9.4.4.1 Exécution du SIA sous le compte de service de la plateforme de BI

Pour une prise en charge de l'authentification AD Kerberos pour la plateforme de BI, vous devez accorder au compte de service le droit d'agir dans le cadre du système d'exploitation. Vous devez le faire sur chaque ordinateur exécutant un SIA (Server Intelligence Agent) avec le CMS (Central Management Server).

Pour permettre au compte de service d'exécuter ou de démarrer le SIA, vous devez configurer des paramètres de système d'exploitation spécifiques décrits dans cette section.

> **Remarque**
>
> Si vous avez besoin d'une connexion unique à la base de données, le SIA doit inclure les serveurs suivants :
>
> - Crystal Reports Processing Server
> - Report Application Server
> - Web Intelligence Processing Server

9.4.4.2 Configuration du SIA pour une exécution sous le compte de service

Avant de configurer le compte SIA pour une exécution sous le compte de service de la plateforme de BI, vous devez remplir les conditions préalables suivantes :

- Un compte de service a été créé sur le contrôleur de domaine pour la plateforme de BI.
- Vous vous êtes assuré que les noms principaux du service (SPN) requis ont été ajoutés au compte de service.
- Vous avez mappé les groupes d'utilisateurs AD à la plateforme de BI.

Si vous souhaitez accorder des droits spécifiques à l'utilisateur, procédez comme suit :

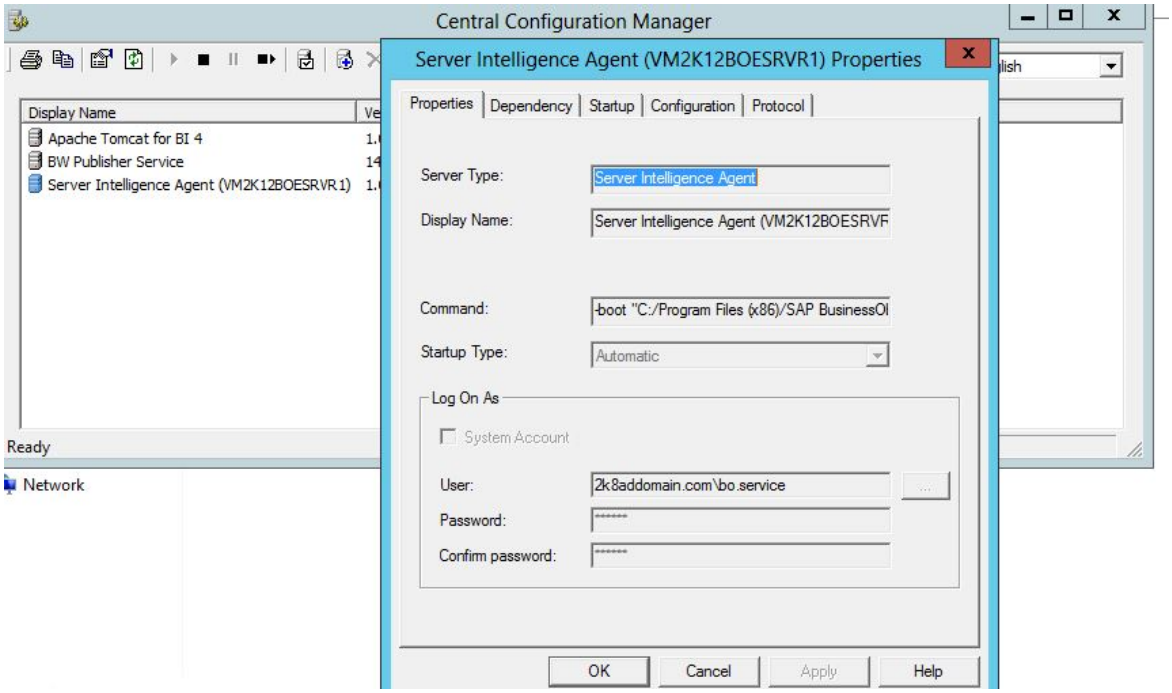
1. Cliquez sur *Démarrer > Panneau de configuration > Outils d'administration > Stratégie de sécurité locale*.
2. Développez *Stratégies locales*, puis cliquez sur *Attribution des droits utilisateur*.
3. Cliquez deux fois sur *Agir en tant que partie du système d'exploitation*.
4. Cliquez sur *Ajouter*, saisissez le nom du compte de service créé, puis cliquez sur *OK*.

Effectuez cette tâche pour tout SIA (Server Intelligence Agent) exécutant les services utilisés par le compte de service.

1. Pour lancer le CCM, sélectionnez *Programmes* > *SAP Business Intelligence* > *Plateforme SAP BusinessObjects BI 4* > *Central Configuration Manager*.
   La page d'accueil du CCM s'ouvre.
2. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Arrêter*.

   > **Remarque**
   >
   > Lorsque vous arrêtez le SIA, tous les services gérés par celui-ci sont arrêtés.

3. Cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*.



4. Désactivez la case à cocher *Compte de système*.
5. Saisissez les références de connexion du compte de service (`<NOMDOMAINE>\<nom du service>`) et cliquez sur *OK*.

   Le compte de service doit disposer des droits suivants sur l'ordinateur exécutant le SIA :

   - Le compte doit disposer spécifiquement du droit « Agir en tant que partie du système d'exploitation ».
   - Le compte doit disposer spécifiquement du droit « Se connecter en tant que service ».
   - Droits de contrôle total sur le dossier où est installée la plateforme de BI.
   - Droits de contrôle total sur « HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects » dans le répertoire système.
6. Répétez les étapes ci-dessus pour chaque ordinateur sur lequel est installé un serveur de la plateforme de BI.

   > **Remarque**
   >
   > Il est important que l'option Droits effectifs soit activée après la sélection de l'option *Agir en tant que partie du système d'exploitation*. En règle générale, vous devez redémarrer le serveur pour ce faire. Si, une fois le serveur redémarré, cette option n'est toujours pas activée, vos paramètres de stratégie locale sont écrasés par vos paramètres de stratégie de domaine.
7. Redémarrez le SIA.
8. Si nécessaire, répétez les étapes 1 à 5 pour chaque SIA exécutant un service à configurer.

Vous devez à présent être en mesure de vous connecter au CCM à l'aide des références de connexion AD.

9.4.4.3 Test des références de connexion AD sur le CCM

Pour effectuer cette tâche, vous devez avoir mappé un groupe d'utilisateurs AD à la plateforme de BI.

1. Ouvrez le CCM, puis cliquez sur l'icône *Gérer les serveurs*.
2. Assurez-vous que les bonnes informations sont affichées dans le champ *Système*.
3. Sélectionnez *Windows AD* dans la liste des options d'authentification.
   Une boîte de dialogue de connexion s'ouvre.
4. Connectez-vous à l'aide d'un compte AD existant du groupe AD que vous avez mappé à la plateforme de BI.

   > **Remarque**
   >
   > Si vous utilisez un compte AD qui ne se trouve pas dans le domaine par défaut, connectez-vous en tant que `domaine\nom d'utilisateur`.

Vous ne devriez pas recevoir de message d'erreur. Vous devez pouvoir vous connecter via le CCM à l'aide d'un compte AD mappé avant de passer à la section suivante.

> **→ Conseil**
>
> Si vous recevez un message d'erreur, accédez à *CMC* > *Authentification* > *Windows AD*. Sous *Options d'authentification*, remplacez *Utiliser l'authentification Kerberos* par *Utiliser l'authentification NTLM*, puis cliquez sur *Mettre à jour*. Répétez les étapes 1 à 4 ci-dessus. Si cela fonctionne, un problème existe avec votre configuration Kerberos.

9.4.5 Configuration du serveur d'applications Web pour l'authentification AD

9.4.5.1 Préparation du serveur d'applications à l'authentification Windows AD (Kerberos)

La procédure de configuration de Kerberos pour un serveur d'applications Web diffère légèrement en fonction du type de serveur d'applications spécifique utilisé. Toutefois, la procédure générale de configuration de Kerberos comprend les étapes suivantes :

- Création du fichier de configuration Kerberos `(krb5.ini)`.
- Création du fichier de configuration de connexion JAAS `bscLogin.conf`.

  > **Remarque**
  >
  > Cette étape n'est pas requise pour le serveur d'applications Java de SAP NetWeaver 7.3. Cependant, vous devrez ajouter le LoginModule à votre serveur SAP NetWeaver.

- Modification des options Java pour votre serveur d'applications.
- Remplacement des propriétés du fichier `BOE.war` pour l'authentification Windows AD.
- Redémarrage du serveur d'applications Java.

Cette section présente les informations de configuration de Kerberos pour une utilisation avec les serveurs d'applications suivants :

- Tomcat

- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Création des fichiers de configuration Kerberos

9.4.5.1.1.1 Création d'un fichier de configuration Kerberos

Avant de poursuivre, assurez-vous d'avoir exécuté les tâches de prérequis suivantes :

- Un compte de service a été créé sur le contrôleur de domaine pour la plateforme de BI.
- Vous vous êtes assuré que les noms principaux du service (SPN) ont été ajoutés au compte de service.
- Vous avez mappé les groupes d'utilisateurs AD à la plateforme de BI.
- Vous avez testé les références de connexion AD sur le CCM.

Procédez comme suit pour créer le fichier de configuration Kerberos si vous utilisez SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere ou WebLogic comme serveur d'applications Web pour le déploiement de votre plateforme de BI.

1. Créez le fichier `krb5.ini` si nécessaire et stockez-le sous `C:\Windows` pour Windows.

   > **Remarque**
   >
   > Si le serveur d'applications est installé sous UNIX, utilisez les répertoires suivants :
   >
   > Solaris : `/etc/krb5/krb5.conf`
   >
   > Linux : `/etc/krb5.conf`

   > **Remarque**
   >
   > Vous pouvez stocker ce fichier à un emplacement différent. Toutefois, vous devrez spécifier son emplacement dans vos options Java. Pour en savoir plus sur `krb5.ini`, allez à l'adresse http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view .

2. Ajoutez les informations requises suivantes dans le fichier de configuration Kerberos :

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
```

```
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

Remarque

Les principaux paramètres sont expliqués dans le tableau ci-dessous.

`DOMAIN.COM`	Nom DNS du domaine. Vous devez le saisir en majuscules au format FQDN.
`kdc`	Nom d'hôte du contrôleur de domaine.
`[capath]`	Définit l'approbation entre les domaines faisant partie d'une autre forêt AD. Dans l'exemple ci-dessus, `DOMAINE2.COM` est un domaine d'une forêt externe et bénéficie d'une approbation directe transitive bidirectionnelle à `DOMAINE.COM`.
`default_realm`	Dans une configuration comportant plusieurs domaines, sous `[libdefaults]`, la valeur `default_realm` peut être n'importe lequel des domaines source. La meilleure solution consiste à utiliser le domaine comportant le plus grand nombre d'utilisateurs qui seront authentifiés à l'aide de leurs comptes AD. Si aucun suffixe UPN n'est fourni à la connexion, la valeur par défaut `default_realm` est utilisée. Cette valeur doit être cohérente avec le paramètre de *domaine par défaut* dans la CMC. Tous les domaines doivent être indiqués en majuscules comme l'illustre l'exemple ci-dessus.

9.4.5.1.2 Création d'un fichier de configuration de connexion JAAS

9.4.5.1.2.1 Création d'un fichier de configuration de connexion JAAS Tomcat ou WebLogic

Le fichier `bscLogin.conf` sert à charger le module de connexion Java et est nécessaire à l'authentification AD Kerberos sur les serveurs d'applications Web Java.

L'emplacement par défaut des fichiers est : `C:\Windows`.

1. Créez un fichier nommé `bscLogin.conf` si nécessaire, puis stockez-le sous `C:\Windows`.

> **Remarque**
>
> Vous pouvez stocker ce fichier à un emplacement différent. Toutefois, si vous le faites, vous devrez spécifier son emplacement dans vos options Java.

2. Ajoutez le code suivant au fichier de configuration JAAS `bscLogin.conf` :

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Enregistrez le fichier et fermez-le.

9.4.5.1.2.2 Création d'un fichier de configuration de connexion JAAS Oracle

1. Recherchez le fichier `jazn-data.xml`.

> **Remarque**
>
> L'emplacement par défaut de ce fichier est `C:\OraHome_1\j2ee\home\config`. Si vous avez installé un serveur d'applications Oracle à un autre emplacement, recherchez le fichier spécifique à votre installation.

2. Ajoutez le contenu suivant au fichier entre les balises `<jazn-loginconfig>` :

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Enregistrez et fermez le fichier `jazn-data.xml`.

9.4.5.1.2.3 Pour créer un fichier de configuration de connexion JAAS Websphere

1. Créez un fichier nommé `bscLogin.conf` si nécessaire, puis stockez-le à l'emplacement par défaut : `C:\Windows`
2. Ajoutez le code suivant au fichier de configuration `bscLogin.conf` :

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Enregistrez le fichier et fermez-le.

9.4.5.1.2.4 Pour ajouter un LoginModule à SAP NetWeaver AS

Pour utiliser Kerberos et SAP NetWeaver AS 7.3, configurez le système comme si vous utilisiez le serveur d'applications Web Tomcat. Vous n'aurez pas à créer de fichier `bscLogin.conf`.

Une fois cette opération effectuée, vous devez ajouter un LoginModule et mettre à jour certains paramètres Java sur SAP NetWeaver AS 7.3.

Pour mapper `com.sun.security.auth.module.Krb5LoginModule` à `com.businessobjects.security.jgss.initiate`, vous devez ajouter manuellement un LoginModule à SAP NetWeaver AS 7.3.

1. Ouvrez l'administrateur SAP NetWeaver en entrant l'adresse suivante dans un navigateur Web : `http://<nom de l'ordinateur>:<port>/nwa`.
2. Cliquez sur *Configuration Management (Gestion de configuration)* > *Security (Sécurité)* > *Authentication (Authentification)* > *Login Modules (Modules de connexion)* > *Edit (Modifier)*.
3. Ajoutez un nouveau module de connexion avec les informations suivantes :

Nom d'affichage	**`Krb5LoginModule`**
Nom de la classe	**`com.sun.security.auth.module.Krb5LoginModule`**

4. Cliquez sur *Enregistrer*.
   SAP NetWeaver crée le module.
5. Cliquez sur *Components (Composants)* > *Edit (Modifier)*.
6. Ajoutez une nouvelle police nommée **`com.businessobjects.security.jgss.initiate`**.
7. Dans *Pile d'authentification*, ajoutez le module de connexion créé à l'étape 3 et définissez-le sur *Requis*.
8. Vérifiez qu'il n'existe aucune autre entrée dans les *Options du module de connexion sélectionné*. Si vous en trouvez, supprimez-les.
9. Cliquez sur *Save (Enregistrer)*.
10. Déconnectez-vous de l'administrateur SAP NetWeaver.

9.4.5.1.3 Modification des paramètres Java du serveur d'applications pour le chargement de fichiers de configuration

9.4.5.1.3.1 Pour modifier les options Java pour Kerberos sur Tomcat

1. Dans le menu *Démarrer*, sélectionnez *Programmes >Tomcat > Configuration Tomcat*.
2. Cliquez sur l'onglet *Java*.
3. Ajoutez les options suivantes :

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
```

```
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

Remplacez XXXX par l'emplacement de stockage du fichier `bscLogin.conf`.

4. Fermez le fichier de configuration Tomcat.
5. Redémarrez Tomcat.

9.4.5.1.3.2 Modification des options Java de SAP NetWeaver AS 7.3

1. Accédez à l'outil de configuration Java (qui se trouve par défaut sous `C:\usr\sap\<ID NetWeaver>\<instance>\j2ee\configtool\`) et cliquez deux fois sur `configtool.bat`.
   L'outil de configuration s'ouvre.
2. Cliquez sur *View (Afficher)* > *Mode Expert (Mode expert)*.
3. Développez *Cluster Data (Données de cluster)* > *Template (Modèle)*.
4. Sélectionnez l'instance qui correspond à votre SAP NetWeaver AS (par exemple *Instance* - `<ID système><nom de l'ordinateur>`).
5. Cliquez sur *Paramètres VM*.
6. Sélectionnez *SAP* dans la liste *Fournisseur* et *GLOBAL* dans la liste *Plateforme*.
7. Cliquez sur *système* et ajoutez les informations des paramètres personnalisés suivants :

java.security.krb5.conf	`<chemin vers le fichier krb5.ini comprenant le nom de fichier>`
javax.security.auth.useSubjectCredsOnly	false

8. Cliquez sur *Enregistrer*, puis cliquez sur *Editeur de configuration*.
9. Cliquez sur *Configurations* > *Security (Sécurité)* > *Configurations* > *com.businessobjects.security.jgss.initiate* > *Securitty (Sécurité)* > *Authentication (Authentification)*.
10. Cliquez sur *Mode Edition*.
11. Cliquez avec le bouton droit sur le nœud *Authentification* et sélectionnez *Créer un sous-nœud*.
12. Sélectionnez *Saisie de valeurs* dans la liste supérieure.
13. Saisissez les informations suivantes :

Nom	create_security_session
Valeur	false

14. Cliquez sur *Créer*, puis fermez la fenêtre.
15. Cliquez sur *Outil de configuration*, puis sur *Enregistrer*.

Après la mise à jour de votre configuration, redémarrez SAP NetWeaver AS.

9.4.5.1.3.3 Pour modifier les options Java pour Kerberos sur WebLogic

Si vous utilisez Kerberos avec WebLogic, vous devez modifier les options Java pour indiquer l'emplacement du fichier de configuration Kerberos, ainsi que le module de connexion Kerberos.

1. Arrêtez le domaine WebLogic qui exécute les applications de la plateforme de BI.
2. Ouvrez le script qui démarre le domaine de WebLogic exécutant les applications de votre plateforme de BI (`startWeblogic.cmd` pour Windows, `startWebLogic.sh` pour UNIX).
3. Ajoutez les informations suivantes à la section Java_Options du fichier :

   ```
   set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
   -Djava.security.krb5.conf=C:/XXX/krb5.ini
   ```

   Remplacez XXX par l'emplacement de stockage du fichier.
4. Redémarrez le domaine de WebLogic qui exécute les applications de la plateforme de BI.

9.4.5.1.3.4 Pour modifier les options Java pour Kerberos sur WebSphere

1. Connectez-vous à la console d'administration de WebSphere.

   Pour IBM WebSphere 5,1, saisissez `http://nomserveur:9090/admin`. Pour IBM WebSphere 6.0, saisissez `http://nomserveur:9060/admin/`
2. Développez Serveur, cliquez sur *Serveurs d'applications*, puis sur le nom du serveur d'applications que vous avez créé pour l'utiliser avec la plateforme de BI.
3. Accédez à la page *JVM*.

   Si vous utilisez WebSphere 5.1, effectuez les étapes suivantes pour accéder à la page *JVM*.
   1. Faites défiler la page du serveur vers le bas jusqu'à ce qu'apparaisse *Définition de processus* dans la colonne *Autres propriétés*.
   2. Cliquez sur *Définition de processus*.
   3. Faites défiler l'écran vers le bas et cliquez sur *Machine virtuelle Java*.

   Si vous utilisez WebSphere 6.0, effectuez les étapes suivantes pour accéder à la page *JVM*.
   1. Dans la page du serveur, sélectionnez *Gestion de processus et Java*.
   2. Sélectionnez *Définition de processus*.
   3. Sélectionnez *Machine virtuelle Java*.
4. Cliquez sur *Generic JVM arguments* (Arguments JVM génériques), puis spécifiez l'emplacement du fichier `Krb5.ini` et du fichier `bscLogin.conf` comme illustré ci-dessous.

   -Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

   -Djava.security.krb5.conf=C:\XXXX\krb5.ini

   Remplacez XXX par l'emplacement de stockage du fichier.
5. Cliquez sur *Appliquer*, puis sur *Enregistrer*.
6. Arrêtez puis redémarrez le serveur.

9.4.5.1.4 Vérification concernant la réception du ticket Kerberos par Java

Avant de tester si Java a reçu le ticket Kerberos, vous devez respecter les actions pré-requises suivantes :

- Créez le fichier `bscLogin.conf` pour votre serveur d'applications.
- Créez le fichier `krb5.ini`.

1. Accédez à l'invite de commande et au répertoire `jdk\bin` de votre installation de la plateforme de BI.

   Par défaut, il se trouve à l'emplacement suivant :
   `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Exécutez `kinit <nom d'utilisateur>`.
3. Appuyez sur `Entrée`.
4. Tapez votre mot de passe.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

   Si le fichier `krb5.ini` a été correctement configuré et que le module de connexion Java a été chargé, vous devez voir le message suivant :

```
Le nouveau ticket est stocké dans le fichier cache
C:\Users\Administrator\krb5cc_Administrator
```

Ne poursuivez pas la configuration AD tant que vous n'avez pas reçu de ticket Kerberos.

Si vous ne pouvez pas recevoir de ticket, envisagez les solutions suivantes :

- Consultez la section de dépannage à la fin de ce chapitre.
- Pour les problèmes concernant le KDC, les fichiers de configuration Kerberos et les références de connexion utilisateur non disponibles dans la base de données Kerberos, voir les articles KBA 1476374 et KBA 1245178 de la Base de connaissances SAP.

9.4.5.1.5 Configuration de la zone de lancement BI pour une connexion AD manuelle

Avant de configurer les applications de la plateforme de BI pour la connexion AD manuelle, vous devez avoir respecté les actions prérequises suivantes :

- Vous avez créé un compte de service sur le contrôleur de domaine pour la plateforme de BI.
- Vous vous êtes assuré que les noms principaux du service (SPN) HTTP ont été ajoutés au compte de service.
- Vous avez mappé les groupes d'utilisateurs AD à la plateforme de BI.
- Vous avez testé les références de connexion AD sur le CCM.
- Vous avez créé, configuré et testé les fichiers de configuration requis pour votre serveur d'applications Web.

- Les paramètres Java de votre serveur d'applications ont été modifiés pour charger les fichiers de configuration.

Pour activer l'option d'authentification Windows AD pour la zone de lancement BI, procédez comme suit :

1. Accédez au dossier personnalisé pour l'application Web BOE sur l'ordinateur hébergeant le serveur d'applications Web.

   `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Effectuez vos modifications dans le répertoire `config\custom` et non dans `config\default`. Sinon, vos modifications seront remplacées lorsque de futurs correctifs seront appliqués à votre déploiement.

   Vous devrez redéployer ultérieurement l'application Web BOE modifiée.
2. Créez un fichier.

   > **Remarque**
   >
   > Utilisez Notepad ou tout autre éditeur de texte.
3. Enregistrez le fichier sous `BIlaunchpad.properties`.
4. Saisissez ce qui suit :

   ```
   authentication.visible=true
   authentication.default=secWinAD
   ```
5. Enregistrez le fichier et fermez-le.
6. Redémarrez le serveur d'applications Web.

Vous devez désormais pouvoir vous connecter manuellement à la zone de lancement BI, accéder à l'une des applications et sélectionner Windows AD dans la liste des options d'authentification.

> **Remarque**
>
> Ne poursuivez pas la configuration de Windows AD tant que vous ne pouvez pas vous connecter manuellement à la zone de lancement BI à l'aide d'un compte AD existant.

Les nouvelles propriétés ne prendront effet qu'après le redéploiement de l'application Web BOE sur l'ordinateur exécutant le serveur d'applications Web. Utilisez Wdeploy pour redéployer BOE sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

> **Remarque**
>
> Si votre déploiement utilise un pare-feu, pensez à ouvrir tous les ports requis, sans quoi les applications Web ne parviendront pas à se connecter aux serveurs de la plateforme de BI.

9.4.6 Configuration de la connexion unique

9.4.6.1 Connexion unique à la plateforme de BI avec l'authentification AD

Options de la connexion unique utilisant Windows AD

Trois méthodes sont prises en charge pour configurer la connexion unique pour l'authentification Windows AD avec la plateforme de BI :

- Vintela : cette option ne peut être utilisée qu'avec Kerberos.
- SiteMinder : cette option ne peut être utilisée qu'avec Kerberos.

Connexion unique à la base de données

La connexion unique à la base de données permet aux utilisateurs connectés d'effectuer des actions nécessitant un accès à la base de données, en particulier, l'affichage et l'actualisation de rapports, sans devoir spécifier à nouveau leurs références de connexion. Bien que la restriction de délégation soit facultative pour la connexion unique Vintela et l'authentification AD, elle est requise pour les scénarios de déploiement impliquant une connexion unique à la base de données système.

Connexion unique de bout en bout

Sur la plateforme de BI, la connexion unique de bout en bout est prise en charge par l'intermédiaire de Windows AD et de Kerberos. Dans ce scénario, les utilisateurs disposent à la fois de la connexion unique à la plateforme de BI au niveau interface client et de la connexion unique aux bases de données principales. Ainsi, les utilisateurs ne doivent fournir leurs références de connexion qu'une seule fois, lorsqu'ils se connectent au système d'exploitation, pour accéder à la plateforme de BI et effectuer des actions requérant un accès à la base de données, telles que l'affichage de rapports.

Configuration de l'authentification AD manuelle ou par connexion unique

Une fois votre déploiement correctement configuré pour permettre aux comptes AD de se connecter manuellement à la zone de lancement BI, vous devez revoir la configuration de l'authentification AD pour activer certaines conditions de connexion unique. Les conditions requises varient selon la méthode de connexion unique choisie.

9.4.6.2 Utilisation de la connexion unique Vintela

9.4.6.2.1 Liste de contrôle pour la configuration de la connexion unique Vintela

Pour configurer la plateforme de BI de sorte à pouvoir utiliser la connexion unique Vintela, vous devez exécuter les tâches suivantes :

1. Configurer votre compte de service spécifiquement pour la connexion unique Vintela.
2. Configurer la restriction de délégation (facultatif).
3. Configurer les options d'authentification de la connexion unique Windows AD dans la CMC.
4. Configurer les propriétés générales et les propriétés spécifiques à la zone de lancement BI pour la connexion unique Vintela.
5. Si vous utilisez Tomcat comme serveur d'applications Web sur votre déploiement, vous devez augmenter la taille limite d'en-tête.
6. Configurez les navigateurs Internet pour Vintela.

9.4.6.2.2 Configuration du compte de service pour la connexion unique Vintela

L'outil de ligne de commande `Ktpass` configure le nom principal de serveur pour l'hôte ou le service d'Active Directory et génère un fichier "keytab" Kerberos contenant la clé de secret partagé du compte de service. Cet outil se trouve généralement sur les contrôleurs de domaine ou peut être téléchargé depuis le site de support de Microsoft : http://support.microsoft.com/kb/892777 .

Votre compte de service doit être configuré spécifiquement pour permettre aux utilisateurs d'un groupe Windows AD donné de s'authentifier automatiquement auprès de la zone de lancement BI à l'aide de leurs références de connexion. Vous pouvez reconfigurer le compte de service créé pour l'authentification AD Kerberos sur le contrôleur de domaine.

Lorsqu'un client tente de se connecter à la zone de lancement BI, une requête au serveur générant les tickets Kerberos est initiée. Pour faciliter cette requête, le compte de service créé pour la plateforme de BI doit avoir un SPN correspondant à l'URL du serveur d'applications. Procédez comme suit sur l'ordinateur hébergeant le contrôleur de domaine.

1. Exécutez la commande de configuration keytab de Kerberos `ktpass` pour créer et placer un fichier `keytab`.

   Spécifiez les paramètres `ktpass` répertoriés dans le tableau suivant :

Paramètre	Description
`-out`	Spécifie le nom du fichier `keytab` Kerberos à générer.

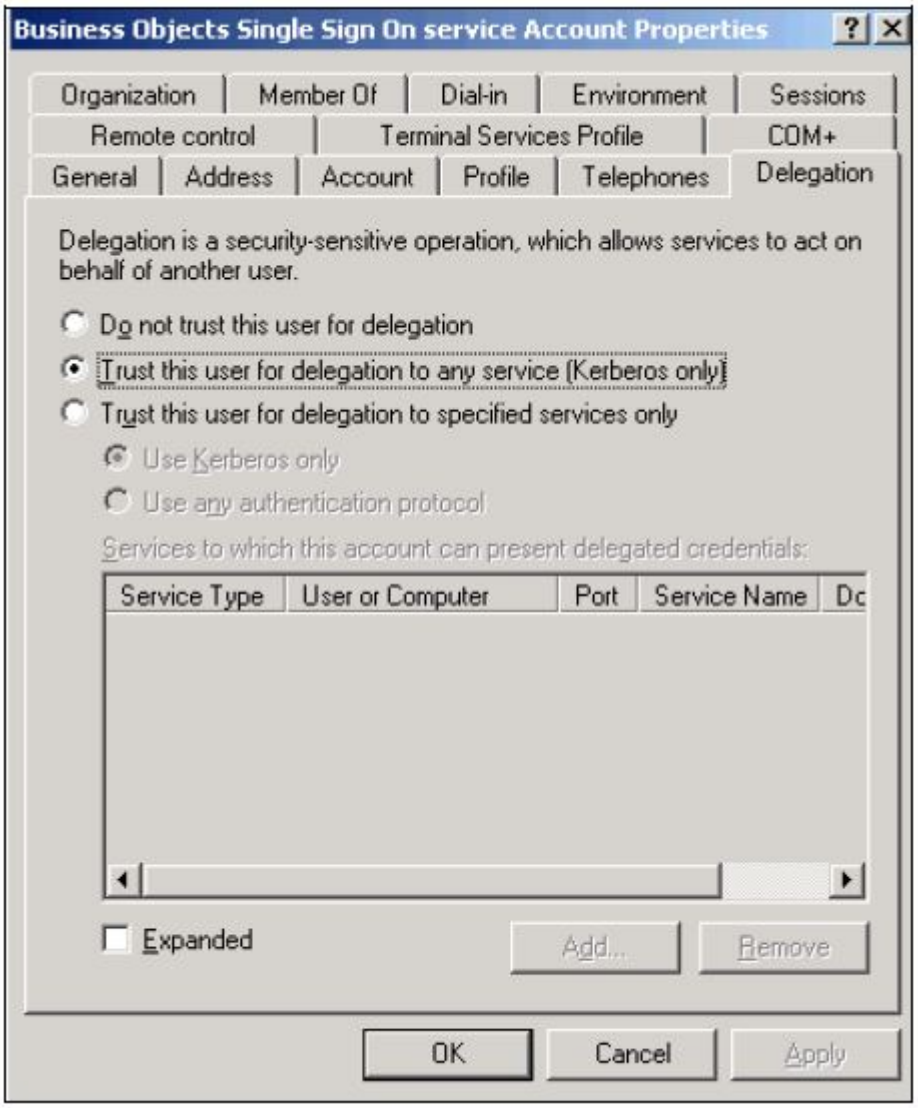
Paramètre	Description
`-princ`	Spécifie le nom principal utilisé pour le compte de service au format SPN :`< MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM`, où `<MYSIAMYSERVER>` est le nom du Service Intelligence Agent spécifié dans le CCM (Central Configuration Manager). **Remarque** Le nom de votre compte de service respecte la casse. Le SPN inclut le nom de l'ordinateur hôte sur lequel l'instance de service est exécutée. **Conseil** Le SPN doit être unique dans la forêt dans laquelle il est enregistré. Pour vérifier, utilisez l'outil de support Windows `Ldp.exe` pour rechercher le SPN.
`-pass`	Indique le mot de passe utilisé par le compte de service.
`-ptype`	Spécifie le type principal. `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Spécifie le type de cryptage à utiliser avec le compte de service : `-crypto RC4-HMAC-NT`

Par exemple :

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Le résultat de la commande `ktpass` doit confirmer le contrôleur de domaine cible et la création d'un fichier `keytab` Kerberos contenant le secret partagé. La commande mappe également le nom principal du compte de service (local).

2. Cliquez avec le bouton droit de la souris sur le compte de service et sélectionnez *Propriétés* > *Délégation*.
3. Cliquez sur *Approuver cet utilisateur pour la délégation à tous les services (Kerberos uniquement)*.



4. Cliquez sur *OK* pour enregistrer vos paramètres.

Ce compte de service a désormais tous les noms principaux de service nécessaires à la connexion unique Vintela et vous avez généré un fichier Keytab avec le mot de passe crypté pour le compte de service.

> **Remarque**
>
> Pour la connexion unique de bout en bout ou la connexion unique aux bases de données avec des scénarios de fichier Keytab :
>
> Si des échecs sont résolus en modifiant KVNO dans le fichier Keytab, il est probable que l'attribut KVNO dans le compte de service soit supérieur au KVNO utilisé dans la création du fichier Keytab (lors de ktpass). Pour en savoir plus sur l'obtention du KV correct, voir http://service.sap.com/sap/support/notes/1853668

9.4.6.2.2.1 Configuration d'une restriction de délégation pour la connexion unique Vintela

La restriction de délégation est facultative pour la configuration de la connexion unique Vintela. Elle est toutefois requise pour les déploiements exigeant une connexion unique à la base de données système.

1. Sur l'ordinateur du contrôleur de domaine AD, ouvrez le composant enfichable *Utilisateurs et ordinateurs* Active Directory.
2. Cliquez avec le bouton droit de la souris sur le compte de service créé dans la section précédente, puis cliquez sur *Propriétés* > *Délégation*.
3. Sélectionnez *N'approuver cet ordinateur que pour la délégation aux services spécifiés*.
4. Sélectionnez *Utiliser uniquement Kerberos*.
5. Cliquez sur *Ajouter* > *Utilisateurs ou ordinateurs*.
6. Saisissez le nom du compte de service et cliquez sur *OK*.
   Une liste de services s'affiche.
7. Sélectionnez les services suivants, puis cliquez sur *OK*.
   - Le service HTTP
   - Le service utilisé pour exécuter le SIA (Service Intelligence Agent) sur l'ordinateur hébergeant la plateforme de BI.

   Les services sont ajoutés à la liste de services pouvant être délégués pour le compte de service.

Vous devrez modifier les propriétés de l'application Web pour justifier cette modification.

9.4.6.2.3 Configuration des paramètres de connexion unique dans la CMC

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Windows AD*.
3. Vérifiez que la case *Activer Windows Active Directory (AD)* est cochée.
4. Sous *Options d'authentification*, assurez-vous que l'option *Utiliser l'authentification Kerberos* est sélectionnée.
5. Si votre configuration requiert une connexion unique à la base de données, sélectionnez *Contexte de sécurité de la mémoire cache*.
6. Sélectionnez *Activez la connexion unique pour le mode d'authentification sélectionné*.
7. Cliquez sur *Mettre à jour*.

9.4.6.2.4 Activation de la connexion unique Vintela pour la zone de lancement BI et OpenDocument

Cette procédure doit être utilisée pour la zone de lancement BI ou OpenDocument. Pour activer la connexion unique aux applications Web de la plateforme de BI, vous devez spécifier les propriétés propres à Vintela et à

la connexion unique dans le fichier `BOE.war`. Pour des raisons de configuration de la connexion unique, il est recommandé de se focaliser sur l'activation de la connexion unique à la zone de lancement BI pour les comptes AD avant de traiter d'autres applications.

1. Accédez au dossier personnalisé pour l'application Web BOE sur l'ordinateur hébergeant le serveur d'applications Web.

   `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Effectuez vos modifications dans le répertoire `config\custom` et non dans le répertoire `config\default`. Sinon, vos modifications seront remplacées lorsque de futurs correctifs seront appliqués à votre déploiement.

   Vous devrez redéployer ultérieurement l'application Web BOE modifiée.
2. Créez un fichier dans un éditeur de texte.
3. Saisissez les informations suivantes :

   ```
   sso.enabled=true
   siteminder.enabled=false
   vintela.enabled=true
   idm.realm=DOMAIN.COM
   idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
   idm.allowUnsecured=true
   idm.allowNTLM=false
   idm.logger.name=simple
   idm.keytab=C:/WIN/filename.keytab
   idm.logger.props=error-log.properties
   ```

   > **Remarque**
   >
   > Les paramètres `idm.realm` et `idm.princ` requièrent des valeurs valides. `idm.realm` doit comporter la même valeur que celle définie lors de la configuration de `default_realm` dans votre fichier `krb5.ini`. Cette valeur doit être en majuscules. Le paramètre `idm.princ` est le SPN utilisé pour le compte de service créé pour la connexion unique Vintela.

   > **Remarque**
   >
   > Les barres obliques sont obligatoires pour spécifier l'emplacement du fichier Keytab.

   Passez l'étape suivante si vous ne souhaitez pas utiliser de restriction de délégation pour l'authentification Windows AD et la connexion unique Vintela.
4. Pour utiliser l'ajout de restriction de délégation, ajoutez :

   ```
   idm.allowS4U=true
   ```
5. Fermez le fichier et enregistrez-le sous le nom `global.properties` :

   > **Remarque**
   >
   > Vérifiez que le nom de fichier n'est pas enregistré sous une autre extension telle que `.txt`.
6. Créez un autre fichier dans le même répertoire. Enregistrez le fichier sous `OpenDocument.properties` ou `BIlaunchpad.properties` selon vos besoins.
7. Saisissez ce qui suit :

   ```
   authentication.default=secWinAD
   ```

```
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Par exemple :

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Enregistrez le fichier et fermez-le.
9. Redémarrez le serveur d'applications Web.

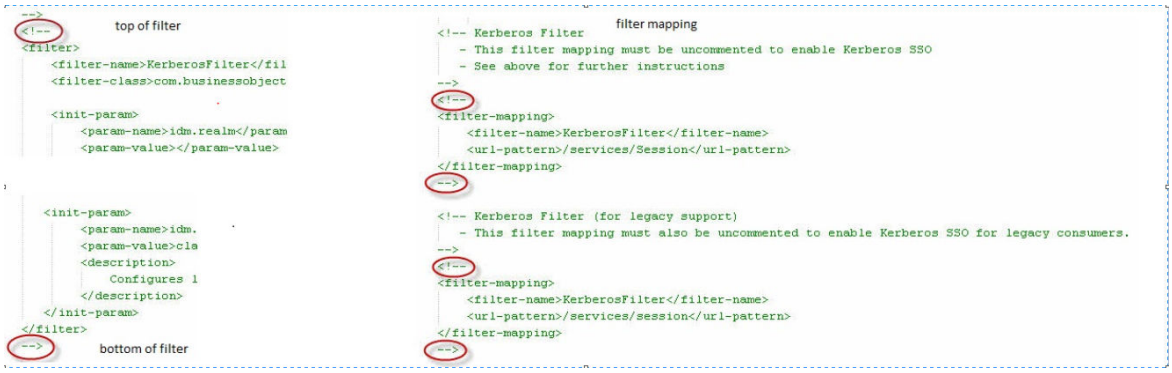
Les nouvelles propriétés ne prendront effet qu'après le redéploiement de l'application Web BOE sur l'ordinateur exécutant le serveur d'applications Web. Utilisez Wdeploy pour redéployer BOE sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects de Business Intelligence*.

> **Remarque**
>
> Si votre déploiement utilise un pare-feu, pensez à ouvrir tous les ports requis, sans quoi les applications Web ne parviendront pas à se connecter aux serveurs de la plateforme de BI.

9.4.6.2.5 Pour activer la connexion unique Vintela pour les services Web

Certains outils client nécessitent une authentification par les services Web. Suivez ces étapes pour activer la connexion unique (SSO) pour les services Web. Pour en savoir plus, consultez la note SAP à l'adresse : http://service.sap.com/sap/support/notes/1646920

1. Sauvegardez ce fichier : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml`, puis ouvrez-le pour le modifier.
2. Supprimez les marques de commentaire des sections Kerberos Proxy Filter et Kerberos Filter pour activer la connexion unique Kerberos pour l'authentification Windows Active Directory (secWinAD).



Les options suivantes doivent être spécifiées (les autres sont facultatives) :

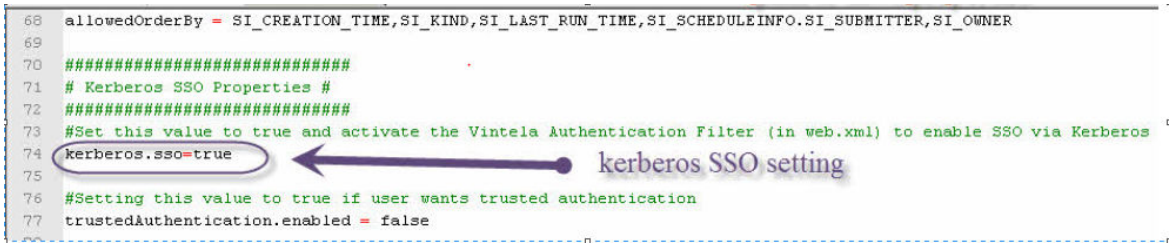
- `idm.realm` (identique à l'option default_realm spécifiée dans le fichier Krb5.ini).
- `idm.princ` (identique à l'option spécifiée pour idm.princ dans le fichier global.properties situé à l'emplacement `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

- `idm.keytab` (identique à l'option spécifiée pour idm.keytab dans le fichier global.properties situé à l'emplacement `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

> **Remarque**
>
> Si vous utilisez le mot de passe figé dans le code défini dans les options Java de Tomcat, n'apportez aucune modification aux lignes keytab dans le fichier `web.xml`.

3. Si SSL n'est pas utilisé avec le serveur d'applications Java, définissez le paramètre idm.allowUnsecured sur **`true`**.

   Pour en savoir plus sur Tomcat SSL, voir l'article 1484802 de la base de connaissances.
4. Sauvegardez ce fichier : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties`, puis ouvrez-le pour le modifier.
5. Définissez le paramètre kerberos.sso sur **`true`** et enregistrez le fichier.



6. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web.

   Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.
7. Redémarrez Tomcat.
8. Pour tester vos paramètres, sur l'ordinateur client où les outils client sont installés, lancez Query as a Web Service Designer.
9. Ajoutez un nouvel hôte géré.
10. Saisissez le nom du serveur d'applications.
11. Entrez l'URL des services Web selon ce format : `http://<ServeurAppWeb>:<NuméroPort>/dswsbobje/services/Session`.

    Exemple : `http://BI4:8080/dswsbobje/services/Session`.
12. Saisissez le nom d'hôte du CMS.
13. Remplacez le type d'authentification par *Windows AD*.
14. Sélectionnez *Activer la connexion unique Windows Active Directory*.
15. A l'invite de connexion, laissez vides les champs *Utilisateur* et *Mot de passe*, puis cliquez sur *OK*.

9.4.6.2.6 Pour activer la connexion unique Vintela pour les services Web RESTful

Certains outils client nécessitent une authentification par les services Web RESTful. Suivez ces étapes pour activer la connexion unique (SSO) pour les services Web.

1. Copiez le fichier `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\biprws.properties` vers `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties`, et ouvrez-le pour le modifier.
2. Pour activer la connexion unique Kerberos pour l'authentification Windows Active Directory (secWinAD), définissez `sso.enabled` sur `true`. Consultez la capture d'écran ci-dessous :

```
# ------------------------------------------------------ SSO Related Default Global Core Web Properties ------------------------------------------------------
# Vintela single sign on properties
sso.enabled=
idm.realm=
idm.princ=
idm.keytab=
idm.allowUnsecured=
idm.allowNTLM=
idm.logger.name=
idm.logger.props=
```

   Spécifiez les options obligatoires suivantes :
   - `idm.realm` (identique à l'option default_realm spécifiée dans le fichier Krb5.ini).
   - `idm.princ` (identique à l'option spécifiée pour idm.princ dans le fichier global.properties situé à l'emplacement `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - `idm.keytab` (identique à l'option spécifiée pour idm.keytab dans le fichier global.properties situé à l'emplacement `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - Le paramètre `idm.allowUnsecured` doit être défini sur `true` si SSL n'est pas utilisé avec le serveur d'applications Java. Pour en savoir plus sur Tomcat SSL, voir l'*article 1484802 de la base de connaissances*.
3. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.
4. Redémarrez Tomcat.
5. Pour tester vos paramètres, sur l'ordinateur client, ouvrez un navigateur et lancez l'URL : http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso.
   Le jeton REST doit s'afficher comme une réponse à l'API.

9.4.6.2.7 Pour augmenter la limite de taille d'en-tête pour Tomcat

Active Directory crée un jeton Kerberos utilisé lors de la procédure d'authentification. Ce jeton est stocké dans l'en-tête HTTP. Votre serveur d'applications Java aura une taille d'en-tête HTTP par défaut. Pour éviter les erreurs, vérifiez que sa taille par défaut minimale est de 16384 octets. (Certains déploiement peuvent nécessiter une taille supérieure. Pour en savoir plus, voir les directives de dimensionnement de Microsoft sur son site de support (http://support.microsoft.com/kb/327825).)

1. Sur le serveur sur lequel Tomcat est installé, ouvrez le fichier `server.xml`.

   Sous Windows, il est situé dans `<REPINSTALLTomcat>/conf`
   - Si vous utilisez la version de Tomcat installée avec la plateforme de BI sous Windows et que vous n'avez pas modifié
     l'emplacement d'installation par défaut, remplacez `<REPINSTALLTomcat>` par :`C:\Program Files (x86)\SAP BusinessObjects\Tomcat\`
   - Si vous utilisez tout autre serveur d'applications Web pris en charge, consultez la documentation de votre serveur d'applications Web pour déterminer le chemin approprié.

2. Recherchez la balise `<Connector …>` du numéro de port que vous avez configuré.

   Si vous utilisez le port par défaut 8080, recherchez la balise `<Connector …>` comportant port=« 8080 ».

   Par exemple :

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Ajoutez la valeur suivante dans la balise `<Connector …>` :

   `maxHttpHeaderSize="16384"`

   Par exemple :

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080"
redirectPort="8443" />
```

4. Enregistrez et fermez le fichier `server.xml`.
5. Redémarrez Tomcat.

> **Remarque**
>
> Pour les autres serveurs d'applications Java, consultez la documentation correspondante.

9.4.6.2.8 Configuration des navigateurs Internet

Pour prendre en charge l'authentification AD Kerberos avec la connexion unique Vintela, vous devez configurer les clients de la plateforme de BI. Cela comprend la configuration du navigateur Web sur les ordinateurs clients.

9.4.6.2.8.1 Pour configurer Internet Explorer sur les ordinateurs client

1. Sur l'ordinateur client, ouvrez un navigateur Internet Explorer.
2. Activez l'authentification intégrée de Windows.
   a. Dans le menu *Outils*, cliquez sur *Options Internet*.
   b. Cliquez sur l'onglet *Avancé*.
   c. Accédez à *Sécurité*, sélectionnez *Activer l'authentification intégrée de Windows*, puis cliquez sur *Appliquer*.
3. Ajoutez le serveur d'applications Java ou l'URL des sites fiables. Vous pouvez saisir le nom de domaine complet du site.

a. Dans le menu *Outils*, cliquez sur *Options Internet*.
b. Cliquez sur l'onglet *Sécurité*.
c. Cliquez sur *Sites*, puis sur *Avancés*.
d. Sélectionnez ou saisissez le site, puis cliquez sur *Ajouter*.
e. Cliquez sur *OK* jusqu'à ce que la boîte de dialogue Options Internet se ferme.

4. Fermez et rouvrez la fenêtre de navigateur Internet Explorer pour appliquer ces modifications.
5. Répétez toutes ces étapes pour chaque ordinateur client de la plateforme de BI.

9.4.6.2.8.2 Pour configurer Firefox sur les ordinateurs client

1. *Modifiez network.negotiate-auth.delegation-uris*
   a. Sur l'ordinateur client, ouvrez un navigateur Firefox.
   b. Saisissez **`about:config`** dans le champ de l'adresse URL.
   Une liste de propriétés configurables s'affiche.
   c. Cliquez deux fois sur *network.negotiate-auth.delegation-uris* pour modifier la propriété.
   d. Saisissez l'URL que vous utiliserez pour accéder à la zone de lancement BI.

   Par exemple, si l'URL de votre zone de lancement BI est http://**`ordinateur.domaine.com<:8080/BOE/BI>`**, vous devrez saisir **`http://<ordinateur.domaine.com>`**.

   > ⓘ Remarque
   >
   > Pour ajouter plusieurs URL, séparez-les par des virgules. Par exemple : **`http://<ordinateur.domaine.com>,<ordinateur2.domaine.com>`** .

   e. Cliquez sur *OK*.
2. *Modifiez network.negotiate-auth.trusted-uris*
   a. Sur l'ordinateur client, ouvrez un navigateur Firefox.
   b. Saisissez **`about:config`** dans le champ de l'adresse URL.
   Une liste de propriétés configurables s'affiche.
   c. Cliquez deux fois sur *network.negotiate-auth.trusted-uris* pour modifier la propriété.
   d. Saisissez l'URL que vous utiliserez pour accéder à la zone de lancement BI.
   Par exemple, si l'URL de votre zone de lancement BI est **`http://<ordinateur.domaine.com>:8080/BOE/BI`**, vous devrez saisir **`http://<ordinateur.domaine.com>`**.

   > ⓘ Remarque
   >
   > Pour ajouter plusieurs URL, séparez-les par des virgules. Par exemple : **`http://<ordinateur.domaine.com>,<ordinateur2.domaine.com>`** .

   e. Cliquez sur *OK*.
3. Fermez et rouvrez la fenêtre de navigateur Firefox pour appliquer ces modifications.
4. Répétez toutes ces étapes pour chaque ordinateur client de la plateforme de BI.

9.4.6.2.9 Test de la connexion unique Vintela pour l'authentification AD Kerberos

Vous devez tester la configuration de votre connexion unique depuis un poste de travail client. Assurez-vous que le client est sur le même domaine que votre déploiement de la plateforme de BI et que vous êtes connecté au poste de travail en tant qu'utilisateur mappé. Ce compte utilisateur doit pouvoir se connecter manuellement à la zone de lancement BI.

Pour tester la connexion unique, ouvrez un navigateur et saisissez l'URL de la zone de lancement BI. Si la connexion unique est correctement configurée, vous ne devriez pas être invité à saisir vos références de connexion.

> → Conseil
>
> Il est recommandé de tester différents scénarios d'utilisateur AD de votre déploiement. Par exemple, si votre environnement est destiné à accueillir des utilisateurs de plusieurs systèmes d'exploitation, vous devriez tester la connexion unique pour des utilisateurs de chaque système. Vous devriez également tester la connexion unique avec tous les navigateurs pris en charge par votre organisation. Si votre environnement est destiné à accueillir des utilisateurs de plusieurs forêts ou domaines, vous devriez tester la connexion unique pour un compte utilisateur de chaque domaine ou forêt.

9.4.6.2.10 Configuration de Kerberos et d'une connexion unique à la base de données pour les serveurs d'applications

La connexion unique à la base de données est prise en charge pour les déploiements répondant à toutes les exigences suivantes :

- Le déploiement de la plateforme de BI se situe sur un serveur d'applications Web.
- Le serveur d'applications Web a été configuré pour l'authentification AD par connexion unique Vintela.
- La base de données pour laquelle une connexion unique est requise est une version prise en charge de SQL Server ou Oracle.
- Les groupes ou utilisateurs devant accéder à la base de données doivent disposer de droits d'accès à SQL Server ou Oracle.

L'étape finale consiste à modifier le fichier `krb5.ini` afin de prendre en charge la connexion unique à la base de données pour les applications Web.

9.4.6.2.10.1 Pour activer la connexion unique à la base de données pour les serveurs d'applications Java

1. Ouvrez le fichier `krb5.ini` utilisé pour le déploiement de la plateforme de BI.

   L'emplacement par défaut de ce fichier est le répertoire WIN du serveur d'applications Web.

> **Remarque**
>
> Si vous ne parvenez pas à localiser ce fichier dans le répertoire WIN, tapez l'argument Java suivant pour déterminer son emplacement :
>
> ```
> -Djava.security.auth.login.config
> ```
>
> Cette variable est spécifiée lors de la configuration d'AD avec Kerberos sur le serveur d'applications Web.

2. Accédez à la section `[libdefaults]` du fichier.
3. Entrez la chaîne suivante avant le début de la section `[realms]` du fichier :

   ```
   forwardable=true
   ```

4. Enregistrez le fichier et fermez-le.
5. Redémarrez le serveur d'applications Web.

La connexion unique à la base de données ne sera activée que lorsque vous aurez coché la case *Contexte de sécurité de la mémoire cache (obligatoire pour une connexion unique à la base de données)* dans la page d'authentification Windows AD de la CMC.

9.4.6.3 Utilisation de SiteMinder

9.4.6.3.1 Utilisation de Windows AD avec SiteMinder

Cette section explique comment utiliser AD et SiteMinder. SiteMinder est un outil tiers qui permet l'authentification et l'accès des utilisateurs et qui peut être employé avec le plug-in de sécurité AD pour créer une connexion unique à la plateforme de BI. Vous pouvez utiliser SiteMinder avec Kerberos.

Assurez-vous que les ressources de gestion de l'identité de SiteMinder sont installées et configurées avant de configurer l'authentification Windows AD en vue d'un fonctionnement avec SiteMinder. Pour en savoir plus sur SiteMinder et sur son installation, reportez-vous à sa documentation.

Pour activer la connexion unique AD avec SiteMinder, vous devez exécuter deux tâches :

- Configurer le plug-in AD pour la connexion unique avec SiteMinder
- Configurer les propriétés de SiteMinder pour l'application Web BOE

> **Remarque**
>
> Vérifiez que l'administrateur SiteMinder a activé la prise en charge des agents 4.x. Cette activation doit être effectuée quelle que soit la version SiteMinder prise en charge que vous utilisez. Pour en savoir plus sur la configuration de SiteMinder, reportez-vous à la documentation relative à SiteMinder.

9.4.6.3.1.1 Activation des propriétés de SiteMinder pour la zone de lancement BI

Les paramètres de SiteMinder doivent être spécifiés pour le plug-in de sécurité Windows AD, mais aussi pour le fichier de propriétés war de BOE.

1. Recherchez le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` dans l'installation de la plateforme de BI.
2. Créez un fichier dans le répertoire à l'aide de Notepad ou d'un autre éditeur de texte.
3. Dans le nouveau fichier, saisissez les valeurs suivantes :

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Enregistrez le fichier sous le nom `global.properties`.

> **Remarque**
>
> Vérifiez que le nom de fichier n'est pas enregistré avec une autre extension telle que `.txt`.

5. Créez un autre fichier dans le même répertoire.
6. Dans le nouveau fichier, saisissez les valeurs suivantes :

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

Par exemple :

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Enregistrez le fichier sous le nom `BIlaunchpad.properties` et fermez-le.

Les nouvelles propriétés ne prennent effet qu'après redéploiement de BOE.war sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

9.4.6.3.1.2 Configuration des paramètres SiteMinder dans la CMC

Avant de configurer la CMC pour SiteMinder, vous devez respecter les actions pré-requises suivantes :

- Vous avez mappé les groupes d'utilisateurs AD à la plateforme de BI.
- Vous avez testé les références de connexion AD sur le CCM.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Windows AD*.

3. Cochez la case *Activer Windows Active Directory (AD)*.
4. Sous Options d'authentification, sélectionnez *Utiliser l'authentification NTLM* ou *Utiliser l'authentification Kerberos*.

   Pour configurer la plateforme de BI pour l'authentification Kerberos et AD à l'aide de Kerberos, vous devez avoir un compte de service. Vous pouvez utiliser un compte de domaine existant ou en créer un nouveau. Le compte de service sera utilisé pour exécuter les serveurs de la plateforme de BI.

   > → Conseil
   >
   > En cas de connexion manuelle à la zone de lancement BI, les utilisateurs issus d'autres domaines doivent faire suivre leur nom d'utilisateur du nom du domaine en majuscules. Par exemple, dans `utilisateur@DOMAINEENFANT.PARENT.COM`, « DOMAINEENFANT.PARENT.COM » est le domaine.

5. Si vous avez sélectionné *Utiliser l'authentification Kerberos* :
   a. Si vous souhaitez configurer une connexion unique à une base de données, sélectionnez *Contexte de sécurité de la mémoire cache*.
   b. Supprimez toutes les informations de la zone *Nom principal du service*.
6. Pour configurer une connexion unique, sélectionnez *Activer la connexion unique pour le mode d'authentification sélectionné*.

   Vous devez également configurer les propriétés générales de l'application Web BOE et de la zone de lancement BI pour activer la connexion unique.
7. Dans la zone *Synchronisation des références de connexion*, sélectionnez une option pour activer et mettre à jour les références de connexion à la source de données de l'utilisateur AD au moment de la connexion.

   Cette option synchronise la source de données avec les références de connexion actuelles de l'utilisateur.
8. Dans la zone *Options de SiteMinder*, configurez SiteMinder comme option de connexion unique pour l'authentification AD avec Kerberos :
   a. Cliquez sur *Désactivé.*

      La page *Windows Active Directory* apparaît.

      Si vous n'avez pas configuré le plug-in Windows AD, un avertissement apparaît et demande si vous souhaitez continuer. Cliquez sur *OK*.
   b. Cliquez sur *Utiliser la connexion unique SiteMinder*.
   c. Dans la zone *Hôte serveur de règles*, saisissez le nom de chaque serveur de règles, puis cliquez sur *Ajouter*.
   d. Pour chaque hôte serveur de règles, saisissez un numéro de port dans les zones *Comptabilisation*, *Authentification* et *Autorisation*.
   e. Dans la zone *Nom de l'agent*, saisissez le nom d'agent.
   f. Dans les zones *Secret partagé*, saisissez le secret partagé.

      Vérifiez que l'administrateur SiteMinder a activé la prise en charge des agents 4.x, quelle que soit la version de SiteMinder que vous utilisez. Pour en savoir plus sur SiteMinder et sur son installation, voir sa documentation.
   g. Cliquez sur *Mettre à jour* pour enregistrer et revenir à la page principale d'authentification AD.
9. Dans la zone *Options d'alias AD*, indiquez comment les nouveaux alias sont ajoutés et mis à jour sur la plateforme de BI.
   a. Dans la zone *Options de nouvel alias*, sélectionnez le mode de mappage des nouveaux alias aux comptes Enterprise :
      - *Affecter chaque nouvel alias AD à un compte utilisateur existant portant le même nom*

Sélectionnez cette option si des utilisateurs possèdent un compte Enterprise portant le même nom ; en d'autres termes, les alias AD seront affectés aux utilisateurs existants (la création automatique d'alias est activée). Les utilisateurs dépourvus de compte Enterprise, ou ne portant pas le même nom dans leurs comptes Enterprise et AD, sont ajoutés en tant que nouveaux utilisateurs.

- *Créer un nouveau compte utilisateur pour chaque nouvel alias AD*
  Sélectionnez cette option pour créer un nouveau compte pour chaque utilisateur.

b. Dans *Options de mise à jour des alias*, sélectionnez le mode de gestion des mises à jour d'alias pour les comptes Enterprise :

- *Créer de nouveaux alias lors de la mise à jour des alias*
  Sélectionnez cette option pour créer automatiquement un alias pour chaque utilisateur AD mappé à la plateforme de BI. De nouveaux comptes AD sont ajoutés pour les utilisateurs dépourvus de compte pour la plateforme de BI ou pour tous les utilisateurs si vous avez sélectionné l'option *Créer un nouveau compte utilisateur pour chaque nouvel alias AD* et cliqué sur *Mettre à jour*.
- *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
  Sélectionnez cette option si l'annuaire AD que vous mappez contient de nombreux utilisateurs dont seulement quelques-uns utiliseront la plateforme de BI. La plateforme ne crée pas automatiquement d'alias et de comptes Enterprise pour tous les utilisateurs. Il crée plutôt des alias (et des comptes, le cas échéant) uniquement pour les utilisateurs qui se connectent à la plateforme de BI.

c. Dans la zone *Options de nouvel utilisateur*, sélectionnez le mode de création des utilisateurs :

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
  Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers et permettent d'accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

  > **Remarque**
  >
  > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
  >
  > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

- *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
  Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateur simultané. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs au système, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

10. Pour configurer le mode de planification des mises à jour d'alias AD, cliquez sur *Planifier*.
    a. Dans la boîte de dialogue *Planifier*, sélectionnez une récurrence dans la liste *Exécuter l'objet*.
    b. Définissez les autres options et paramètres de planification selon vos besoins.

c. Cliquez sur *Planifier*.
   Lorsque la mise à jour des alias se produit, les informations sur le groupe sont également mises à jour.

11. Dans la zone *Options de liaison d'attributs*, spécifiez la priorité de liaison d'attributs pour le plug-in AD :
    a. Cochez la case *Importer le nom complet, l'adresse électronique et d'autres attributs*.
       Les noms complets et les descriptions utilisés dans les comptes AD sont importés et stockés avec les objets utilisateur sur la plateforme de BI.
    b. Spécifiez une option pour *Rendre la liaison d'attributs AD prioritaire par rapport aux autres liaisons d'attributs*.

       Si l'option est définie sur 1, les attributs AD sont prioritaires lorsqu'AD et les autres plug-ins (LDAP et SAP) sont activés. Si l'option est définie sur 3, les attributs des autres plug-ins sont prioritaires. Les liaisons doivent être définies sur des valeurs différentes. La définition de plusieurs plug-ins d'authentification sur la même valeur de liaison conduit à des résultats inattendus.
12. Dans la zone *Options du groupe AD*, configurez les mises à jour du groupe AD :
    a. Cliquez sur *Planifier*.
       La boîte de dialogue *Planifier* s'affiche.
    b. Sélectionnez une récurrence dans la liste *Exécuter l'objet*.
    c. Définissez les autres options et paramètres de planification selon vos besoins.
    d. Cliquez sur *Planifier*.

    Le système planifie la mise à jour et l'exécute conformément à la planification que vous avez définie. La prochaine mise à jour planifiée pour les comptes du groupe AD est affichée sous *Options du groupe AD*.
13. Dans la zone *Mise à jour d'AD à la demande*, sélectionnez une option pour indiquer si les groupes ou utilisateurs AD doivent être mis à jour lorsque vous cliquez sur *Mettre à jour* :
    - *Mettre à jour les groupes AD maintenant*
      Sélectionnez cette option pour démarrer la mise à jour de tous les groupes AD planifiés lorsque vous cliquez sur *Mettre à jour*. La prochaine mise à jour planifiée du groupe AD est répertoriée sous *Options du diagramme de groupe AD*.
    - *Mettre à jour les alias et les groupes AD maintenant*
      Sélectionnez cette option pour démarrer la mise à jour de tous les alias utilisateur et groupes AD planifiés lorsque vous cliquez sur *Mettre à jour*. Les prochaines mises à jour planifiées sont répertoriées sous *Options du groupe AD* et *Options d'alias AD*.
    - *Ne pas mettre à jour les alias et les groupes AD maintenant*
      Aucun alias utilisateur ou groupe AD ne sera mis à jour lorsque vous cliquerez sur *Mettre à jour*.
14. Cliquez sur *Mettre à jour*, puis sur *OK*.

9.4.6.3.1.3 Pour désactiver SiteMinder

Si vous souhaitez empêcher la configuration de SiteMinder ou le désactiver après sa configuration dans la CMC, modifiez le fichier de configuration Web pour la zone de lancement BI.

9.4.6.3.1.3.1 Désactivation de SiteMinder pour les clients Java

Les paramètres de SiteMinder doivent être désactivés pour le plug-in de sécurité Windows AD, mais aussi pour le fichier war BOE sur le serveur d'applications Web.

1. Accédez au répertoire suivant de votre installation de la plateforme de BI :

   `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Ouvrez le fichier `global.properties`.
3. Passez `siteminder.enabled` à false

   ```
   siteminder.enabled=false
   ```
4. Enregistrez les modifications et fermez le fichier.

La modification ne prend effet qu'après redéploiement de `BOE.war` sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

9.4.7 Dépannage de l'authentification Windows AD

9.4.7.1 Dépannage de votre configuration

Ces deux procédures peuvent vous aider si vous rencontrez des difficultés lors de la configuration de Kerberos :

- Activation de la journalisation
- Test de la configuration Kerberos du SDK Java

9.4.7.1.1 Pour activer la journalisation

1. Dans le menu *Démarrer*, sélectionnez *Programmes >Tomcat > Configuration Tomcat*.
2. Cliquez sur l'onglet *Java*.
3. Ajoutez les options suivantes :

   ```
   -Dcrystal.enterprise.trace.configuration=verbose
   -sun.security.krb5.debug=true
   ```

   Vous créez ainsi un fichier journal à l'emplacement suivant :

   ```
   C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
   ```

9.4.7.1.2 Pour tester la configuration Kerberos

Exécutez la commande suivante pour tester la configuration Kerberos, `servant` correspondant au compte de service et au domaine sous lesquels s'exécute le CMS et `Password` au mot de passe associé au compte de service.

```
<RépInstall>\SAP BusinessObjects Enterprise XI
4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

Par exemple :

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

Votre domaine et votre nom de service principal doivent correspondre exactement à ceux d'Active Directory. Si le problème persiste, contrôlez si vous avez saisi le même nom. Pensez que le nom est sensible à la casse.

9.4.7.1.3 Echec de la connexion dû à des noms UPN et SAM différents dans AD

L'ID Active Directory d'un utilisateur a été correctement mappé à la plateforme de BI. Malgré cela, l'utilisateur ne peut pas se connecter à la CMC ou à la zone de lancement BI avec l'authentification Windows AD et Kerberos au format suivant : `DOMAIN\ABC123`

Ce problème peut se produire lorsque l'utilisateur est configuré dans Active Directory avec un nom UPN et un nom SAM qui ne sont pas exactement identiques. Les exemples suivants peuvent causer un problème :

- Le nom UPN est abc123@company.com mais le nom SAM est DOMAIN\ABC123.
- Le nom UPN est jsmith@company mais le nom SAM est DOMAIN\johnsmith.

Il y a deux façons de traiter ce problème :

- Demandez aux utilisateurs de se connecter à l'aide de leurs noms UPN plutôt que de leurs noms SAM.
- Vérifiez que le nom de compte SAM et le nom UPN sont identiques.

9.4.7.1.4 Erreur de pré-authentification

Un utilisateur qui a pu se connecter au préalable ne parvient plus à le faire. Il obtient le message d'erreur suivant : Informations de compte non reconnues. Les journaux d'erreur Tomcat font état de l'erreur suivante : `"Pre-authentication information was invalid (24)"` (Informations de pré-authentification non valides).

Ceci peut se produire lorsque la base de données d'utilisateurs Kerberos n'a pas été mise à jour après un changement d'UPN dans AD. Ceci peut également indiquer que la base de données d'utilisateurs Kerberos et les informations AD ne sont pas synchronisées.

Pour résoudre ce problème, réinitialisez le mot de passe de l'utilisateur dans AD. Ainsi, les modifications seront correctement diffusées.

> **Remarque**
>
> Ce problème n'en est pas un dans J2SE 5.0.

9.5 Authentification SAP

9.5.1 Configuration de l'authentification SAP

Cette section explique comment configurer l'authentification de la plateforme de BI pour votre environnement SAP.

L'authentification SAP permet aux utilisateurs SAP de se connecter à la plateforme de BI à l'aide de leurs noms d'utilisateur et mots de passe SAP, sans stocker les mots de passe sur la plateforme de BI. Elle permet également de conserver les informations relatives aux rôles utilisateur dans SAP, et d'utiliser ces informations sur la plateforme pour affecter des droits permettant d'effectuer des tâches administratives ou d'accéder au contenu.

Accès à l'application d'authentification SAP

Vous devez fournir à la plateforme de BI des informations sur votre système SAP. Vous pouvez accéder à une application Web dédiée via l'outil d'administration principal de la plateforme de BI, la Central Management Console (CMC). Pour y accéder depuis la page d'accueil de la CMC, cliquez sur *Authentification*.

Authentification des utilisateurs SAP

Les plug-ins de sécurité développent et personnalisent la manière dont la plateforme de BI authentifie les utilisateurs. La fonction Authentification SAP inclut un plug-in de sécurité SAP (`secSAPR3.dll`) pour le composant CMS (Central Management Server) de la plateforme de BI. Ce plug-in de sécurité SAP offre plusieurs avantages clés :

- Il agit comme un fournisseur d'authentification qui compare les références de connexion de l'utilisateur à celles du système SAP pour le compte du CMS. Lorsque les utilisateurs se connectent directement à la plateforme de BI, ils peuvent choisir l'authentification SAP et fournir leurs nom d'utilisateur et mot de passe SAP habituels. La plateforme de BI peut également valider les tickets de connexion du portail Enterprise dans les systèmes SAP.
- Cela facilite la création de compte en permettant de mapper les rôles de SAP aux groupes d'utilisateurs de la plateforme de BI, ainsi que la gestion des comptes en permettant d'affecter des droits aux utilisateurs et aux groupes de manière cohérente au sein de la plateforme de BI.
- Il tient à jour les listes de rôles SAP de façon dynamique. Ainsi, lorsque vous mappez un rôle SAP sur la plateforme, tous les utilisateurs appartenant à ce rôle peuvent se connecter au système. Si, par la suite, vous modifiez l'appartenance au rôle SAP, vous n'avez pas besoin de mettre à jour ou d'actualiser la liste sur la plateforme de BI.

- Le composant d'authentification SAP comprend une application Web pour la configuration du plug-in. Vous pouvez accéder à cette application dans la zone *Authentification* de la CMC (Central Management Console).

9.5.2 Création d'un compte utilisateur pour la plateforme de BI

Le système de la plateforme de BI requiert un compte utilisateur SAP autorisé à accéder aux listes d'appartenance aux rôles SAP et à authentifier les utilisateurs SAP. Vous avez besoin des références de connexion pour connecter la plateforme de BI à votre système SAP. Pour en savoir plus sur la manière de créer des comptes utilisateur SAP et d'affecter des autorisations par le biais des rôles, consultez votre documentation SAP BW.

Utilisez la transaction `SU01` pour créer un nouveau compte d'utilisateur SAP appelé `CRYSTAL`. Utilisez la transaction `PFCG` pour créer un nouveau rôle appelé `CRYSTAL_ENTITLEMENT`. Notez que ces noms sont recommandés mais pas obligatoires. Modifiez l'autorisation du nouveau rôle en définissant les valeurs des objets d'autorisation suivants :

Objet d'autorisation	Champ	Valeur
Autorisation d'accès aux fichiers (S_DATASET)	Activité (ACTVT)	Lecture, écriture (33, 34)
	Nom de fichier physique (FILENAME)	* (signifie TOUS)
	Nom de programme ABAP (PROGRAM)	*
Contrôle des autorisations pour accès RFC (S_RFC)	Activité (ACTVT)	16
	Nom de RFC à protéger (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type d'objet RFC à protéger (RFC_TYPE)	Groupe de fonctions (FUGR)
Maintenance principale des utilisateurs : Groupes d'utilisateurs (S_USER_GRP)	Activité (ACTVT)	Créer ou générer, et afficher (03)
	Groupe d'utilisateurs dans maintenance du fichier utilisateur (CLASS)	* **Remarque** Pour plus de sécurité, vous pouvez répertorier explicitement les groupes d'utilisateurs dont les membres doivent accéder à la plateforme de BI.

Enfin, ajoutez l'utilisateur `CRYSTAL` au rôle `CRYSTAL_ENTITLEMENT`.

→ Conseil

Si les règles de votre système exigent que les utilisateurs modifient leur mot de passe à la première ouverture de session, ouvrez une session avec le compte utilisateur CRYSTAL et redéfinissez le mot de passe.

ⓘ Remarque

Des autorisations supplémentaires pour l'objet S_RFC peuvent être nécessaires lorsque certaines extensions de performance ont été activées dans l'environnement ABAP. Ces erreurs seront signalées dans la page Importation de rôle, avec la fonction pour laquelle l'autorisation a échoué :

Exemple : Aucune autorisation RFC pour le module fonction RFC_METADATA_GET.

Objet d'autorisation	Champ	Valeur
Contrôle des autorisations pour accès RFC (S_RFC)	Activité (ACTVT)	16
	Nom de RFC à protéger (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY et RFC_METADATA
	Type d'objet RFC à protéger (RFC_TYPE)	Groupe de fonctions (FUGR)

9.5.3 Connexion aux systèmes d'autorisation de SAP

Avant d'importer des rôles ou de publier du contenu BW dans la plateforme de BI, vous devez fournir des informations sur les systèmes d'autorisation SAP auxquels vous souhaitez vous intégrer. La plateforme de BI utilise ces informations pour se connecter au système SAP cible lors de la définition de l'appartenance aux rôles et de l'authentification des utilisateurs SAP.

9.5.3.1 Ajout d'un système d'autorisation SAP

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*.

   Les paramètres des systèmes d'autorisation s'affichent.

   → Conseil

   Si un système d'autorisation est déjà affiché dans la liste *Nom du système logique*, cliquez sur *Nouveau*.

3. Dans le champ *Système*, saisissez les trois caractères de l'identifiant de votre système SAP (SID).

4. Dans le champ *Client*, saisissez le numéro de client que la plateforme de BI doit utiliser lorsqu'elle se connecte à votre système SAP.
   La plateforme de BI associe vos informations Système et Client, puis ajoute une entrée à la liste *Nom du système logique*.
5. Vérifiez que la case *Désactivé* est décochée.

   > ⓘ Remarque
   >
   > La case à cocher *Désactivé* permet d'indiquer à la plateforme de BI qu'un système SAP particulier est momentanément indisponible.

6. Le cas échéant, remplissez les champs *Serveur de messagerie* et *Groupe de connexion* si vous avez configuré l'équilibrage de charge pour que la plateforme de BI se connecte via un serveur de messagerie.

   > ⓘ Remarque
   >
   > Vous devez définir les entrées appropriées dans le fichier `Services` de l'ordinateur de votre plateforme de BI pour activer l'équilibrage de charge, en particulier si le déploiement est effectué sur plusieurs ordinateurs. Prenez en compte les ordinateurs qui hébergent le CMS, le serveur d'applications Web et tous les ordinateurs qui gèrent vos comptes et paramètres d'authentification.

7. Si vous n'avez pas configuré l'équilibrage de charge (ou si vous préférez que la plateforme de BI se connecte directement au système SAP), renseignez les champs *Serveur d'applications* et *Numéro du système* selon les besoins.
8. Dans les champs prévus à cet effet, saisissez le *Nom d'utilisateur*, le *Mot de passe* et la *Langue* du compte SAP que doit utiliser la plateforme de BI pour se connecter à SAP.

   > ⓘ Remarque
   >
   > Ces références de connexion doivent correspondre au compte utilisateur que vous avez créé pour la plateforme de BI.

9. Cliquez sur *Mettre à jour*.

Si vous ajoutez plusieurs systèmes d'autorisation, cliquez sur l'onglet *Options* pour spécifier le système que la plateforme de BI utilise par défaut (c'est-à-dire le système contacté pour authentifier les utilisateurs qui tentent de se connecter avec des références de connexion SAP mais sans spécifier un système SAP particulier).

9.5.3.2 Pour vérifier qu'un système d'autorisation a été correctement ajouté

1. Cliquez sur l'onglet *Importation de rôle*.
2. Sélectionnez le système d'autorisation approprié dans la liste *Nom de système logique*.

   Si celui-ci a été correctement ajouté, la liste *Rôles disponibles* contient la liste des rôles que vous pouvez importer.

   > → Conseil
   >
   > Si la liste .*Rôles disponibles* ne contient aucun rôle, recherchez les éventuels messages d'erreur sur la page Vous y trouverez peut-être les informations nécessaires pour résoudre le problème.

9.5.3.3 Pour désactiver temporairement une connexion à un système d'autorisation SAP

Dans la CMC, vous pouvez désactiver temporairement une connexion entre la plateforme de BI et un système d'autorisation SAP. Cette opération peut s'avérer utile pour maintenir la réactivité de la plateforme de BI, par exemple lors du temps d'arrêt planifié d'un système d'autorisation SAP.

1. Dans la CMC, accédez à la zone de gestion *Authentification*.
2. Cliquez deux fois sur le lien *SAP*.
3. Dans la liste *Nom de système logique*, sélectionnez le système à désactiver.
4. Cochez la case *Désactivé*.
5. Cliquez sur *Mettre à jour*.

9.5.4 Définition des options d'authentification SAP

L'authentification SAP comprend un certain nombre d'options que vous pouvez spécifier lors de l'intégration de la plateforme de BI à votre système SAP. Les options incluent :

- Activation ou désactivation de l'authentification SAP
- Spécification des paramètres de connexion
- Mise en relation des utilisateurs importés aux modèles de licence de la plateforme de BI.
- Configuration de la connexion unique dans le système SAP

9.5.4.1 Pour définir les options d'authentification SAP

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*, puis cliquez sur l'onglet *Options*.
3. Examinez et modifiez les paramètres suivants en fonction de vos besoins :

Paramètre	Description
Activer l'authentification SAP	Décochez cette case pour désactiver l'authentification SAP. **Remarque** Pour désactiver l'authentification SAP d'un système SAP spécifique, cochez la case *Désactivé* du système en question dans l'onglet *Système d'autorisation*.
Racine du dossier Contenu	Spécifiez l'emplacement où la plateforme de BI doit commencer à dupliquer la structure des dossiers BW dans la CMC et dans la zone de lancement BI.

Paramètre	Description
	Par défaut, il s'agit du dossier `/SAP/2.0`, mais vous pouvez indiquer un autre dossier. Si vous le souhaitez, vous pouvez modifier la valeur dans la CMC et dans le Workbench d'administration de contenu.
Système par défaut	Sélectionnez un système d'autorisation SAP pour la plateforme de BI à contacter pour authentifier les utilisateurs qui essayent de se connecter avec des références de connexion SAP mais sans indiquer de système SAP. **Remarque** Si vous sélectionnez un système par défaut, les utilisateurs de ce système n'ont pas à saisir leur ID système ou client lorsqu'ils se connectent à partir d'outils client tels que Live Office ou Universe Designer à l'aide de l'authentification SAP. Par exemple, si SYS~100 est défini comme système par défaut, SYS~100/utilisateur1 peut se connecter comme utilisateur1 lorsque l'authentification SAP est sélectionnée.
Nombre maximal d'échecs d'accès au système d'autorisation	Saisissez le nombre de fois que la plateforme de BI doit essayer de contacter un système SAP pour satisfaire les demandes d'authentification. Lorsque vous définissez la valeur sur -1, la plateforme peut tenter de contacter indéfiniment le système d'autorisation. Lorsque vous définissez la valeur sur 0, la plateforme de BI n'a droit qu'à une seule tentative d'accès au système d'autorisation. **Remarque** Utilisez ce paramètre avec l'option *Laisser le système d'autorisation désactivé [secondes]* pour configurer la façon dont la plateforme de BI doit gérer les systèmes d'autorisation SAP qui sont momentanément indisponibles. Le système utilise les deux options pour déterminer à quel moment les communications avec les systèmes SAP indisponibles doivent être interrompues puis reprises.
Laisser le système d'autorisation désactivé [secondes]	Saisissez le nombre de secondes pendant lesquelles la plateforme de BI doit attendre avant de reprendre les tentatives d'authentification des utilisateurs dans le système SAP. Par exemple, si vous saisissez la valeur 3 pour *Nombre maximal d'échecs d'accès au système d'autorisation*, la plateforme de BI ne permet que trois tentatives

Paramètre	Description
	(non abouties) pour authentifier les utilisateurs sur un système SAP spécifique. Après une quatrième tentative non aboutie, le système interrompt ses tentatives d'authentification des utilisateurs pour ce système durant le nombre de secondes indiqué.
Nombre maximal de connexions simultanées par système	Indiquez le nombre maximal de connexions qui peuvent être ouvertes simultanément sur votre système SAP. Par exemple, si vous saisissez 2, la plateforme de BI garde deux connexions ouvertes sur SAP.
Nombre d'utilisations par connexion	Indiquez le nombre d'opérations que vous autorisez par connexion au système SAP. Par exemple, si l'option *Nombre maximal de connexions simultanées par système* est définie sur 2 et que l'option *Nombre d'utilisations par connexion* est définie sur 3, la plateforme de BI ferme et redémarre cette connexion lorsque trois sessions se trouvent sur une connexion.
Utilisateurs simultanés et *Utilisateurs nommés*	Indiquez si les comptes des nouveaux utilisateurs utilisent des licences Utilisateur nommé ou utilisateur simultané. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée car un petit nombre de licences peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs au système, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs. Les licences Utilisateur nommé sont associées à des utilisateurs qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. **Remarque** Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.

Paramètre	Description
	Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public. **Remarque** L'option que vous sélectionnez ici ne change ni le nombre, ni le type des licences utilisateur installées dans la plateforme de BI. Vous devez disposer des licences adéquates sur votre système.
Importer le nom complet, l'adresse électronique et d'autres attributs	Spécifiez un niveau de priorité pour le plug-in d'authentification SAP. Les noms complets et les descriptions des comptes SAP sont importés et stockés avec les objets utilisateur dans la plateforme de BI.
Rendre la liaison d'attributs SAP prioritaire par rapport aux autres liaisons d'attributs	Spécifie une priorité pour la liaison des attributs utilisateur SAP (nom complet et adresse électronique). Si l'option est définie sur 1, les attributs SAP sont prioritaires dans les scénarios où SAP et les autres plug-ins (Windows AD et LDAP) sont activés. Si l'option est définie sur 3, les attributs des autres plug-ins sont prioritaires. Les liaisons doivent être définies sur des valeurs différentes. La définition de plusieurs plug-ins d'authentification sur la même valeur de liaison conduit à des résultats inattendus.

Définissez les options suivantes pour configurer le service de connexion unique SAP :

Paramètre	Description
ID système	Identificateur système fourni par la plateforme de BI au système SAP lors de l'exécution du service de connexion unique SAP.
Parcourir	Cliquez pour télécharger le fichier de `stockage des clés` généré pour permettre la connexion unique SAP. Vous pouvez aussi saisir manuellement le chemin complet du fichier.
Mot de passe du stockage de clés	Fournissez le mot de passe requis pour accéder au fichier de `stockage de clés`.
Mot de passe de la clé privée	Fournissez le mot de passe requis pour accéder au certificat correspondant au fichier de `stockage de clés`. Le certificat est stocké sur le système SAP
Alias de clé privée	Fournissez l'alias requis pour accéder au fichier de `stockage de clés`.

4. Cliquez sur *Mettre à jour*.

9.5.4.2 Pour modifier la racine du dossier Contenu

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*.
3. Cliquez sur *Options* et saisissez le nom du dossier dans le champ *Racine du dossier Contenu*.

   Le nom du dossier que vous saisissez ici correspond au dossier à partir duquel la plateforme de BI doit commencer à dupliquer la structure des dossiers BW.
4. Cliquez sur *Mettre à jour*.
5. Dans le Workbench d'administration de contenu BW, développez *Système Enterprise*.
6. Développez *Systèmes disponibles*, puis cliquez deux fois sur le système auquel la plateforme de BI se connecte.
7. Cliquez sur l'onglet *Disposition*, puis dans *Dossier de base de contenu*, saisissez le dossier que vous voulez utiliser comme dossier SAP racine dans la plateforme de BI (par exemple, `/SAP/2.0/`) .

9.5.5 Importation de rôles SAP

En important des rôles SAP dans la plateforme de BI, vous permettez aux membres correspondants de se connecter au système avec leurs références de connexion SAP habituelles. De plus, la connexion unique est activée, de sorte que les utilisateurs SAP puissent être automatiquement connectés à la plateforme de BI lorsqu'ils accèdent aux rapports à partir de l'interface utilisateur SAP ou d'un portail SAP Enterprise Portal.

> **Remarque**
>
> L'activation de la connexion unique repose bien souvent sur de nombreux préalables. Certains peuvent concerner l'utilisation d'un pilote et d'une application compatibles avec cette fonction, ainsi que la certitude que votre serveur et le serveur Web font partie du même domaine.

Pour chaque rôle importé, la plateforme de BI génère un groupe. Chaque groupe est nommé en respectant la convention suivante : **`<IDSystème~NuméroClient@NomDuRôle>`**. Vous pouvez afficher les nouveaux groupes dans la zone de gestion *Utilisateurs et groupes* de la CMC. Vous pouvez également utiliser ces groupes pour définir la sécurité des objets dans la plateforme de BI.

Tenez compte de trois catégories principales d'utilisateurs lors de la configuration de la plateforme de BI pour une publication et lors de l'importation de rôles vers le système :

- Administrateurs de la plateforme de BI
  Les administrateurs Enterprise configurent le système pour publier du contenu à partir de SAP. Ils importent les rôles appropriés, créent les dossiers nécessaires et affectent des droits à ces rôles et dossiers dans la plateforme de BI.
- Editeurs de contenu
  Les éditeurs de contenu sont les utilisateurs autorisés à publier le contenu dans les rôles. L'objectif de cette catégorie d'utilisateurs est de séparer les membres des rôles standard de ces utilisateurs autorisés à publier des rapports.
- Membres de rôle
  Les membres de rôle sont des utilisateurs appartenant aux rôles « portant le contenu ». En d'autres termes, ces utilisateurs appartiennent aux rôles vers lesquels les rapports sont publiés. Ils disposent des droits de *visualisation*, de *visualisation à la demande* et de *planification* pour les rapports publiés vers les

rôles dont ils sont membres. Toutefois, les membres de rôle standard ne peuvent ni publier de nouveaux contenus, ni publier des versions de contenu mises à jour.

Vous devez importer tous les rôles de publication de contenu ou ayant trait au contenu dans la plateforme de BI avant d'effectuer la première publication.

> **Remarque**
>
> Nous vous recommandons fortement de distinguer les activités des rôles. Par exemple, alors qu'il est possible de réaliser une publication à partir du rôle d'un administrateur, il est préférable de publier uniquement à partir de rôles d'éditeurs de contenu. En outre, la fonction des rôles de publication de contenu consiste uniquement à définir les utilisateurs pouvant publier du contenu. Ainsi, les rôles de publication de contenu ne doivent pas contenir de contenu ; les éditeurs de contenu doivent publier vers des rôles portant le contenu qui sont accessibles aux membres de rôle standard.

9.5.5.1 Pour importer des rôles SAP

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*.
3. Dans l'onglet *Options*, sélectionnez *Utilisateurs simultanés* ou *Utilisateurs nommés* selon votre contrat de licence.

   Cette option ne change ni le nombre, ni le type des licences utilisateur que vous avez installées dans la plateforme de BI. Vous devez disposer des licences adéquates sur votre système.
4. Cliquez sur *Mettre à jour*.
5. Dans l'onglet *Importation de rôle*, sélectionnez le système d'autorisation approprié dans la liste *Nom de système logique*.
6. Dans la zone *Rôles disponibles*, sélectionnez le ou les rôles que vous souhaitez importer, puis cliquez sur *Ajouter*.
7. Cliquez sur *Mettre à jour*.

9.5.5.2 Pour vérifier que les rôles et les utilisateurs ont été importés correctement

Avant de commencer cette procédure, notez le nom d'utilisateur et le mot de passe d'un utilisateur SAP qui appartient à l'un des rôles que vous avez mappés à la plateforme de BI.

1. Pour la zone de lancement BI Java, accédez à **`http://<serveurWeb>:<numéroport>/BOE/BI`**.

   Remplacez `<serveurWeb>` par le nom du serveur Web et `<numérodeport>` par le numéro de port de la plateforme de BI. Il vous faudra peut-être demander à votre administrateur le nom du serveur Web, le numéro de port ou l'URL exacte à saisir.
2. Dans la liste *Type d'authentification*, sélectionnez *SAP*.

> **Remarque**
>
> Par défaut, la liste *Type d'authentification* est masquée dans la zone de lancement BI. Si la liste n'est pas visible, demandez à votre administrateur système d'activer la liste *Type d'authentification* dans le fichier `BIlaunchpad.properties` puis redémarrez le serveur de l'application.

3. Saisissez le système SAP et le client système auxquels vous souhaitez vous connecter.
4. Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur mappé.
5. Cliquez sur *Connexion*.

   Vous êtes connecté à la Zone de lancement BI en tant qu'utilisateur sélectionné.

9.5.5.3 Mise à jour des rôles et des utilisateurs SAP

Une fois l'authentification SAP activée, il est nécessaire de planifier et d'exécuter des mises à jour régulières sur les rôles mappés qui ont été importés dans la plateforme de BI. Cela garantira que les informations des rôles SAP sont reflétées avec précision dans la plateforme de BI.

Il existe deux options pour l'exécution et la planification des mises à jour de rôles SAP :

- Mettre à jour les rôles uniquement : cette option permet uniquement de mettre à jour les liens entre les rôles actuellement mappés qui ont été importés dans la plateforme de BI. Nous vous recommandons d'utiliser cette option si vous avez l'intention d'exécuter des mises à jour fréquentes et que vous êtes préoccupé par l'utilisation des ressources système. Aucun nouveau compte utilisateur ne sera créé si vous effectuez uniquement une mise à jour des rôles SAP.
- Mettre à jour les rôles et les alias : cette option permet non seulement de mettre à jour les liens entre les rôles, mais aussi de créer des comptes utilisateur dans la plateforme de BI pour les alias utilisateur ajoutés à des rôles dans le système SAP.

> **Remarque**
>
> Si vous n'avez pas spécifié de créer automatiquement des alias utilisateur pour les mises à jour lors de l'activation de l'authentification SAP, aucun compte ne sera créé pour les nouveaux alias.

9.5.5.3.1 Planification de mises à jour pour les rôles SAP

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer la manière dont le système doit mettre à jour les rôles.

1. Cliquez sur l'onglet *Mise à jour de l'utilisateur*.
2. Cliquez sur *Planifier* dans la section *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

   > **→ Conseil**
   >
   > Pour effectuer une mise à jour immédiate, cliquez sur *Mettre à jour maintenant*.

> → Conseil
>
> Utilisez l'option *Mettre à jour les rôles uniquement* si vous souhaitez effectuer des mises à jour fréquentes et que vous êtes préoccupé par les ressources système. Le système met plus de temps à mettre à jour à la fois les rôles et les alias.

La boîte de dialogue *Périodicité* s'affiche.

3. Sélectionnez une option dans la liste déroulante *Exécuter l'objet* et indiquez toutes les informations de planification demandées dans les champs correspondants.

   Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous indiquez l'heure de début ainsi que les dates de début et de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les `<n>`jours(`<n>` étant le nombre de jours que vous indiquez). Vous pouvez indiquer l'heure de début ainsi que les dates de début et de fin.
Toutes les semaines	La mise à jour s'exécutera une fois par semaine ou plusieurs fois par semaine. Vous pouvez indiquer les jours d'exécution, l'heure de début et les dates de début et de fin.
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez indiquer l'heure de début ainsi que les dates de début et de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

4. Cliquez sur *Planifier*.
   La date de la prochaine mise à jour de rôles planifiée est affichée dans l'onglet *Mise à jour de l'utilisateur*.

> → Conseil
>
> Pour annuler la prochaine mise à jour, cliquez sur *Annuler les mises à jour planifiées* dans la zone *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

9.5.6 Configuration de la communication réseau sécurisée (SNC)

Cette section explique comment configurer la SNC dans le cadre du processus de configuration d'authentification SAP à la plateforme de BI

Pour en savoir plus, voir Note SAP 1396213.

Avant de configurer la sécurité entre les systèmes SAP et la plateforme de BI, assurez-vous que le SIA est configuré pour démarrer et s'exécuter sous un compte configuré pour la SNC. Vous devez également configurer votre système SAP pour valider la plateforme de BI.

Informations associées

Présentation de la sécurité côté serveur [page 354]

9.5.6.1 Présentation de la sécurité côté serveur

Cette section contient des procédures permettant de configurer la sécurité côté serveur entre les serveurs d'applications Web SAP (versions 6.20 et supérieures) et la plateforme SAP BusinessObjects Business Intelligence. Vous devez configurer la sécurité côté serveur si vous utilisez la méthode d'éclatement de rapports multipassage (pour les publications dans lesquelles la requête de rapport dépend du contexte de l'utilisateur).

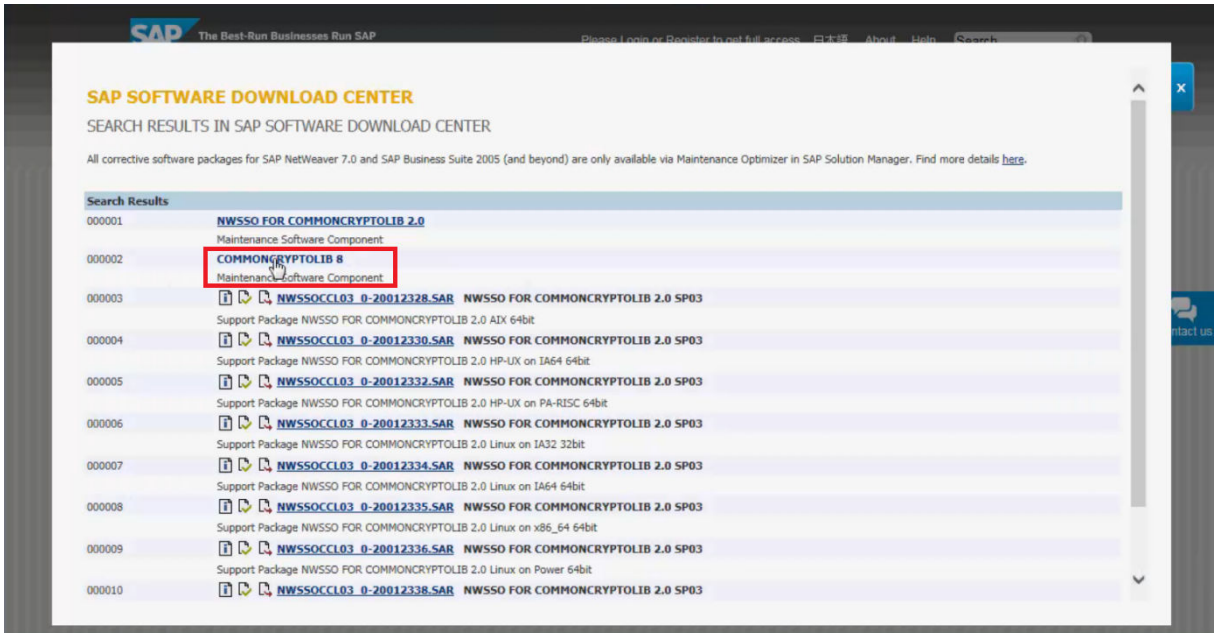
La sécurité côté serveur nécessite un emprunt d'identité sans mot de passe. Pour pouvoir emprunter l'identité d'un utilisateur SAP sans fournir de mot de passe, l'utilisateur doit être identifié auprès de SAP à l'aide d'une méthode plus sécurisée qu'un simple nom d'utilisateur et mot de passe. (Un utilisateur SAP ayant le profil d'autorisation SAP_ALL ne peut pas emprunter l'identité d'un autre utilisateur SAP sans connaître son mot de passe.)

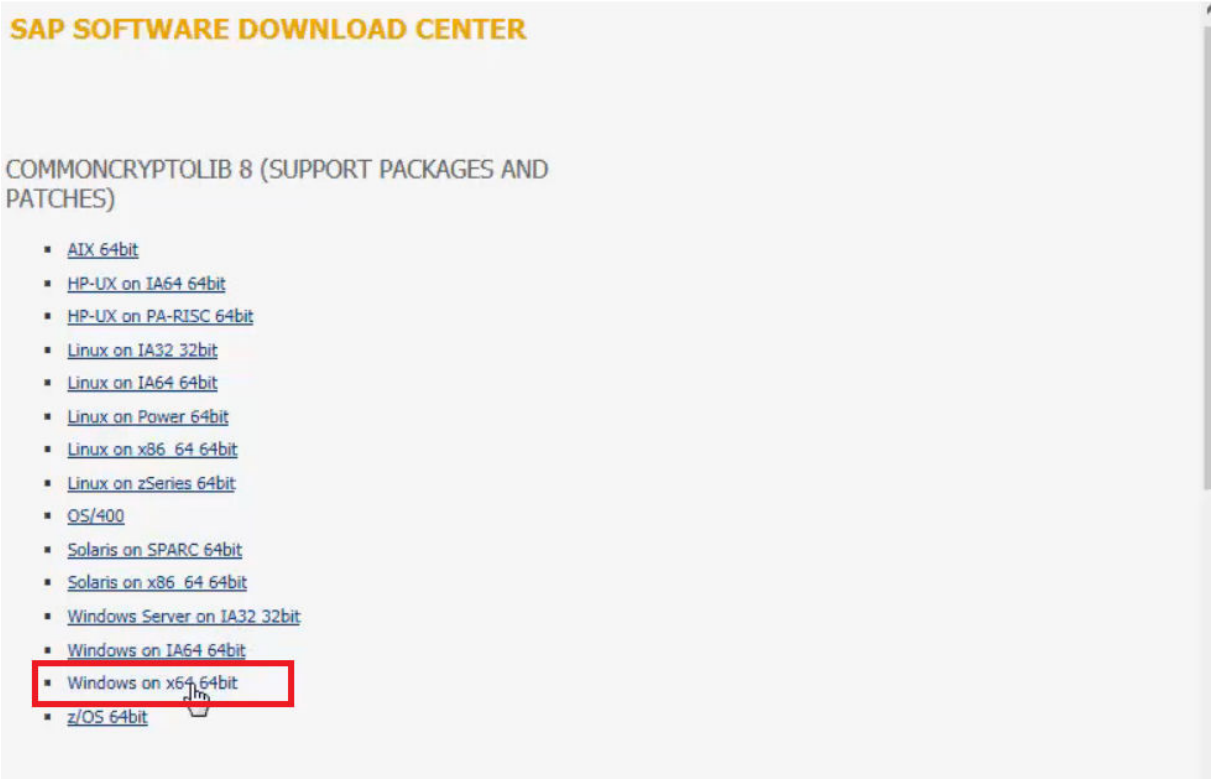
Activation de la sécurité côté serveur à l'aide de la bibliothèque cryptographique SAP

Pour activer la sécurité côté serveur pour la plateforme de BI à l'aide de la bibliothèque cryptographique SAP, vous devez exécuter les serveurs correspondants avec des références de connexion qui sont authentifiées à l'aide d'un fournisseur de communication réseau sécurisée (SNC) agréé. Ces références de connexion sont configurées dans SAP de façon à autoriser l'emprunt d'identité sans mot de passe. Pour la plateforme de BI, vous devez exécuter les serveurs impliqués dans l'éclatement de rapports, tels que l'Adaptive Job Server, avec ces références de connexion SNC.

Vous avez besoin de fichiers binaires SNC 32 bits pour les processus 32 bits et de fichiers binaires SNC 64 bits pour les processus 64 bits. Une bibliothèque cryptographique SAP est installée avec la plateforme de BI.

Notez que la bibliothèque cryptographique SAP peut uniquement être utilisée pour configurer la sécurité côté serveur. La bibliothèque cryptographique est disponible pour Windows et Unix.





Add to Download Basket | Maintain Download Basket | Select All | Deselect All

The following objects are available for download:

	File Type	Download Object	Title	Patch Level	Info File	File Size [kb]	Last Changed
☐	SAR	SAPCRYPTOLIBP_8433-20011729.SAR	SAPCRYPTOLIBP	8433	Info	6651	21.01.2015
☐	SAR	SAPCRYPTOLIBP_8434-20011729.SAR	SAPCRYPTOLIBP	8434	Info	6641	16.02.2015
☐	SAR	SAPCRYPTOLIBP_8435-20011729.SAR	SAPCRYPTOLIBP	8435	Info	6659	19.03.2015
☐	SAR	SAPCRYPTOLIBP_8436-20011729.SAR	SAPCRYPTOLIBP	8436	Info	6668	05.05.2015
☐	SAR	SAPCRYPTOLIBP_8437-20011729.SAR	SAPCRYPTOLIBP	8437	Info	6666	19.05.2015

Add to Download Basket | Maintain Download Basket | Select All | Deselect All

Pour plus d'informations sur la bibliothèque SAP Cryptographic Library, voir les notes SAP 711093, 597059 et 397175 sur le site Web de SAP.

Le serveur SAP et la plateforme de BI doivent se voir attribuer des certificats prouvant mutuellement leur identité. Chaque serveur a son propre certificat ainsi qu'une liste de certificats pour les parties approuvées. Pour configurer la sécurité côté serveur entre SAP et la plateforme de BI, vous devez créer un jeu de certificats protégé par mot de passe appelé environnement de sécurité personnelle (Personal Security Environment, PSE). Cette section explique comment configurer et gérer les PSE et comment les associer de façon sécurisée aux serveurs de traitement de la plateforme de BI.

Responsabilités des serveurs de la plateforme SAP BusinessObjects BI

Certains serveurs de la plateforme de BI servent à l'intégration SAP en matière de connexion unique. Le tableau suivant répertorie ces serveurs et leurs domaines de responsabilités.

Serveur	Domaines de responsabilités
Serveur d'applications Web	Liste de rôles de l'authentification SAP
Service BW Publisher	Personnalisation et listes de sélection des paramètres dynamiques de Crystal Reports
CMS	Listes de mots de passe, de tickets, de vérification des appartenances du rôle et d'utilisateurs
Page Server	Affichage à la demande de Crystal Reports
Job Server	Planification de Crystal Reports
Web Intelligence Processing Server	Affichage et planification des rapports Web Intelligence et des invites de liste de valeurs
Service MDAS (Multi-Dimensional Analysis Service)	Analyse

9.5.6.2 Configuration de SAP pour une sécurité côté serveur

La sécurité côté serveur s'applique uniquement aux rapports Crystal et Web Intelligence basés sur les univers (`.unv`). Vous devez configurer SNC pour l'utiliser avec la plateforme de BI. Pour en savoir plus ou pour obtenir de l'aide pour le dépannage, consultez la documentation SAP fournie avec votre serveur SAP.

9.5.6.2.1 Pour configurer SAP pour la sécurité côté serveur

1. Assurez-vous que vous disposez des références de connexion d'administrateur SAP pour SAP et l'ordinateur exécutant SAP, ainsi que les références de connexion d'administrateur pour la plateforme de BI et le ou les ordinateurs l'exécutant.
2. Sur l'ordinateur SAP, vérifiez que la bibliothèque cryptographique SAP et l'outil SAPGENPSE se trouvent dans le répertoire `<LECTEUR>:\usr\sap\<SID>\SYS\exe\run\` (sous Windows).
3. Créez une variable d'environnement appelée **`<SECUDIR>`** qui pointe vers le répertoire contenant le fichier ticket.

   > **Remarque**
   >
   > Cette variable doit être accessible à l'utilisateur dont les références de connexion sont utilisées pour exécuter le processus *disp+work* de SAP.

4. Dans l'interface utilisateur SAP, recherchez la transaction RZ10 et modifiez le profil d'instance en mode *maintenance étendue*.
5. En mode d'édition de profil, faites pointer les variables de profil SAP vers la bibliothèque cryptographique et donnez un nom distinctif (DN) au système SAP. Ces variables doivent suivre la convention d'attribution de noms LDAP :

Balise	Signification	Description
`CN`	Nom usuel	Nom usuel du propriétaire du certificat.
`OU`	Unité organisationnelle	EP pour Equipe produits, par exemple.
`O`	Organisation	Nom de l'organisation pour laquelle le certificat a été émis.
`C`	Pays	Pays dans lequel se situe l'organisation.

Par exemple, pour R21 : **`p:CN=R21, OU=EP, O=BOBJ, C=CA`**

> **Remarque**
>
> Le préfixe **`p:`** correspond à la bibliothèque cryptographique SAP. Il est requis lorsqu'il est fait référence au DN dans SAP, mais il n'est pas visible lors de l'examen des certificats dans STRUST ou lors de l'utilisation de SAPGENPSE.

6. Entrez les valeurs de profil suivantes, en utilisant les valeurs correspondant à votre système SAP.

Variable de profil	Valeur
`ssf/name`	`SAPSECULIB`
`ssf/ssfapi_lib`	Chemin complet de la bibliothèque cryptographique SAP
`sec/libsapsecu`	Chemin complet de la bibliothèque cryptographique SAP
`snc/gssapi_lib`	Chemin complet de la bibliothèque cryptographique SAP
`snc/identity/as`	DN de votre système SAP

7. Redémarrez l'instance SAP.
8. Lorsque le système est de nouveau exécuté, connectez-vous, puis recherchez la transaction STRUST, qui doit maintenant posséder des entrées supplémentaires pour SNC et SSL.
9. Cliquez avec le bouton droit de la souris sur le nœud SNC et cliquez sur *Créer*.
   L'identité que vous avez spécifiée dans RZ10 doit à présent s'afficher.
10. Cliquez sur *OK*.
11. Pour attribuer un mot de passe au PSE de la SNC, cliquez sur l'icône représentant un verrou.

> **Remarque**
>
> N'égarez pas ce mot de passe. STRUST vous demandera de l'indiquer chaque fois que vous affichez ou modifiez le PSE de la SNC.

12. Enregistrez les modifications.

> **Remarque**
>
> Si vous n'enregistrez pas les changements, le serveur d'applications ne redémarre pas lorsque vous activez la SNC.

13. Retournez à la transaction RZ10 et ajoutez les paramètres restants du profil SNC.

Variable de profil	Paramètre
`snc/accept_insecure_rfc`	`1`
`snc/accept_insecure_r3int_rfc`	`1`
`snc/accept_insecure_gui`	`1`
`snc/accept_insecure_cpic`	`1`
`snc/permit_insecure_start`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/max`	`3`
`snc/enable`	`1`

Le niveau de protection minimal est défini sur authentification seulement (1) et le niveau maximal est confidentiel (3). La valeur `snc/data_protection/use` définit que seule l'authentification doit être utilisée dans ce cas, mais elle peut être définie sur (2) pour le niveau intégrité, (3) pour confidentiel et (9) pour le maximum disponible. Les valeurs `snc/accept_insecure_rfc`,

`snc/accept_insecure_r3int_rfc`, `snc/accept_insecure_gui` et `snc/accept_insecure_cpic` définies sur (1) indiquent que les méthodes de communication précédentes (et potentiellement non sécurisées) sont toujours permises.

14. Redémarrez votre système SAP.

Configurez ensuite la plateforme de BI pour une sécurité côté serveur.

9.5.6.3 Configuration de la plateforme de BI pour une sécurité côté serveur

Pour configurer la plateforme de BI pour une sécurité côté serveur, suivez la procédure ci-après. Notez que ces étapes sont effectuées sous Windows ; cependant, étant donné que l'outil SAP est un outil de ligne de commande, ces étapes sont similaires sous Unix.

1. Configurez l'environnement
2. Générez un PSE (Personal Security Environment)
3. Configurez les serveurs de la plateforme de BI
4. Configurez l'accès au PSE
5. Configurez les paramètres SNC d'authentification SAP
6. Configurez les groupes de serveurs dédiés SAP

Informations associées

Pour configurer l'environnement [page 359]
Pour générer un PSE (environnement de sécurité personnelle) [page 360]
Pour configurer les serveurs de la plateforme de Business Intelligence [page 361]
Pour configurer l'accès au PSE [page 362]
Pour configurer les paramètres SNC d'authentification SAP [page 363]
Utilisation de groupes de serveurs [page 364]

9.5.6.3.1 Pour configurer l'environnement

La plateforme de BI comprend une bibliothèque cryptographique SAP par défaut. Si vous utilisez la bibliothèque par défaut, vous devez suivre uniquement les deux dernières étapes : créer un sous-dossier et ajouter une variable d'environnement. Sinon, pour configurer une copie personnalisée de la bibliothèque cryptographique SAP, suivez l'ensemble des étapes.

La bibliothèque cryptographique SAP par défaut se trouve à cet emplacement :

- Windows : `<REPINSTALL>\sap\sapcrypto.dll`
- Unix : `<REPINSTALL>/sap/libsapcrypto.so`

Avant de commencer, assurez-vous que :

- La bibliothèque cryptographique SAP a été développée sur l'hôte exécutant les serveurs de traitement de la plateforme de BI.
- Les systèmes SAP appropriés ont été configurés pour utiliser la bibliothèque cryptographique SAP comme fournisseur SNC.

Avant de pouvoir gérer le PSE, vous devez configurer la bibliothèque, l'outil et l'environnement dans lequel les PSE sont stockés.

1. Copiez la bibliothèque cryptographique SAP (y compris l'outil de gestion PSE) dans un dossier de l'ordinateur exécutant la plateforme de BI.

   Par exemple : `C:\Program Files\SAP\Crypto`.
2. Ajoutez le dossier à la variable d'environnement `<PATH>`.
3. Ajoutez une variable d'environnement système `<SNC_LIB>` pointant vers la bibliothèque cryptographique.

   Par exemple : `C:\Program Files\SAP\Crypto\sapcrypto.dll`

   > **Remarque**
   >
   > La longueur maximale du chemin est de 100 caractères.
4. Créez un sous-dossier appelé **`sec`**.

   Par exemple : `C:\Program Files\SAP\Crypto\sec`.
5. Ajoutez une variable d'environnement système `<SECUDIR>` pointant vers le dossier **`sec`**.

Informations associées

Configuration de SAP pour une sécurité côté serveur [page 357]

9.5.6.3.2 Pour générer un PSE (environnement de sécurité personnelle)

SAP accepte un serveur de la plateforme de BI comme entité sécurisée lorsque les serveurs de la plateforme de BI correspondants ont un PSE associé à SAP. Cette « sécurité » entre SAP et les composants de la plateforme de BI est établie par le partage de la version publique du certificat de chacun. La première étape consiste à générer un PSE pour la plateforme de BI qui génère automatiquement son propre certificat.

1. Ouvrez une invite de commande et exécutez **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`** depuis le dossier de la bibliothèque cryptographique.
2. Choisissez un code PIN et un DN (nom distinctif) pour votre système de la plateforme de BI.

   Par exemple, **`CN=MyBOE01, OU=EP, O=BOBJ, C=CA`**.

   Vous disposez maintenant d'un PSE par défaut ayant son propre certificat.
3. Utilisez la commande suivante pour exporter le certificat dans le PSE :

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```

4. Dans l'interface utilisateur de SAP, allez à la transaction STRUST et ouvrez le PSE système associé à votre système SAP.

   Vous pouvez alors être invité à saisir le mot de passe que vous avez déjà attribué à ce PSE système.
5. Importez le fichier `<MyBOECert.crt>` créé précédemment en cliquant sur le bouton « Importer le certificat » dans la partie inférieure gauche de l'écran de transaction STRUST.

   Les certificats de SAPGENPSE sont codés en Base64. N'oubliez pas de sélectionner Base64 lorsque vous les importez.
6. Pour ajouter le certificat de la plateforme de BI à la liste de certificats PSE du serveur SAP, cliquez sur le bouton *Ajouter à la liste de certificats*.
7. Enregistrez les changements dans STRUST.
8. Cliquez sur le bouton *Exporter* et donnez un nom au certificat.

   Par exemple, **`MonCertSAP.crt`**.

   > ⓘ Remarque
   >
   > Le format doit rester Base64.
9. Allez à la transaction SNCO.
10. Ajoutez une nouvelle entrée, où :
    - L'ID du système est arbitraire mais reflète votre système de la plateforme de BI.
    - Le nom SNC doit correspondre au DN (précédé de **`p:`**) que vous avez saisi lorsque vous avez créé le PSE de la plateforme de BI (à l'étape 2).
    - Les cases à cocher *Entrée pour RFC activée* et *Entrée pour ID externe activée* sont sélectionnées :
11. Pour ajouter le certificat exporté au PSE de la plateforme de BI, exécutez la commande suivante dans l'invite de commande :

    ```
    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
    ```

La bibliothèque cryptographique SAP est installée sur l'ordinateur de la plateforme de BI. Vous avez créé un PSE qui sera utilisé par les serveurs de la plateforme de BI pour s'identifier auprès des serveurs SAP. SAP et le PSE de la plateforme de BI ont échangé leurs certificats. SAP autorise les entités ayant accès au PSE de la plateforme de BI à effectuer des appels RFC et un emprunt d'identité sans mot de passe.

Informations associées

Pour configurer les serveurs de la plateforme de Business Intelligence [page 361]

9.5.6.3.3 Pour configurer les serveurs de la plateforme de Business Intelligence

Après avoir généré un PSE pour la plateforme de BI, vous devez configurer une structure de serveurs appropriée pour le traitement SAP. La procédure suivante crée un nœud pour les serveurs de traitement SAP, de façon à ce que vous puissiez définir les références de connexion du système d'exploitation au niveau du nœud.

> **Remarque**
>
> Dans cette version de la plateforme de BI, les serveurs ne sont plus configurés dans le CCM (Central Configuration Manager). Un nouveau Server Intelligence Agent (SIA) doit être créé à la place.

1. Dans le CCM, créez un nœud pour les serveurs de traitement SAP.

   Donnez au nœud un nom approprié, par exemple, **`ProcesseurSAP`**.
2. Dans le CCM, ajoutez les serveurs de traitement requis au nouveau nœud, puis démarrez les nouveaux serveurs.

9.5.6.3.4 Pour configurer l'accès au PSE

Après avoir configuré les nœuds et les serveurs de la plateforme de BI, vous devez configurer l'accès au PSE à l'aide de l'outil SAPGENPSE.

1. Exécutez la commande suivante à partir de l'invite de commande :

   `sapgenpse.exe seclogin -p SBOE.pse`

   > **Remarque**
   >
   > Vous êtes invité à entrer le code PIN du PSE. Si vous exécutez l'outil sous les mêmes références de connexion que les serveurs de traitement SAP de la plateforme de BI, vous n'avez pas besoin de spécifier un nom d'utilisateur.

2. Pour vérifier que la liaison de connexion unique (SSO) est établie, affichez le contenu du PSE à l'aide de la commande suivante :

   `sapgenpse.exe maintain_pk -l`

   Les résultats doivent se présenter comme suit :

   ```
   C:\Documents and
   Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My
   Documents\snc\sec\bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ------------------------------------------------------------
              Version:                  0 (X.509v1-1988)
              SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
              IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
              SerialNumber:             00
              Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                  NotAfter:
   Thu Dec 31 16:00:01 2037 (380101000001Z)
              Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
              SubjectKey:               Algorithm RSA (OID
   1.2.840.113549.1.1.1), NULL
   C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
   ```

   Vous ne devez pas être invité à entrer de nouveau le PIN du PSE une fois la commande **`seclogin`** correctement exécutée.

> **Remarque**
>
> Si vous rencontrez des problèmes pour accéder au PSE, utilisez l'argument `-O` pour spécifier l'accès au PSE. Par exemple, pour accorder l'accès au PSE à un utilisateur spécifique dans un domaine spécifique, sous Windows, saisissez :
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 Pour configurer les paramètres SNC d'authentification SAP

Lorsque vous avez configuré l'accès au PSE, vous devez configurer les paramètres d'authentification SAP dans la CMC (Central Management Console).

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*.

   Les paramètres des systèmes d'autorisation s'affichent.
3. Cliquez sur l'onglet *Paramètres SNC* de la page *Authentification SAP*.
4. Sélectionnez le système d'autorisation approprié dans la liste *Nom de système logique*.
5. Sélectionnez *Activer la communication réseau sécurisée (SNC)* sous *Paramètres de base*.
6. Sélectionnez l'option *Utiliser par défaut* pour accepter le chemin d'accès à la bibliothèque par défaut ou sélectionnez l'option *Définir le chemin d'accès personnalisé* pour choisir un emplacement différent.

7. Sélectionnez un niveau de protection sous *Qualité de la protection*.

   Par exemple, sélectionnez *Authentification*.

   > **Remarque**
   >
   > Ne dépassez pas le niveau de protection configuré sur le système SAP. Le niveau de protection est personnalisable et déterminé par les besoins de votre entreprise et les fonctions de sa bibliothèque SNC.
   >
   > *Qualité de la protection* se rapporte uniquement au traitement, côté plateforme. Par exemple, le visualiseur DHTML doit être conforme au niveau spécifié. Cependant, la communication côté client avec SAP Business Warehouse (BW) doit être considérée comme étant non protégée. Par exemple, la communication de Web Intelligence Rich Client ou l'outil de conception d'information est toujours crypté(e).

8. Saisissez le nom SNC du système SAP sous *Paramètres d'authentification mutuelle*.

   Le format de nom SNC dépend de la bibliothèque SNC. Avec la bibliothèque cryptographique SAP, le nom distinctif doit suivre les conventions d'appellation LDAP et comporter le préfixe `p:` .

9. Vérifiez si le nom SNC des références de connexion selon lesquelles les serveurs de la plateforme de BI s'exécutent figure dans la zone *Nom SNC du système Enterprise*.

   Si plusieurs noms SNC sont configurés, ce champ doit rester vide.

10. Indiquez le DN du système SAP et du PSE de la plateforme de BI.

9.5.6.3.6 Utilisation de groupes de serveurs

Si la connexion aux serveurs de traitement (Crystal Reports ou Web Intelligence) n'a pas été effectuée avec des références autorisant l'accès au PSE, vous devez créer un groupe de serveurs spécifique ne contenant que ces serveurs ainsi que les serveurs requis de prise en charge. Pour obtenir des informations et des descriptions supplémentaires relatives aux serveurs de la plateforme de BI, voir le chapitre « Architecture ».

Il existe trois options pour la configuration des serveurs de traitement du contenu SAP :

1. Conservez un seul SIA, comprenant tous les serveurs de la plateforme de BI auxquels la connexion a été effectuée avec des références ayant accès au PSE. Cette option est la plus simple et ne nécessite pas la création de groupes de serveurs. Donnant accès au PSE à un grand nombre de serveurs, cette option est également celle offrant le niveau de sécurité le plus faible.
2. Créez un deuxième SIA ayant accès au PSE et ajoutez-lui les serveurs de traitement Crystal Reports ou Web Intelligence. Supprimez les serveurs dupliqués du SIA d'origine. La création de groupes de serveurs n'est pas nécessaire, mais le nombre de serveurs ayant accès au PSE est inférieur à celui de la première option.
3. Créez un SIA destiné exclusivement à SAP et ayant accès au PSE. Ajoutez-lui les serveurs de traitement Crystal Reports ou Web Intelligence. Avec cette option, seul le contenu SAP doit être exécuté sur ces serveurs et, surtout, le contenu SAP ne doit être exécuté que sur ces serveurs. Le contenu devant être dirigé vers certains serveurs, vous devrez créer des groupes de serveurs pour le SIA.

Instructions sur l'utilisation d'un groupe de serveurs

Le groupe de serveurs doit faire référence au SIA utilisé exclusivement pour le traitement du contenu SAP. Il doit en outre faire référence aux serveurs suivants :

- serveurs Adaptive Server
- Aux Adaptive Job Servers

Tout le contenu SAP, tous les documents Web Intelligence et tous les rapports Crystal doivent être associés le plus strictement possible au groupe de serveurs, c'est-à-dire qu'ils doivent être exécutés sur des serveurs du groupe. Une fois cette association effectuée à niveau d'objet, le paramètre de groupe de serveurs doit être propagé aux paramètres pour la planification directe et pour les publications.

Afin d'éviter le traitement de tout autre contenu (non SAP) sur les serveurs de traitement spécifiques à SAP, vous devez créer un autre groupe de serveurs comprenant tous les serveurs sous le SIA d'origine. Il est recommandé de configurer une association stricte entre ce contenu et le groupe de serveurs non SAP.

9.5.6.4 Configuration de publications multipassage

Dépannage des publications multipassage

Si vous rencontrez des problèmes avec les publications multipassage, activez la fonction de traces pour le pilote Crystal Reports (CR) ou Multidimensional Data Access (MDA) et recherchez la chaîne de connexion utilisée pour chaque tâche ou destinataire. Ces chaînes de connexion ont l'aspect suivant :

```
 SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

La chaîne de connexion doit avoir la valeur **`EXTIDTYPE=UN`** (pour le nom d'utilisateur) appropriée et **`EXTIDDATA`** doit être le nom d'utilisateur SAP du destinataire. Dans cet exemple, la tentative de connexion a réussi.

9.5.6.5 Workflow d'intégration à la communication réseau sécurisée (SNC)

La plateforme de BI prend en charge les environnements qui implémentent la communication réseau sécurisée (SNC) pour l'authentification et le cryptage des données entre les composants SAP. Si vous avez déployé la bibliothèque cryptographique SAP (ou un autre produit de sécurité externe utilisant l'interface SNC), vous devez configurer certaines valeurs supplémentaires pour intégrer efficacement la plateforme de BI à votre environnement sécurisé.

Pour configurer la plateforme de BI de façon à utiliser votre communication réseau sécurisée, vous devez exécuter les tâches suivantes :

1. Configurez les serveurs de la plateforme de BI de manière à ce qu'ils démarrent et s'exécutent sous un compte utilisateur adéquat.
2. Configurez le système SAP de manière à ce qu'il sécurise le système de votre plateforme de BI.
3. Configurez les paramètres SNC dans le lien SNC de la CMC (Central Management Console).
4. Importez les utilisateurs et les rôles SAP dans la plateforme de BI.

Informations associées

Importation de rôles SAP [page 350]

9.5.6.6 Configuration des paramètres SNC dans la Central Management Console

Avant de pouvoir configurer les paramètres SNC, vous devez ajouter un nouveau système d'autorisation à la plateforme de BI, vous assurer que le fichier de la bibliothèque SNC se trouve dans un répertoire connu et créer une variable d'environnement `<RFC_LIB>` pour désigner le fichier.

1. Cliquez sur l'onglet *Paramètres SNC* de la page *Authentification SAP*.
2. Sélectionnez le système d'autorisation approprié dans la liste *Nom de système logique*.
3. Sélectionnez *Activer la communication réseau sécurisée (SNC)* sous *Paramètres de base*.
4. Si vous configurez l'authentification SAP pour l'utilisation d'univers `.unx` ou de connexions OLAP BICS et prévoyez l'emploi de STS, cochez la case *Interdire les connexions RFC entrantes non sécurisées*.
5. Sélectionnez l'option *Utiliser par défaut* pour accepter le chemin d'accès à la bibliothèque par défaut ou sélectionnez l'option *Définir le chemin d'accès personnalisé* pour choisir un emplacement différent.

   Le serveur d'applications Web et le CMS doivent être sous le même type de système d'exploitation et avoir le même chemin d'accès à la bibliothèque cryptographique.
6. Sélectionnez un niveau de protection sous *Qualité de la protection*.

   Par exemple, sélectionnez *Authentification*.

   > **Remarque**
   >
   > Le niveau de protection est personnalisable et déterminé par les besoins de votre entreprise et les fonctions de sa bibliothèque SNC.
7. Saisissez le nom SNC du système SAP sous *Paramètres d'authentification mutuelle*.

   Le format de nom SNC dépend de la bibliothèque SNC. Avec la bibliothèque cryptographique SAP, le nom distinctif doit suivre les conventions d'appellation LDAP et comporte le préfixe `p:`.
8. Vérifiez que le nom SNC des références de connexion selon lesquelles les serveurs de la plateforme de BI s'exécutent figure dans la zone *Nom SNC du système Enterprise*.
9. Cliquez sur *Mettre à jour*.

Informations associées

Connexion aux systèmes d'autorisation de SAP [page 344]

9.5.6.7 Pour associer l'utilisateur d'autorisation à un nom de SNC

1. Connectez-vous à votre système SAP BW, puis exécutez la transaction `SU01`.

   L'écran "Maintenance des utilisateurs : Ecran initial" s'ouvre.
2. Dans le champ *Utilisateur*, saisissez le nom du compte SAP désigné comme utilisateur d'autorisation, puis cliquez sur *Modifier* dans la barre d'outils.

   L'écran Gérer utilisateur s'ouvre.
3. Cliquez sur l'onglet SNC.
4. Dans le champ *Nom SNC*, saisissez `COMPTE UTILISATEUR SNC`, comme à l'étape 2.
5. Cliquez sur *Enregistrer*.

9.5.6.8 Pour ajouter un ID système à la liste des contrôles d'accès à SNC

1. Connectez-vous à votre système SAP BW, puis exécutez la transaction `SNC0`.

   L'écran de changement de vue "SNC : liste de contrôle d'accès (ACL) pour les systèmes : présentation" s'ouvre.
2. Cliquez sur *New Entries* (Nouvelles entrées) dans la barre d'outils.

   L'écran "Nouvelles entrées : Détails des entrées ajoutées" s'affiche.
3. Saisissez le nom de votre ordinateur de la plateforme de BI dans le champ *ID système*.
4. Saisissez `p:<NOM UTILISATEUR SNC>` dans le champ *SNC user name* (Nom d'utilisateur SNC), où `NOM UTILISATEUR SNC` représente le compte que vous avez utilisé lors de la configuration des serveurs de la plateforme de BI.

   > **Remarque**
   >
   > Si votre fournisseur SNC est gssapi32.dll, le nom d'utilisateur SNC doit être saisi en majuscules. Vous devez inclure le nom de domaine lors de la spécification du compte utilisateur. Par exemple : domaine\nomutilisateur
5. Sélectionnez *Entrée pour RFC activée* et *Entrée pour ID externe activée*.
6. Désactivez toutes les autres options, puis cliquez sur *Enregistrer*.

9.5.7 Configuration de la connexion unique au système SAP

Différents services du backend et client de la plateforme de BI interagissent avec les systèmes backend ABAP de SAP NetWeaver dans un environnement intégré. Il est utile de configurer la connexion unique de la plateforme de BI à ces systèmes backend (habituellement BW). Après configuration d'un système ABAP comme système d'authentification externe, les jetons SAP propriétaires sont utilisés pour fournir un mécanisme qui prend en charge la connexion unique de tous les clients et services de la plateforme de BI et des services se connectant aux systèmes ABAP de SAP NetWeaver.

Pour en savoir plus, voir la note SAP 1670073.

Pour activer la connexion unique au système SAP, vous devez créer un fichier `keystore` et un certificat correspondant. Utilisez le programme de ligne de commande `keytool` pour générer le fichier et le certificat. Le programme keytool est installé par défaut dans le répertoire `sdk/bin` de chaque plateforme.

Le certificat doit être ajouté au système SAP ABAP BW et à la plateforme de BI à l'aide de la CMC.

> **Remarque**
>
> Le plug-in d'authentification SAP doit être configuré pour pouvoir paramétrer la connexion unique à la base de données utilisée par SAP BW.

9.5.7.1 Génération du fichier de stockage de clés

La rubrique contient des instructions sur l'utilisation de l'utilitaire keytool de Java pour la génération de fichiers de stockage des clés. Le tableau ci-dessous répertorie les emplacements par défaut de l'utilitaire keytool de Java :

Plateforme	Emplacement par défaut
Windows	`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\ win64_x64\sapjvm\bin`
Linux	`sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool`

1. Accédez à l'emplacement par défaut de l'utilitaire keytool de Java et lancez l'invite de commandes.
2. Exécutez l'utilitaire keytool de Java pour générer le fichier de stockage des clés.
   a. Accédez à <INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.
   b. Exécutez la commande suivante :
      - Windows : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
      - Linux : `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

→ Conseil

Pour remplacer les valeurs par défaut, exécutez l'outil avec le paramètre -?. Le message suivant s'affiche :

{·} Exemple de code

```
Usage: keytool -genkey <options>
        -keystore <filename(keystore.p12)>
        -alias <key entry alias(mywin)>
        -storepass <keystore password (admin1)>
        -dname <certificate subject DN(CN=palmtree)>
        -validity <number of days (365)>
        -cert <filename (cert.der)>
         (No certificate is generated when importing a keystore)
        -importkeystore <filename>
```

Vous pouvez utiliser les paramètres pour remplacer les valeurs par défaut.

ⓘ Remarque

L'utilitaire keytool de Java remplace l'outil PKCS12 pour la génération d'un fichier de stockage des clés. Pour en savoir plus, voir 2524775.

9.5.7.2 Exportation du certificat de clé publique

Vous devez créer et exporter un certificat pour le fichier de stockage de clés.

1. Lancez une invite de commande et accédez au répertoire où se trouve le programme keytool
2. Pour exporter un certificat de clé pour le fichier de stockage de clés, utilisez la commande suivante :

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

Remplacez <fichier de stockage de clés> par le nom du fichier de stockage de clés.
Remplacez <nom de fichier> par le nom du certificat.
Remplacez <alias> par l'alias utilisé pour créer le fichier de stockage de clés.

3. Quand vous y êtes invité, saisissez le mot de passe que vous avez fourni pour le fichier de stockage de clés.

Vous avez alors un fichier de stockage de clés et un certificat dans le répertoire où se trouve le programme keytool.

9.5.7.3 Importation du fichier du certificat dans le système ABAP SAP cible

Il vous faut un fichier de stockage de clés et un certificat associé pour votre déploiement de la plateforme de BI afin d'effectuer la tâche suivante.

> **Remarque**
>
> Cette action ne peut s'effectuer que sur un système ABAP SAP.

1. Connectez-vous au système SAP ABAP BW à l'aide de l'interface utilisateur SAP.

   > **Remarque**
   >
   > Vous devez vous connecter en tant qu'utilisateur possédant des droits d'administrateur.

2. Exécutez STRUSTSSO2 dans l'interface utilisateur SAP.
   Le système est prêt pour l'importation du fichier de certificat.
3. Accédez à l'onglet *Certificat*.
4. Assurez-vous que la case *Utiliser l'option binaire* est cochée.
5. Cliquez sur le bouton du chemin du fichier pour accéder à l'emplacement où se trouve le fichier du certificat.
6. Cliquez sur la coche verte.
   Le fichier de certificat est téléchargé.
7. Cliquez sur *Ajouter à la liste de certificats*.
   Le certificat est affiché dans la liste de certificats.
8. Cliquez sur *Ajouter à ACL* et spécifiez un ID système et un client.

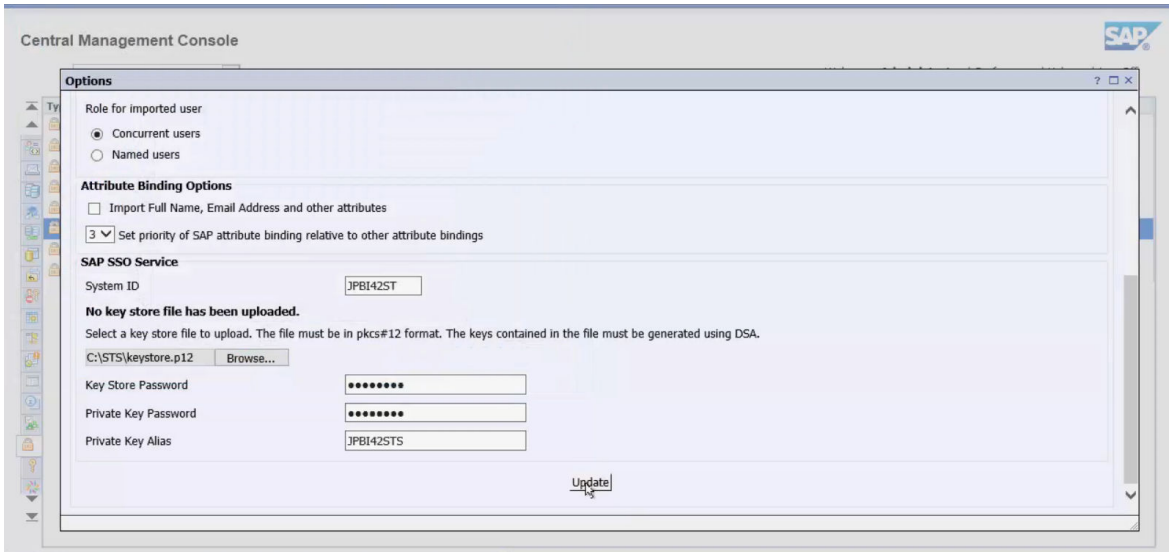
   L'ID système doit être celui utilisé pour identifier le système de la plateforme de BI dans SAP BW.

   Le certificat est ajouté à la liste de contrôle d'accès (ACL). Le client doit être spécifié comme suit : « 000 ».
9. Enregistrez vos paramètres et quittez.
   Les modifications sont enregistrées dans le système SAP.

9.5.7.4 Configuration de la connexion unique à la base de données SAP dans la CMC

Pour appliquer la procédure suivante, vous devez accéder au plug-in de sécurité SAP à l'aide d'un compte administrateur.

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur le lien *SAP*, puis cliquez sur l'onglet *Options*.



Si aucun certificat n'a été importé, le message suivant doit s'afficher dans la section *Service de connexion unique SAP* :

```
Aucun fichier de stockage de clés n'a été téléchargé
```

3. Spécifiez l'ID système de votre système de la plateforme de BI dans le champ prévu.

   Il doit être identique à la valeur utilisée pour importer le certificat dans le système ABAP SAP cible.

4. Cliquez sur le bouton *Parcourir* pour localiser le fichier de stockage de clés.
5. Fournissez les détails obligatoires suivants :

Champ	Informations requises
Mot de passe du stockage de clés	Fournissez le mot de passe requis pour accéder au fichier de stockage de clés. Ce mot de passe a été spécifié lors de la création du fichier de stockage de clés.
Mot de passe de la clé privée	Fournissez le mot de passe requis pour accéder au certificat correspondant au fichier de stockage de clés. Ce mot de passe a été spécifié lors de la création du certificat du fichier de stockage de clés.
Alias de clé privée	Fournissez l'alias requis pour accéder au fichier de stockage de clés. Cet alias a été spécifié lors de la création du fichier de stockage de clés.

6. Cliquez sur *Mettre à jour* pour soumettre vos paramètres.
   Une fois que les paramètres ont bien été soumis, le message suivant s'affiche sous le champ ID système :

   ```
   Le fichier de stockage de clés a été téléchargé
   ```

9.5.7.5 Ajout du service de jetons de sécurité au serveur de traitement adaptatif

Dans un environnement en cluster, des services de jetons de sécurité sont ajoutés séparément à chaque serveur de traitement adaptatif.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur *Services principaux*.
   La liste des serveurs s'affiche sous *Services principaux*.
3. Cliquez avec le bouton droit sur le serveur de traitement adaptatif et sélectionnez *Arrêter le serveur*.

   Ne continuez pas tant que l'état du serveur n'est pas Arrêté.
4. Cliquez avec le bouton droit sur le serveur de traitement adaptatif et sélectionnez *Sélectionner des services*.
   La boîte de dialogue *Sélectionner des services* s'affiche.
5. Utilisez le bouton *Ajouter* pour déplacer le service de jetons de sécurité de la liste *Services disponibles* à la liste *Services*.
6. Cliquez sur *OK*.
7. Redémarrez le serveur de traitement adaptatif.

9.5.8 Configuration de la connexion unique pour SAP Crystal Reports et SAP NetWeaver

Par défaut, la plateforme de BI est configurée pour permettre aux utilisateurs de SAP Crystal Reports d'accéder aux données SAP à l'aide de la connexion unique.

9.5.8.1 Pour désactiver la connexion unique pour SAP NetWeaver et SAP Crystal Reports

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sélectionnez l'un des deux pilotes suivants :

Pilote	Nom affiché
Pilote du magasin de données opérationnelles	*crdb_ods*
pilote Open SQL	*crdb_opensql*
Pilote InfoSet	*crdb_infoset*
pilote BW MDX Query	*crdb_bwmdx*

5. Cliquez sur *Supprimer*.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez SAP Crystal Reports.

9.5.8.2 Pour réactiver la connexion unique pour SAP NetWeaver et SAP Crystal Reports

Pour réactiver la connexion unique pour SAP NetWeaver (ABAP) et SAP Crystal Reports, procédez comme suit.

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sous *Utiliser le contexte de connexion unique pour se connecter à la base de données*, saisissez :

`crdb_ods`	Pour activer le pilote ODS
`crdb_opensql`	Pour activer le pilote Open SQL
`crdb_bwmdx`	Pour activer le pilote SAP BW MDX Query
`crdb_infoset`	Pour activer le pilote InfoSet

5. Cliquez sur *Ajouter*.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez SAP Crystal Reports.

9.6 Authentification PeopleSoft

9.6.1 Présentation

Pour utiliser vos données PeopleSoft Enterprise avec la plateforme de BI, vous devez fournir au programme les informations sur votre déploiement. Ces informations permettent à la plateforme de BI d'authentifier les utilisateurs afin qu'ils puissent utiliser leurs références de connexion PeopleSoft pour se connecter au programme.

9.6.2 Activation de l'authentification PeopleSoft Enterprise

Pour que les informations de PeopleSoft Enterprise puissent être utilisées par la plateforme de BI, la plateforme de BI a besoin d'informations sur le mode d'authentification dans votre système PeopleSoft Enterprise.

9.6.2.1 Pour activer l'authentification PeopleSoft Enterprise dans la plateforme de BI

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez deux fois sur *PeopleSoft Enterprise*.
   La page *PeopleSoft Enterprise* s'affiche. Elle comporte quatre onglets : *Options*, *Domaines*, *Rôles* et *Mise à jour de l'utilisateur*.
4. Dans l'onglet *Options*, cochez la case *Activer l'authentification PeopleSoft Enterprise*.
5. Effectuez les modifications appropriées dans les champs *Nouvel alias*, *Options de mise à jour* et *Options de nouvel utilisateur* en fonction de votre déploiement de plateforme de BI.

   Cliquez sur *Mettre à jour* pour enregistrer vos modifications avant de passer à l'onglet *Domaines*.
6. Cliquez sur l'onglet *Domaines*.
7. Dans la zone *Utilisateur système PeopleSoft Enterprise*, saisissez un nom d'utilisateur et un mot de passe de base de données qui seront utilisés par la plateforme de BI pour se connecter à votre base de données PeopleSoft Enterprise.
8. Dans la zone *Domaines PeopleSoft Enterprise*, saisissez le nom de domaine et l'adresse QAS utilisés pour se connecter à votre environnement PeopleSoft Enterprise, puis cliquez sur *Ajouter*.

   > **Remarque**
   >
   > Si vous disposez de plusieurs domaines PeopleSoft, répétez cette étape pour chaque domaine supplémentaire auquel vous souhaitez accéder. Le premier domaine que vous saisissez deviendra le domaine par défaut.
9. Cliquez sur *Mettre à jour* pour enregistrer les modifications.

9.6.3 Mappage de rôles PeopleSoft à la plateforme de BI

La plateforme de BI crée automatiquement un groupe pour chaque rôle PeopleSoft que vous mappez. De même, le programme crée des alias pour représenter les membres des rôles PeopleSoft mappés.

Vous pouvez créer un compte utilisateur pour chaque alias créé.

Cependant, si vous exécutez plusieurs systèmes et que vos utilisateurs possèdent des comptes sur plusieurs systèmes, vous pouvez affecter chaque utilisateur à un alias avec le même nom avant de créer les comptes sur la plateforme de BI.

Cela permet de réduire le nombre de comptes créés pour un même utilisateur sur la plateforme de BI.

Par exemple, si vous exécutez PeopleSoft HR 8.3 et PeopleSoft Financials 8.4, et que 30 de vos utilisateurs ont accès aux deux systèmes, 30 comptes seulement sont créés pour ces utilisateurs. Si vous choisissez de ne pas affecter chaque utilisateur à un alias avec le même nom, 60 comptes sont créés pour les 30 utilisateurs sur la plateforme de BI.

Cependant, si vous exécutez plusieurs systèmes et que les noms d'utilisateurs identiques créent des conflits, vous devez créer un compte de membre pour chaque alias créé.

Par exemple, si vous exécutez PeopleSoft HR 8.3 avec un compte utilisateur pour Russell Aquino (nom d'utilisateur "raquino") et que vous exécutez PeopleSoft Financials 8.4 avec un compte utilisateur pour Raoul

Aquino (nom d'utilisateur "raquino"), vous devez créer un compte distinct pour l'alias de chaque utilisateur. Sinon, les deux utilisateurs sont ajoutés au même compte de la plateforme de BI. Ils pourront se connecter à la plateforme de BI avec leurs propres références de connexion PeopleSoft et auront accès aux données des deux systèmes PeopleSoft.

9.6.3.1 Pour mapper un rôle PeopleSoft à la plateforme de BI

Si la JVM (Java virtual machine) de la plateforme de BI ne possède pas de certificat pour le serveur PeopleSoft, suivez ces étapes supplémentaires avant les étapes principales ci-dessous :

1. Récupérez le fichier .cer depuis le serveur PeopleSoft.
2. Copiez le fichier .cer à l'emplacement `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Exécutez la commande suivante depuis le répertoire de sécurité : `"<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`.
4. Redémarrez le serveur d'applications Web.

Étapes principales :

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Cliquez sur *Authentification*.
3. Cliquez deux fois sur *PeopleSoft Enterprise*.
4. Dans l'onglet *Rôles*, dans la zone Domaines PeopleSoft Enterprise, sélectionnez le domaine associé au rôle à mapper à la plateforme de BI.
5. Utilisez l'une des options suivantes pour sélectionner les rôles que vous souhaitez mapper :
   - Dans la zone *Rôles PeopleSoft Enterprise*, dans la zone Rechercher des rôles, saisissez le rôle que vous souhaitez localiser et mapper à la plateforme de BI, puis cliquez sur >.
   - Dans la liste *Rôles disponibles*, sélectionnez le rôle à mapper à la plateforme de BI, puis cliquez sur >.

   > **Remarque**
   >
   > Lorsque vous recherchez un utilisateur ou un rôle particulier, vous pouvez utiliser le caractère générique %. Par exemple, pour rechercher tous les rôles commençant par "A", saisissez *A%*. La recherche respecte également la casse.

   > **Remarque**
   >
   > Si vous voulez mapper un rôle d'un autre domaine, vous devez sélectionner le nouveau domaine dans la liste des domaines disponibles pour mettre en correspondance un rôle d'un autre domaine.

6. Accédez à l'onglet *Mise à jour de l'utilisateur*, puis cliquez sur le bouton *Mettre à jour* ou planifiez les mises à jour.
7. Dans l'onglet *Options*, accédez à la zone *Options de nouvel utilisateur* et sélectionnez une des options suivantes :
   - *Affecter chaque alias ajouté à un compte portant le même nom*

Sélectionnez cette option si vous exécutez plusieurs systèmes PeopleSoft Enterprise avec des utilisateurs possédant des comptes sur plusieurs systèmes (et si deux utilisateurs ne possèdent pas des noms identiques sur les différents systèmes).

- *Créer un compte pour chaque alias ajouté*
  Sélectionnez cette option si vous exécutez un seul système PeopleSoft Enterprise, si la majorité de vos utilisateurs possèdent des comptes sur un seul de vos systèmes ou si des noms d'utilisateurs identiques créent des conflits sur deux de vos systèmes ou plus.

8. Dans la zone *Options de mise à jour des alias*, sélectionnez l'une des options suivantes :
   - *Créer de nouveaux alias lors de la mise à jour des alias*
     Sélectionnez cette option pour créer un alias pour chaque utilisateur mappé à la plateforme de BI. De nouveaux comptes sont ajoutés pour les utilisateurs dépourvus de comptes de la plateforme de BI ou pour tous les utilisateurs si vous avez sélectionné l'option Créer un nouveau compte pour chaque alias ajouté.
   - *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
     Sélectionnez cette option si le rôle que vous souhaitez mapper contient plusieurs utilisateurs dont un petit nombre utilisera la plateforme de BI. La plateforme ne crée pas automatiquement d'alias ni de comptes pour les utilisateurs. À la place, elle crée des alias (et des comptes, au besoin) uniquement pour les utilisateurs lorsqu'ils se connectent pour la première fois à la plateforme de BI. Il s'agit de l'option par défaut.
9. Dans la zone *Options de nouvel utilisateur*, indiquez le nombre d'utilisateurs créés.

   Sélectionnez l'une des options suivantes :

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
     Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

     > **Remarque**
     >
     > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
     >
     > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
     Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs à la plateforme de BI, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

   Les rôles que vous avez sélectionnés apparaissent maintenant sous forme de groupes sur la plateforme de BI.

9.6.3.2 Remarques sur le remappage

Si vous ajoutez des utilisateurs à un rôle déjà mappé à la plateforme de BI, vous devrez remapper le rôle pour ajouter les utilisateurs à la plateforme de BI. Lorsque vous remappez le rôle, l'option de mappage des utilisateurs en tant qu'utilisateurs nommés ou simultanés affecte uniquement les nouveaux utilisateurs que vous avez ajoutés au rôle.

Par exemple, vous mappez d'abord un rôle à la plateforme de BI en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *nommés*". Ensuite, vous ajoutez des utilisateurs au même rôle et remappez le rôle en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *simultanés*".

Dans ce cas, seuls les nouveaux utilisateurs dans le rôle sont mappés à la plateforme de BI en tant qu'utilisateurs simultanés ; les utilisateurs qui étaient déjà mappés demeurent des utilisateurs nommés. La même condition s'applique si vous mappez d'abord les utilisateurs en tant qu'utilisateurs simultanés et que vous modifiez ensuite les paramètres pour remapper les nouveaux utilisateurs en tant qu'utilisateurs nommés.

9.6.3.3 Pour démapper un rôle

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Cliquez sur *Authentification*.
3. Cliquez sur *PeopleSoft Enterprise*.
4. Cliquez sur *Rôles*.
5. Sélectionnez le rôle à supprimer, puis cliquez sur <.
6. Cliquez sur *Mettre à jour*.

   Les membres de ce rôle ne pourront plus accéder à la plateforme de BI, à moins de posséder d'autres comptes ou alias.

   > **Remarque**
   >
   > Vous pouvez également supprimer des comptes individuels ou retirer des utilisateurs des rôles avant de les mapper à la plateforme de BI afin d'empêcher certains utilisateurs de se connecter.

9.6.4 Planification de mises à jour utilisateur

Pour vous assurer que les modifications des données utilisateur de votre système ERP sont correctement reflétées dans les données utilisateur de votre plateforme de BI, vous pouvez planifier des mises à jour d'utilisateurs régulières. Ces mises à jour synchronisent automatiquement les utilisateurs d'ERP et de la plateforme de BI selon les paramètres de mappage configurés dans la CMC (Central Management Console).

Il existe deux options pour l'exécution et la planification des mises à jour de rôles importés :

- Mettre à jour les rôles uniquement : cette option permet de mettre à jour uniquement les liens entre les rôles actuellement mappés qui ont été importés dans la plateforme de BI. Utilisez cette option si vous avez l'intention d'exécuter des mises à jour fréquentes et que vous êtes préoccupé par l'utilisation des

ressources système. Aucun nouveau compte utilisateur ne sera créé si vous effectuez uniquement une mise à jour des rôles.

- Mettre à jour les rôles et les alias : cette option permet non seulement de mettre à jour les liens entre les rôles, mais aussi de créer des comptes utilisateur dans la plateforme de BI pour les nouveaux alias utilisateur ajoutés au système ERP.

> **ⓘ Remarque**
>
> Si vous n'avez pas spécifié de créer automatiquement des alias utilisateur pour les mises à jour lors de l'activation de l'authentification, aucun compte ne sera créé pour les nouveaux alias.

9.6.4.1 Pour planifier des mises à jour utilisateur

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer comment le système doit les mettre à jour.

1. Cliquez sur l'onglet *Mise à jour de l'utilisateur*.
2. Cliquez sur *Planifier* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

   > **→ Conseil**
   >
   > Pour exécuter une mise à jour immédiate, cliquez sur *Mettre à jour maintenant*.

   > **→ Conseil**
   >
   > Utilisez l'option *Mettre à jour les rôles uniquement* si vous souhaitez effectuer des mises à jour fréquentes et que vous êtes préoccupé par les ressources système. Le système met plus de temps à mettre à jour à la fois les rôles et les alias.

   La boîte de dialogue *Périodicité* s'affiche.
3. Sélectionnez une option dans la liste *Exécuter l'objet* et indiquez toutes les informations de planification demandées.

   Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous pouvez spécifier l'heure à laquelle l'exécution démarrera, de même que sa date de début et sa date de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les N jours. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Toutes les semaines	La mise à jour s'exécutera toutes les semaines. Elle peut être exécutée une ou plusieurs fois par semaine. Vous pouvez préciser les jours et l'heure auxquels l'exécution doit avoir lieu, ainsi qu'une date de début et une date de fin.

Schéma de périodicité	Description
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

4. Cliquez sur *Planifier* une fois les informations de planification fournies.
   La date de la prochaine mise à jour de rôles planifiée est affichée dans l'onglet *Mise à jour de l'utilisateur*.

> **Remarque**
>
> Vous pouvez annuler à tout moment la prochaine mise à jour planifiée en cliquant sur *Annuler les mises à jour planifiées* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

9.6.5 Utilisation de la passerelle de sécurité PeopleSoft

La fonction Passerelle de sécurité de la plateforme de BI permet d'importer les paramètres de sécurité PeopleSoft EPM sur la plateforme de BI.

Cette fonction opère dans deux modes :

- **Mode Configuration**
  En mode Configuration, la passerelle de sécurité fournit une interface qui permet de créer un fichier réponse. Ce fichier réponse régit le comportement de la passerelle de sécurité en mode Exécution.
- **Mode Exécution**
  Selon les paramètres que vous définissez dans le fichier réponse, la passerelle de sécurité importe les paramètres de sécurité des tables de dimensions de PeopleSoft EPM dans les univers de la plateforme de BI.

9.6.5.1 Importation des paramètres de sécurité

Pour importer les paramètres de sécurité, vous devez effectuer les tâches suivantes en respectant l'ordre donné :

- Définissez les objets qui seront gérés par la passerelle de sécurité.
- Créez un fichier de réponse.
- Exécutez la passerelle de sécurité.

Pour en savoir plus sur la gestion de la sécurité après avoir importé les paramètres, voir Gestion des paramètres de sécurité [page 383].

9.6.5.1.1 Définition d'objets gérés

Avant d'exécuter la passerelle de sécurité, il est important de déterminer les objets gérés par l'application. La passerelle de sécurité gère un ou plusieurs rôles PeopleSoft, un groupe Plateforme de BI et un ou plusieurs univers.

- Rôles PeopleSoft gérés
  Il s'agit de rôles du système PeopleSoft. Les membres de ces rôles travaillent avec des données PeopleSoft via PeopleSoft EPM. Vous devez choisir les rôles qui incluent les membres auxquels vous souhaitez fournir des droits d'accès aux univers gérés de la plateforme de BI ou pour lesquels vous souhaitez mettre à jour ces droits.
  Les droits d'accès définis pour les membres de ces rôles dépendent de leurs droits dans PeopleSoft EPM. La passerelle de sécurité importe ces paramètres de sécurité sur la plateforme de BI.
- Groupe Plateforme de BI géré
  Lorsque vous exécutez la passerelle de sécurité, le programme crée un utilisateur sur la plateforme de BI pour chaque membre d'un rôle PeopleSoft géré.
  Le groupe dans lequel les utilisateurs sont créés est le groupe Plateforme de BI géré. Les membres de ce groupe sont les utilisateurs dont les droits d'accès aux univers gérés sont gérés par la passerelle de sécurité. Les utilisateurs étant créés dans un seul groupe, vous pouvez configurer la passerelle de sécurité de sorte qu'elle ne mette pas à jour les paramètres de sécurité de certains utilisateurs en supprimant simplement des utilisateurs du groupe Plateforme de BI géré.
  Avant d'exécuter la passerelle de sécurité, vous devez choisir sur la plateforme de BI le groupe dans lequel les utilisateurs seront créés. Si vous spécifiez un groupe qui n'existe pas, la passerelle de sécurité crée le groupe sur la plateforme de BI.
- Univers gérés
  Les univers gérés sont les univers dans lesquels la passerelle de sécurité importe les paramètres de sécurité de PeopleSoft EPM. Vous devez choisir, dans les univers stockés dans votre système de plateforme de BI, ceux qui seront gérés par la passerelle de sécurité. Les membres de rôles PeopleSoft gérés qui sont également membres du groupe Plateforme de BI géré ne peuvent accéder à aucune donnée via les univers auxquels ils n'ont pas accès depuis PeopleSoft EPM.

9.6.5.1.2 Pour créer un fichier de réponse

1. Accédez au dossier que vous avez indiqué durant l'installation de la passerelle de sécurité et exécutez le fichier `crpsepmsecuritybridge.bat` (sous Windows) et `crpsempsecuritybridge.sh` (sous Unix).

   > **Remarque**
   >
   > Sous Windows, cet emplacement est par défaut `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

   La boîte de dialogue Passerelle de sécurité pour PeopleSoft EPM apparaît.
2. Sélectionnez *Nouveau* pour créer un fichier réponse, ou sélectionnez *Ouvrir* et cliquez sur *Parcourir* pour spécifier le fichier réponse que vous souhaitez modifier. Sélectionnez la langue que vous souhaitez pour le fichier.
3. Cliquez sur *Suivant*.
4. Indiquez les emplacements du SDK *PeopleSoft EPM* et du SDK *Plateforme de BI*.

   > **Remarque**
   >
   > Le SDK PeopleSoft EPM se trouve généralement sur le serveur PeopleSoft dans `<PS_HOME>/class/com.peoplesoft.epm.pf.jar.`

   > **Remarque**
   >
   > Le SDK de la plateforme de BI se trouve généralement dans `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.
5. Cliquez sur *Suivant*.

   La boîte de dialogue suivante vous invite à fournir des informations relatives à la connexion et au pilote pour la base de données PeopleSoft.
6. Dans la liste de bases de données, sélectionnez le type de base de données approprié et renseignez les champs suivants :

Champ	Description
Base de données	Le nom de la base de données PeopleSoft.
Hôte	Le nom du serveur qui héberge la base de données.
Numéro de port	Le numéro de port pour accéder au serveur.
Emplacement de classe	L'emplacement des fichiers de classe pour le pilote de base de données.
Nom d'utilisateur	Votre nom d'utilisateur.
Mot de passe	Votre mot de passe.

7. Cliquez sur *Suivant*.

   La boîte de dialogue suivante affiche la liste de toutes les classes que la passerelle de sécurité utilisera pour l'exécution. Si nécessaire, vous pouvez ajouter des classes dans la liste ou en supprimer.
8. Cliquez sur *Suivant*.

   La boîte de dialogue suivante vous invite à fournir les informations de connexion à la plateforme de BI.

9. Indiquez les informations appropriées pour les champs suivants :

Champ	Description
Serveur	Le nom du serveur sur lequel est situé le CMS (Central Management Server).
Nom d'utilisateur	Votre nom d'utilisateur.
Mot de passe	Votre mot de passe.
Authentification	Votre type d'authentification.

10. Cliquez sur *Suivant*.
11. Choisissez un groupe de la plateforme de BI, puis cliquez sur *Suivant*.

> **Remarque**
>
> Le groupe que vous spécifiez dans ce champ correspond à l'emplacement dans lequel la passerelle de sécurité crée des utilisateurs pour les membres des rôles PeopleSoft gérés.

> **Remarque**
>
> Si vous spécifiez un groupe qui n'existe pas encore, il sera créé par la passerelle de sécurité.

La boîte de dialogue suivante affiche la liste des rôles du système PeopleSoft.

12. Sélectionnez l'option *Importé* pour les rôles devant être gérés par la passerelle de sécurité et cliquez sur *Suivant*.

> **Remarque**
>
> La passerelle de sécurité crée un utilisateur dans le groupe Plateforme de BI géré (spécifié à l'étape précédente) pour chaque membre de rôle que vous sélectionnez.

La boîte de dialogue suivante affiche la liste des univers de la plateforme de BI.

13. Sélectionnez les univers dans lesquels la passerelle de sécurité doit importer les paramètres de sécurité et cliquez sur *Suivant*.
14. Spécifiez un nom pour le fichier journal de la passerelle de sécurité, ainsi que son emplacement d'enregistrement. Vous pouvez utiliser ce fichier journal pour vérifier si la passerelle de sécurité importe correctement les paramètres de sécurité de PeopleSoft EPM.
15. Cliquez sur *Suivant*.

    La boîte de dialogue suivante affiche un aperçu du fichier réponse que la passerelle de sécurité utilisera en mode Exécution.

16. Cliquez sur *Enregistrer*, puis choisissez l'emplacement où vous souhaitez enregistrer le fichier réponse.
17. Cliquez sur *Suivant*.

    La création du fichier réponse de la passerelle de sécurité est à présent terminée.

18. Cliquez sur *Quitter*.

> **Remarque**
>
> Le fichier réponse est un fichier de propriétés Java que vous pouvez également créer et/ou modifier manuellement. Pour en savoir plus, voir la section « Fichier de réponse PeopleSoft ».

9.6.5.2 Application des paramètres de sécurité

Pour appliquer les paramètres de sécurité, exécutez le fichier batch `crpsepmsecuritybridge.bat` (sous Windows) ou le fichier `crpsempsecuritybridge.sh` (sous UNIX) et utilisez le fichier réponse que vous avez créé en tant qu'argument. Par exemple, tapez **`crpsepmsecuritybridge.bat myresponsefile.properties`** sous Windows ou **`crpsempsecuritybridge.sh myresponsefile.properties`** sous Unix.

La passerelle de sécurité est en cours d'exécution. Elle crée des utilisateurs sur la plateforme de BI pour les membres des rôles PeopleSoft spécifiés dans le fichier réponse et importe les paramètres de sécurité de PeopleSoft EPM dans les univers appropriés.

9.6.5.2.1 Remarques sur le mappage

En mode Exécution, la passerelle de sécurité crée un utilisateur sur la plateforme de BI pour chaque membre d'un rôle PeopleSoft géré.

Les utilisateurs sont créés de telle sorte qu'ils n'aient que des alias d'authentification Entreprise et des mots de passe aléatoires leur sont attribués par la plateforme de BI. Les utilisateurs ne peuvent donc pas se connecter à la plateforme de BI tant que l'administrateur ne réattribue pas manuellement de nouveaux mots de passe ou qu'il ne mappe pas les rôles à la plateforme de BI via le plug-in de sécurité PeopleSoft afin de permettre aux utilisateurs de se connecter à l'aide de leurs références de connexion PeopleSoft.

9.6.5.3 Gestion des paramètres de sécurité

Vous pouvez gérer les paramètres de sécurité que vous avez appliqués en modifiant les objets gérés par la passerelle de sécurité.

9.6.5.3.1 Utilisateurs gérés

La passerelle de sécurité gère les utilisateurs en fonction des critères suivants :

- Appartenance ou non de l'utilisateur à un rôle PeopleSoft géré.
- Appartenance ou non de l'utilisateur au groupe Plateforme de BI géré.

Si vous souhaitez permettre à un utilisateur d'accéder aux données PeopleSoft par l'intermédiaire d'univers de la plateforme de BI, assurez-vous que l'utilisateur est un membre, *à la fois*, d'un rôle PeopleSoft géré et du groupe Plateforme de BI géré.

- Pour les membres de rôles PeopleSoft gérés n'ayant pas de comptes sur la plateforme de BI, la passerelle de sécurité crée des comptes et leur attribue des mots de passe aléatoires. L'administrateur doit décider s'il réaffecte ou non manuellement de nouveaux mots de passe ou s'il mappe les rôles à la plateforme de BI par l'intermédiaire du plug-in de sécurité PeopleSoft afin de permettre aux utilisateurs de se connecter à la plateforme de BI.

- Pour les membres de rôles PeopleSoft gérés qui sont également membres du groupe Plateforme de BI géré, la passerelle de sécurité met à jour les paramètres de sécurité qui sont appliqués aux utilisateurs afin qu'ils aient accès aux données appropriées à partir des univers gérés.

Si un membre d'un rôle PeopleSoft géré dispose d'un compte existant sur la plateforme de BI, mais qu'il n'est *pas* membre du groupe Plateforme de BI géré, la passerelle de sécurité ne met *pas* à jour les paramètres de sécurité appliqués à cet utilisateur. En général, cette situation se produit uniquement lorsque l'administrateur supprime manuellement des comptes utilisateur qui ont été créés par la passerelle de sécurité à partir du groupe Plateforme de BI géré.

> **Remarque**
>
> Cette méthode permet de mieux gérer la sécurité : en supprimant des utilisateurs du groupe Plateforme de BI géré, vous pouvez configurer leurs paramètres de sécurité afin qu'ils soient différents de ceux qu'ils utilisent dans PeopleSoft.

Inversement, si un membre du groupe Plateforme de BI géré n'est *pas* membre d'un rôle PeopleSoft géré, la passerelle de sécurité ne lui permet *pas* d'accéder aux univers gérés. En général, cette situation se produit uniquement lorsque les administrateurs PeopleSoft suppriment des utilisateurs ayant précédemment été mappés à la plateforme de BI par la passerelle de sécurité à partir des rôles PeopleSoft gérés.

> **Remarque**
>
> Il s'agit là d'une autre méthode de gestion de la sécurité : en supprimant des utilisateurs des rôles PeopleSoft gérés, vous faites en sorte que les utilisateurs n'aient pas accès aux données PeopleSoft.

9.6.5.3.2 Univers gérés

La passerelle de sécurité gère des univers via des ensembles de restrictions qui limitent les données auxquelles les utilisateurs gérés peuvent accéder à partir des univers gérés.

Ces ensembles sont des groupes de restrictions (par exemple, restrictions relatives aux commandes de requêtes, à la génération du SQL, etc.). La passerelle de sécurité applique et met à jour les restrictions d'accès à la ligne et aux objets des univers gérés :

- Les restrictions d'accès à la ligne sont appliquées aux tables de dimensions définies dans PeopleSoft EPM. Ces restrictions sont spécifiques à l'utilisateur et peuvent être configurées de l'une des façons suivantes :
  - L'utilisateur a accès à toutes les données.
  - L'utilisateur n'a accès à aucune donnée.
  - Les utilisateurs ont accès aux données en fonction de leurs droits au niveau de la ligne dans PeopleSoft, lesquels sont exposés via les tables de jointure de sécurité (SJT, Security Join Tables) définies dans PeopleSoft EPM.
- Les restrictions Accès à l'objet sont appliquées aux objets de type indicateur en fonction des champs auxquels ces indicateurs ont accès.
  Si un indicateur accède à des champs définis comme métriques dans PeopleSoft, l'accès à l'indicateur est alors autorisé/refusé selon que l'utilisateur peut ou ne peut pas accéder aux métriques référencées dans PeopleSoft. Si un utilisateur ne peut accéder à aucune métrique, l'accès à l'indicateur est refusé. Si l'utilisateur peut accéder à toutes les métriques, l'accès à l'indicateur est alors accordé.

En tant qu'administrateur, vous pouvez également restreindre les données auxquelles les utilisateurs ont accès à partir du système PeopleSoft en limitant le nombre d'univers gérés par la passerelle de sécurité.

9.6.5.4 Fichier de réponse PeopleSoft

La fonction Passerelle de sécurité de la plateforme de BI fonctionne selon les paramètres que vous spécifiez dans un fichier réponse.

Généralement, vous générez le fichier réponse à l'aide de l'interface fournie par la passerelle de sécurité en mode Configuration. Toutefois, le fichier étant un fichier de propriétés Java, vous pouvez également le créer ou le modifier manuellement.

Cette annexe fournit des informations sur les paramètres que vous devez inclure dans le fichier réponse si vous choisissez de le générer manuellement.

> **Remarque**
>
> Lorsque vous créez le fichier, vous devez respecter les consignes relatives aux séquences d'échappement du fichier de propriétés Java (par exemple, le signe ':' correspond à '\:')

9.6.5.4.1 Paramètres du fichier de réponse

Le tableau suivant décrit les paramètres inclus dans le fichier réponse :

Paramètre	Description
classpath	Le chemin de classes pour le chargement des fichiers .jar nécessaires. Lorsqu'il y a plusieurs chemins de classes, ceux-ci doivent être séparés par le signe ';' à la fois dans Windows et UNIX. Les chemins de classes requis sont pour le fichier `com.peoplesoft.epm.pf.jar` et les fichiers .jar du pilote JDBC (Java Database Connectivity).
db.driver.name	Le nom du pilote JDBC utilisé pour se connecter à la base de données PeopleSoft (par exemple, `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	La chaîne de connexion JDBC utilisée pour se connecter à la base de données PeopleSoft (par exemple, `jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO`).

Paramètre	Description
db.user.name	Le nom d'utilisateur utilisé pour se connecter à la base de données PeopleSoft.
db.password	Le mot de passe utilisé pour se connecter à la base de données PeopleSoft.
db.password.encrypted	La valeur de ce paramètre permet de déterminer si le mot de passe dans le fichier réponse est chiffré. La valeur peut être définie sur True ou False. (Si aucune valeur n'est spécifiée, le paramètre prend la valeur False par défaut.)
enterprise.cms.name	Le CMS (Crystal Management Server) dans lequel se trouvent les univers.
enterprise.user.name	Le nom d'utilisateur utilisé pour se connecter au CMS.
enterprise.password	Le mot de passe utilisé pour se connecter au CMS.
enterprise.password.encrypted	La valeur de ce paramètre permet de déterminer si le mot de passe dans le fichier réponse est chiffré. La valeur peut être définie sur True ou False. (Si aucune valeur n'est spécifiée, le paramètre prend la valeur False par défaut.)
enterprise.authMethod	La méthode d'authentification permettant de se connecter au CMS.
enterprise.role	Le groupe Plateforme de BI géré. Pour en savoir plus, voir Définition d'objets gérés [page 380].
enterprise.license	Contrôle le type de licence lors de l'importation d'utilisateurs depuis PeopleSoft. 0 définit la licence Utilisateur nommé, 1 la licence Utilisateur Simultané.
peoplesoft.role.n	La liste de rôles PeopleSoft gérés. Pour en savoir plus, voir Définition d'objets gérés [page 380]. **<n>** est un entier, et chaque entrée occupe une propriété avec le préfixe peoplesoft.role. **Remarque** **<n>** est en base 1. Vous pouvez utiliser le signe '*' pour signaler tous les rôles PeopleSoft disponibles, étant entendu que n correspond à 1, et qu'il s'agit de la seule propriété ayant le préfixe peoplesoft.role dans le fichier réponse.

Paramètre	Description
mapped.universe.n	La liste des univers que la passerelle de sécurité doit mettre à jour. Pour en savoir plus, voir Définition d'objets gérés [page 380]. **<n>** est un entier, et chaque entrée occupe une propriété avec le préfixe mapped.universe. **Remarque** **<n>** est en base 1. Vous pouvez utiliser le signe '*' pour signaler tous les univers disponibles, étant entendu que n correspond à 1, et qu'il s'agit de la seule propriété ayant le préfixe mapped.universe dans le fichier réponse.
log4j.appender.file.File	Fichier journal enregistré par la passerelle de sécurité.
log4j.*	Propriétés log4j par défaut requises pour que log4j puisse fonctionner correctement : log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	Chemin de classes des fichiers .jar de l'API (Application Programming Interface) PeopleSoft EPM. Ce paramètre est facultatif.
enterprise.classpath	Le chemin de classes des fichiers .jar du SDK de la plateforme de BI. Ce paramètre est facultatif.

Paramètre	Description
db.driver.type	Type de la base de données PeopleSoft. Ce paramètre peut avoir l'une des valeurs suivantes : Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Personnalisé La valeur Personnalisé peut être utilisée pour spécifier des bases de données dont le type ou la version n'est pas reconnu. Ce paramètre est facultatif.
sql.db.class.location sql.db.host sql.db.port sql.db.database	Emplacement des fichiers .jar du pilote JDB SQL Server, l'ordinateur hôte SQL Server, le port SQL Server et le nom de base de données SQL Server. Ces paramètres peuvent être utilisés uniquement si db.driver.type a pour valeur Microsoft SQL Server 2000. Ces paramètres sont facultatifs.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	Emplacement des fichiers .jar du pilote JDBC Oracle, l'ordinateur hôte hébergeant la base de données Oracle, le port utilisé pour la base de données Oracle et la base de données Oracle SID. Ces paramètres peuvent être utilisés uniquement si db.driver.type a pour valeur Oracle Database 10.1. Ces paramètres sont facultatifs.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	Emplacement des fichiers .jar du pilote JDBC DB2, l'ordinateur hôte hébergeant la base de données DB2, le port utilisé pour la base de données DB2 et la base de données DB2 SID. Ces paramètres peuvent être utilisés uniquement si db.driver.type a pour valeur DB2 UDB 8.2 Fixpack 7 Ces paramètres sont facultatifs.
custom.db.class.location custom.db.drivername custom.db.connectStr	Emplacement, nom et chaîne de connexion du pilote JDBC personnalisé. Ces paramètres peuvent être utilisés uniquement si db.driver.type a pour valeur Personnalisé. Ces paramètres sont facultatifs.

9.7 Authentification JD Edwards

9.7.1 Présentation générale

Pour utiliser vos données JD Edwards avec la plateforme de BI, vous devez fournir au système les informations concernant votre déploiement JD Edwards. Ces informations permettront à la plateforme de BI d'authentifier les utilisateurs afin qu'ils puissent utiliser leurs références de connexion JD Edwards EnterpriseOne pour se connecter à la plateforme de BI.

9.7.2 Activation de l'authentification JD Edwards EnterpriseOne

Pour que les informations de JD Edwards EnterpriseOne puissent être utilisées par la plateforme de BI, la plateforme a besoin d'informations sur le mode d'authentification dans votre système JD Edwards EnterpriseOne.

9.7.2.1 Pour activer l'authentification JD Edwards dans la plateforme de BI

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez deux fois sur *JD Edwards EnterpriseOne*.
   La page *JD Edwards EnterpriseOne* s'affiche.
4. Dans l'onglet *Options*, cochez la case *Activer l'authentification JD Edwards EnterpriseOne*.
5. Effectuez les modifications appropriées dans les champs *Nouvel alias*, *Options de mise à jour* et *Options de nouvel utilisateur* en fonction de votre déploiement de plateforme de BI. Cliquez sur *Mettre à jour* pour enregistrer vos modifications avant de passer à l'onglet *Systèmes*.
6. Cliquez sur l'onglet *Servers* (Serveurs).
7. Copiez `jdeutil.jar`, `kernel.jar` et `log4j.jar` depuis l'installation JD Edwards à ces emplacements : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` et `<INSTALLDIR>\Tomcat\lib\`.
8. Redémarrez Tomcat et le Server Intelligence Agent.
9. Dans le champ *Utilisateur système JD Edwards EnterpriseOne*, saisissez un nom d'utilisateur et un mot de passe qui seront utilisés par la plateforme de BI pour se connecter à votre base de données JD Edwards EnterpriseOne.
10. Dans le champ *Domaine JD Edwards EnterpriseOne*, saisissez le nom, l'hôte et le port utilisés pour vous connecter à votre environnement JD Edwards EnterpriseOne.
11. Saisissez un nom pour l'environnement et cliquez sur *Ajouter*.
12. Cliquez sur *Mettre à jour* pour enregistrer les modifications.

9.7.3 Mappage de rôles JD Edwards EnterpriseOne à la plateforme de BI

La plateforme de BI crée automatiquement un groupe pour chaque rôle JD Edwards EnterpriseOne que vous mappez. De même, le système crée des alias pour représenter les membres des rôles JD Edwards EnterpriseOne mappés.

Vous pouvez créer un compte utilisateur pour chaque alias créé.

Cependant, si vous exécutez plusieurs systèmes et que vos utilisateurs possèdent des comptes sur plusieurs systèmes, vous pouvez affecter chaque utilisateur à un alias avec le même nom avant de créer les comptes sur la plateforme de BI.

Cela permet de réduire le nombre de comptes créés pour un même utilisateur sur la plateforme de BI.

Par exemple, si vous exécutez à la fois un environnement de test et un environnement de production JD Edwards EnterpriseOne, et si 30 de vos utilisateurs ont accès aux deux systèmes, 30 comptes seulement sont créés pour ces utilisateurs. Si vous choisissez de ne pas affecter chaque utilisateur à un alias avec le même nom, 60 comptes sont créés pour les 30 utilisateurs sur la plateforme de BI.

Cependant, si vous exécutez plusieurs systèmes et que les noms d'utilisateurs identiques créent des conflits, vous devez créer un compte de membre pour chaque alias créé.

Par exemple, si vous exécutez votre environnement de test avec un compte utilisateur pour Russell Aquino (nom d'utilisateur "raquino") et que vous exécutez votre environnement de production avec un compte utilisateur pour Raoul Aquino (nom d'utilisateur "raquino"), vous devez créer un compte distinct pour l'alias de chaque utilisateur. Sinon, les deux utilisateurs sont ajoutés au même compte de la plateforme de BI. Ils ne pourront pas se connecter à la plateforme de BI avec leurs propres références de connexion JD Edwards EnterpriseOne.

9.7.3.1 Pour mapper un rôle JD Edwards EnterpriseOne

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone *Gérer*, cliquez sur *Authentification*.
3. Cliquez deux fois sur *JD Edwards EnterpriseOne*.
4. Dans la zone *Options de nouvel alias*, sélectionnez l'une des options suivantes :
   - *Affecter chaque alias ajouté à un compte portant le même nom*
     Sélectionnez cette option si vous exécutez plusieurs systèmes JD Edwards EnterpriseOne Enterprise avec des utilisateurs possédant des comptes sur plusieurs systèmes (et si deux utilisateurs ne possèdent pas des noms identiques sur les différents systèmes).
   - *Créer un compte pour chaque alias ajouté*
     Sélectionnez cette option si vous exécutez un seul système JD Edwards EnterpriseOne Enterprise, si la majorité de vos utilisateurs possèdent des comptes sur un seul de vos systèmes ou si des noms d'utilisateurs identiques créent des conflits sur deux de vos systèmes ou plus.
5. Dans la zone *Options de mise à jour*, sélectionnez l'une des options suivantes :
   - *Les nouveaux alias seront ajoutés et les nouveaux utilisateurs seront créés*
     Sélectionnez cette option pour créer un alias pour chaque utilisateur mappé à la plateforme de BI. De nouveaux comptes sont ajoutés pour les utilisateurs dépourvus de compte plateforme de BI ou

pour tous les utilisateurs si vous avez sélectionné l'option Créer un nouveau compte pour chaque alias ajouté.

- *Aucun nouvel alias ne sera ajouté et les nouveaux utilisateurs ne seront pas créés*
  Sélectionnez cette option si le rôle que vous souhaitez mapper contient plusieurs utilisateurs dont un petit nombre utilisera la plateforme de BI. Le système ne crée pas automatiquement d'alias ni de comptes pour les utilisateurs. À la place, elle crée des alias (et des comptes, au besoin) uniquement pour les utilisateurs lorsqu'ils se connectent pour la première fois à la plateforme de BI. Il s'agit de l'option par défaut.

6. Dans la zone *Options de nouvel utilisateur*, indiquez le nombre d'utilisateurs créés.

   Sélectionnez l'une des options suivantes :

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
     Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

     > **Remarque**
     >
     > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
     >
     > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
     Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs à la plateforme de BI, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

   Les rôles que vous avez sélectionnés apparaissent maintenant sous forme de groupes sur la plateforme de BI.

7. Cliquez sur l'onglet *Rôles*.
8. Dans la zone *Liste des domaines*, sélectionnez le serveur JD Edwards qui contient les rôles à mapper.
9. Sous *Rôles disponibles*, sélectionnez les rôles que vous voulez mapper à la plateforme de BI et cliquez sur <.
10. Cliquez sur *Mettre à jour*.
    Les rôles seront mappés à la plateforme de BI.

9.7.3.2 Remarques sur le remappage

Si vous ajoutez des utilisateurs à un rôle déjà mappé à la plateforme de BI, vous devrez remapper le rôle pour ajouter les utilisateurs à la plateforme de BI. Lorsque vous remappez le rôle, l'option de mappage des

utilisateurs en tant qu'utilisateurs nommés ou simultanés affecte uniquement les nouveaux utilisateurs que vous avez ajoutés au rôle.

Par exemple, vous mappez d'abord un rôle à la plateforme de BI en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *nommés*". Ensuite, vous ajoutez des utilisateurs au même rôle et remappez le rôle en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *simultanés*".

Dans ce cas, seuls les nouveaux utilisateurs dans le rôle sont mappés à la plateforme de BI en tant qu'utilisateurs simultanés ; les utilisateurs qui étaient déjà mappés demeurent des utilisateurs nommés. La même condition s'applique si vous mappez d'abord les utilisateurs en tant qu'utilisateurs simultanés et que vous modifiez ensuite les paramètres pour remapper les nouveaux utilisateurs en tant qu'utilisateurs nommés.

9.7.3.3 Pour démapper un rôle

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone *Gérer*, cliquez sur *Authentification*.
3. Cliquez sur l'onglet correspondant à *JD Edwards EnterpriseOne*.
4. Dans la zone *Rôles*, sélectionnez le rôle que vous souhaitez supprimer, puis cliquez sur <.
5. Cliquez sur *Mettre à jour*.

   Les membres de ce rôle ne pourront plus accéder à la plateforme de BI, à moins de posséder d'autres comptes ou alias.

   > **Remarque**
   >
   > Vous pouvez également supprimer des comptes individuels ou retirer des utilisateurs des rôles avant de les mapper à la plateforme de BI afin d'empêcher certains utilisateurs de se connecter.

9.7.4 Planification de mises à jour utilisateur

Pour vous assurer que les modifications des données utilisateur de votre système ERP sont correctement reflétées dans les données utilisateur de votre plateforme de BI, vous pouvez planifier des mises à jour d'utilisateurs régulières. Ces mises à jour synchronisent automatiquement les utilisateurs d'ERP et de la plateforme de BI selon les paramètres de mappage configurés dans la CMC (Central Management Console).

Il existe deux options pour l'exécution et la planification des mises à jour de rôles importés :

- Mettre à jour les rôles uniquement : cette option permet de mettre à jour uniquement les liens entre les rôles actuellement mappés qui ont été importés dans la plateforme de BI. Utilisez cette option si vous avez l'intention d'exécuter des mises à jour fréquentes et que vous êtes préoccupé par l'utilisation des ressources système. Aucun nouveau compte utilisateur ne sera créé si vous effectuez uniquement une mise à jour des rôles.
- Mettre à jour les rôles et les alias : cette option permet non seulement de mettre à jour les liens entre les rôles, mais aussi de créer des comptes utilisateur dans la plateforme de BI pour les nouveaux alias utilisateur ajoutés au système ERP.

> **Remarque**
>
> Si vous n'avez pas spécifié de créer automatiquement des alias utilisateur pour les mises à jour lors de l'activation de l'authentification, aucun compte ne sera créé pour les nouveaux alias.

9.7.4.1 Pour planifier des mises à jour utilisateur

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer comment le système doit les mettre à jour.

1. Cliquez sur l'onglet *Mise à jour de l'utilisateur*.
2. Cliquez sur *Planifier* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

   > **→ Conseil**
   >
   > Pour exécuter une mise à jour immédiate, cliquez sur *Mettre à jour maintenant*.

   > **→ Conseil**
   >
   > Utilisez l'option *Mettre à jour les rôles uniquement* si vous souhaitez effectuer des mises à jour fréquentes et que vous êtes préoccupé par les ressources système. Le système met plus de temps à mettre à jour à la fois les rôles et les alias.

   La boîte de dialogue *Périodicité* s'affiche.
3. Sélectionnez une option dans la liste *Exécuter l'objet* et indiquez toutes les informations de planification demandées.

   Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous pouvez spécifier l'heure à laquelle l'exécution démarrera, de même que sa date de début et sa date de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les N jours. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Toutes les semaines	La mise à jour s'exécutera toutes les semaines. Elle peut être exécutée une ou plusieurs fois par semaine. Vous pouvez préciser les jours et l'heure auxquels l'exécution doit avoir lieu, ainsi qu'une date de début et une date de fin.
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.

Schéma de périodicité	Description
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

4. Cliquez sur *Planifier* une fois les informations de planification fournies.
   La date de la prochaine mise à jour de rôles planifiée est affichée dans l'onglet *Mise à jour de l'utilisateur*.

> ⓘ Remarque
>
> Vous pouvez annuler à tout moment la prochaine mise à jour planifiée en cliquant sur *Annuler les mises à jour planifiées* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

9.8 Authentification Siebel

9.8.1 Activation de l'authentification Siebel

Pour que les informations de Siebel puissent être utilisées par la plateforme de BI, des informations sont nécessaires sur le mode d'authentification dans votre système Siebel.

9.8.1.1 Pour activer l'authentification Siebel dans la plateforme de BI

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez deux fois sur *Siebel*.
   La page *Siebel* s'affiche. Elle contient quatre onglets : *Options*, *Systèmes*, *Responsabilités* et *Mise à jour de l'utilisateur*.
4. Dans l'onglet *Options*, sélectionnez la case à cocher *Activer l'authentification Siebel*.
5. Effectuez les modifications appropriées dans les champs *Nouvel alias*, *Options de mise à jour* et *Options de nouvel utilisateur* en fonction de votre déploiement de plateforme de BI. Cliquez sur *Mettre à jour* pour enregistrer vos modifications avant de passer à l'onglet *Systèmes*.

6. Cliquez sur l'onglet *Domaines*.
7. Dans le champ *Nom de domaine*, saisissez le nom de domaine du système Siebel auquel vous souhaitez vous connecter.
8. Sous *Connexion*, saisissez la chaîne de connexion de ce domaine.
9. Dans la zone *Nom d'utilisateur*, saisissez un nom d'utilisateur et un mot de passe de base de données qui seront utilisés par la plateforme de BI pour se connecter à votre base de données Siebel.
10. Dans la zone *Mot de passe*, saisissez le mot de passe de l'utilisateur sélectionné.
11. Cliquez sur *Ajouter* pour ajouter les informations système à la liste *Domaines actuels*.
12. Cliquez sur *Mettre à jour* pour enregistrer les modifications.

9.8.2 Mappage de rôles à la plateforme de BI

La plateforme de BI crée automatiquement un groupe pour chaque rôle Siebel que vous mappez. De même, le programme crée des alias pour représenter les membres des rôles Siebel mappés.

Vous pouvez créer un compte utilisateur pour chaque alias créé.

Cependant, si vous exécutez plusieurs systèmes et que vos utilisateurs possèdent des comptes sur plusieurs systèmes, vous pouvez affecter chaque utilisateur à un alias avec le même nom avant de créer les comptes sur la plateforme de BI.

Cela permet de réduire le nombre de comptes créés pour un même utilisateur dans le programme.

Par exemple, si vous exécutez à la fois un environnement de test et un environnement de production Siebel eBusiness et que 30 de vos utilisateurs ont accès aux deux systèmes, 30 comptes seulement sont créés pour ces utilisateurs. Si vous choisissez de ne pas affecter chaque utilisateur à un alias avec le même nom, 60 comptes sont créés pour les 30 utilisateurs sur la plateforme de BI.

Cependant, si vous exécutez plusieurs systèmes et que les noms d'utilisateurs identiques créent des conflits, vous devez créer un compte de membre pour chaque alias créé.

Par exemple, si vous exécutez votre environnement de test avec un compte utilisateur pour Russell Aquino (nom d'utilisateur "raquino") et que vous exécutez votre environnement de production avec un compte utilisateur pour Raoul Aquino (nom d'utilisateur "raquino"), vous devez créer un compte distinct pour l'alias de chaque utilisateur. Sinon, les deux utilisateurs seront ajoutés au même compte et ne pourront pas se connecter à la plateforme de BI avec leurs propres références de connexion Siebel eBusiness.

9.8.2.1 Pour mapper un rôle Siebel eBusiness à la plateforme de BI

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Cliquez sur *Authentification*.
3. Cliquez deux fois sur *Siebel*.
4. Cochez la case *Activer l'authentification Siebel*.
5. Dans la zone *Options de nouvel alias*, sélectionnez l'une des options suivantes :

- *Affecter chaque alias ajouté à un compte portant le même nom*
  Sélectionnez cette option si vous exécutez plusieurs systèmes Siebel eBusiness avec des utilisateurs possédant des comptes sur plusieurs systèmes (les utilisateurs ne possèdent pas de nom identique sur les différents systèmes).
- *Créer un compte pour chaque alias ajouté*
  Sélectionnez cette option si vous exécutez un seul système Siebel eBusiness, si la plupart de vos utilisateurs possèdent des comptes sur un seul de vos systèmes ou si les noms d'utilisateur sont identiques pour différents utilisateurs sur au moins deux de vos systèmes.

6. Dans la zone *Options de mise à jour des alias*, sélectionnez l'une des options suivantes :
   - *Créer de nouveaux alias lors de la mise à jour des alias*
     Sélectionnez cette option pour créer un alias pour chaque utilisateur mappé à la plateforme de BI. De nouveaux comptes sont ajoutés pour les utilisateurs dépourvus de compte plateforme de BI ou pour tous les utilisateurs si vous avez sélectionné l'option Créer un nouveau compte pour chaque alias ajouté.
   - *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
     Sélectionnez cette option si le rôle que vous souhaitez mapper contient plusieurs utilisateurs dont un petit nombre utilisera la plateforme de BI. Le programme ne crée pas automatiquement d'alias et de comptes pour les utilisateurs. À la place, elle crée des alias (et des comptes, au besoin) uniquement pour les utilisateurs lorsqu'ils se connectent pour la première fois à la plateforme de BI. Il s'agit de l'option par défaut.
7. Dans la zone *Options de nouvel utilisateur*, indiquez le nombre d'utilisateurs créés.

   Si votre licence de plateforme de BI est basée sur les rôles utilisateur, sélectionnez l'une des options suivantes :

   Sélectionnez l'une des options suivantes :

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
     Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

     > **Remarque**
     >
     > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
     >
     > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
     Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs à la plateforme de BI, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

8. Cliquez sur l'onglet *Rôles*.
9. Sélectionnez le domaine correspondant au serveur Siebel pour lequel vous souhaitez mapper des rôles.
10. Sous *Rôles disponibles*, sélectionnez les rôles que vous souhaitez mapper, puis cliquez sur >.

> **Remarque**
>
> Vous pouvez utiliser le champ *Rechercher les rôles commençant par :* pour affiner votre recherche si vous disposez d'un grand nombre de rôles. Saisissez les premiers caractères des rôles en les faisant suivre du caractère générique (%) et cliquez sur *Rechercher*.

> **Remarque**
>
> Pour que la fonction de recherche fonctionne, un fichier jar de plug-in Siebel doit être déployé dans le répertoire lib de Tomcat : `<REPINSTALL>\tomcat\webapps\BOE\WEB-INF\lib` et dans `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. Redémarrez ensuite le serveur Tomcat et le Server Intelligence Agent.

11. Cliquez sur *Mettre à jour*.
    Les rôles seront mappés à la plateforme de BI.

9.8.2.2 Remarques sur le remappage

Pour appliquer la synchronisation des groupes et des utilisateurs entre la plateforme de BI et Siebel, activez la case *Forcer la synchronisation utilisateur*.

> **Remarque**
>
> Pour pouvoir sélectionner *Forcer la synchronisation utilisateur*, il faut d'abord sélectionner *Les nouveaux alias seront ajoutés et les nouveaux utilisateurs seront créés*.

Lorsque vous remappez le rôle, l'option de mappage des utilisateurs en tant qu'utilisateurs nommés ou simultanés affecte uniquement les nouveaux utilisateurs que vous avez ajoutés au rôle.

Par exemple, vous mappez d'abord un rôle à la plateforme de BI en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *nommés*". Ensuite, vous ajoutez des utilisateurs au même rôle et remappez le rôle en sélectionnant l'option "Les nouveaux utilisateurs sont créés en tant qu'utilisateurs *simultanés*".

Dans ce cas, seuls les nouveaux utilisateurs dans le rôle sont mappés à la plateforme de BI en tant qu'utilisateurs simultanés ; les utilisateurs qui étaient déjà mappés demeurent des utilisateurs nommés. La même condition s'applique si vous mappez d'abord les utilisateurs en tant qu'utilisateurs simultanés et que vous modifiez ensuite les paramètres pour remapper les nouveaux utilisateurs en tant qu'utilisateurs nommés.

9.8.2.3 Pour démapper un rôle

1. Connectez-vous en tant qu'administrateur à la Central Management Console.

2. Dans la zone *Gérer*, cliquez sur *Authentification*.
3. Cliquez deux fois sur *Siebel*.
4. Dans l'onglet *Domaines*, sélectionnez le domaine Siebel correspondant aux rôles que vous souhaitez démapper.
5. Dans l'onglet *Rôles*, sélectionnez le rôle que vous souhaitez supprimer, puis cliquez sur <.
6. Cliquez sur *Mettre à jour*.

   Les membres de cette responsabilité ne pourront plus accéder à la plateforme de BI, à moins de posséder d'autres comptes ou alias.

   > ⓘ Remarque
   >
   > Vous pouvez également supprimer des comptes individuels ou retirer des utilisateurs des rôles avant de les mapper à la plateforme de BI afin d'empêcher certains utilisateurs de se connecter.

9.8.3 Planification de mises à jour utilisateur

Pour vous assurer que les modifications des données utilisateur de votre système ERP sont correctement reflétées dans les données utilisateur de votre plateforme de BI, vous pouvez planifier des mises à jour d'utilisateurs régulières. Ces mises à jour synchronisent automatiquement les utilisateurs d'ERP et de la plateforme de BI selon les paramètres de mappage configurés dans la CMC (Central Management Console).

Il existe deux options pour l'exécution et la planification des mises à jour de rôles importés :

- Mettre à jour les rôles uniquement : cette option permet de mettre à jour uniquement les liens entre les rôles actuellement mappés qui ont été importés dans la plateforme de BI. Utilisez cette option si vous avez l'intention d'exécuter des mises à jour fréquentes et que vous êtes préoccupé par l'utilisation des ressources système. Aucun nouveau compte utilisateur ne sera créé si vous effectuez uniquement une mise à jour des rôles.
- Mettre à jour les rôles et les alias : cette option permet non seulement de mettre à jour les liens entre les rôles, mais aussi de créer des comptes utilisateur dans la plateforme de BI pour les nouveaux alias utilisateur ajoutés au système ERP.

> ⓘ Remarque
>
> Si vous n'avez pas spécifié de créer automatiquement des alias utilisateur pour les mises à jour lors de l'activation de l'authentification, aucun compte ne sera créé pour les nouveaux alias.

9.8.3.1 Pour planifier des mises à jour utilisateur

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer comment le système doit les mettre à jour.

1. Cliquez sur l'onglet *Mise à jour de l'utilisateur*.
2. Cliquez sur *Planifier* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

> → Conseil
>
> Pour exécuter une mise à jour immédiate, cliquez sur *Mettre à jour maintenant*.

> → Conseil
>
> Utilisez l'option *Mettre à jour les rôles uniquement* si vous souhaitez effectuer des mises à jour fréquentes et que vous êtes préoccupé par les ressources système. Le système met plus de temps à mettre à jour à la fois les rôles et les alias.

La boîte de dialogue *Périodicité* s'affiche.

3. Sélectionnez une option dans la liste *Exécuter l'objet* et indiquez toutes les informations de planification demandées.

   Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous pouvez spécifier l'heure à laquelle l'exécution démarrera, de même que sa date de début et sa date de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les N jours. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Toutes les semaines	La mise à jour s'exécutera toutes les semaines. Elle peut être exécutée une ou plusieurs fois par semaine. Vous pouvez préciser les jours et l'heure auxquels l'exécution doit avoir lieu, ainsi qu'une date de début et une date de fin.
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

4. Cliquez sur *Planifier* une fois les informations de planification fournies.
   La date de la prochaine mise à jour de rôles planifiée est affichée dans l'onglet *Mise à jour de l'utilisateur*.

> **Remarque**
>
> Vous pouvez annuler à tout moment la prochaine mise à jour planifiée en cliquant sur *Annuler les mises à jour planifiées* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

9.9 Authentification Oracle EBS

9.9.1 Activation de l'authentification Oracle EBS

Pour que les informations d'Oracle EBS puissent être utilisées par la plateforme de BI, le système a besoin d'informations sur le mode d'authentification dans votre système Oracle EBS.

9.9.1.1 Activation de l'authentification Oracle E-Business Suite

Avant d'appliquer la procédure, la DLL Oracle et les fichiers JAR doivent être déployés sur la plateforme de BI :

1. Téléchargez `ojdbc11.dll` depuis l'application client de la base de données Oracle.
2. Copiez le fichier à cet emplacement :
   - Sous Windows : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
   - Sous UNIX : `<REPINSTALL>/sap_bobj/enterprise_xi40/platform`
3. Téléchargez `ojdbc5.jar` depuis l'application client de la base de données Oracle.
4. Copiez le fichier à cet emplacement :
   - Sous Windows : `<REPINSTALL>\Tomcat\lib`
   - Sous UNIX : `<REPINSTALL>/sap_bobj/tomcat/lib`

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez sur *Oracle EBS*.
   La page *Oracle EBS* s'affiche. Elle contient quatre onglets : *Options*, *Systèmes*, *Responsabilités* et *Mise à jour de l'utilisateur*.
4. Dans l'onglet *Options*, activez la case *L'authentification Oracle EBS est activée*.
5. Effectuez les modifications appropriées dans les champs *Nouvel alias*, *Options de mise à jour* et *Options de nouvel utilisateur* en fonction de votre déploiement de plateforme de BI. Cliquez sur *Mettre à jour* pour enregistrer vos modifications avant de passer à l'onglet *Systèmes*.
6. Cliquez sur l'onglet *Systèmes*.
7. Dans la zone *Utilisateur système Oracle EBS*, saisissez un nom d'utilisateur et un mot de passe de base de données qui seront utilisés par la plateforme de BI pour se connecter à votre base de données Oracle E-Business Suite.
8. Dans la zone *Services Oracle EBS*, saisissez le nom du service utilisé par votre environnement Oracle EBS et cliquez sur *Ajouter*.

9. Cliquez sur *Mettre à jour* pour enregistrer les modifications.

Vous devez maintenant mapper les rôles Oracle EBS dans le système.

Informations associées

Pour mapper les rôles Oracle E-Business Suite [page 401]

9.9.2 Mappage de rôles Oracle E-Business Suite à la plateforme de BI

La plateforme de BI crée automatiquement un groupe pour chaque rôle Oracle E-Business Suite (EBS) que vous mappez. Le système crée également des alias pour représenter les membres des rôles Oracle E-Business Suite mappés.

Vous pouvez créer un compte utilisateur pour chaque alias créé. Cependant, si vous exécutez plusieurs systèmes et que vos utilisateurs possèdent des comptes sur plusieurs systèmes, vous pouvez affecter chaque utilisateur à un alias avec le même nom avant de créer les comptes sur la plateforme de BI.

Cela permet de réduire le nombre de comptes créés pour un même utilisateur dans le système.

Par exemple, si vous exécutez à la fois un environnement de test et un environnement de production EBS, et si 30 de vos utilisateurs ont accès aux deux systèmes, 30 comptes seulement sont créés pour ces utilisateurs. Si vous choisissez de ne pas affecter chaque utilisateur à un alias avec le même nom, 60 comptes sont créés pour les 30 utilisateurs sur la plateforme de BI.

Cependant, si vous exécutez plusieurs systèmes et que les noms d'utilisateurs identiques créent des conflits, vous devez créer un compte de membre pour chaque alias créé.

Par exemple, si vous exécutez votre environnement de test avec un compte utilisateur pour Russell Aquino (nom d'utilisateur "raquino") et que vous exécutez votre environnement de production avec un compte utilisateur pour Raoul Aquino (nom d'utilisateur "raquino"), vous devez créer un compte distinct pour l'alias de chaque utilisateur. Autrement, les deux utilisateurs sont ajoutés au même compte de la plateforme de BI. Ils pourront se connecter au système avec leurs propres références Oracle EBS et auront accès aux données des deux environnements EBS.

9.9.2.1 Pour mapper les rôles Oracle E-Business Suite

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez sur *Oracle EBS*.
   La page *Oracle EBS* présentant l'onglet *Options* s'affiche.
4. Dans la zone *Options de nouvel alias*, sélectionnez l'une des options suivantes :
   - *Affectez chaque alias Oracle EBS ajouté à un compte portant le même nom*

Sélectionnez cette option si vous exécutez plusieurs systèmes Oracle E-Business Suite avec des utilisateurs possédant des comptes sur plusieurs systèmes (et si deux utilisateurs ne possèdent pas des noms identiques sur les différents systèmes).

- *Créer un nouveau compte pour chaque alias Oracle EBS ajouté*
  Sélectionnez cette option si vous exécutez un seul système Oracle E-Business Suite, si la majorité de vos utilisateurs possèdent des comptes sur un seul de vos systèmes ou si des noms d'utilisateurs identiques créent des conflits sur deux de vos systèmes ou plus.

5. Dans la zone *Options de mise à jour*, sélectionnez l'une des options suivantes :
   - *Créer de nouveaux alias lors de la mise à jour des alias*
     Sélectionnez cette option pour créer un alias pour chaque utilisateur mappé à la plateforme de BI. De nouveaux comptes sont ajoutés pour les utilisateurs dépourvus de comptes pour la plateforme de BI ou pour tous les utilisateurs si vous avez sélectionné l'option *Créer un nouveau compte pour chaque alias Oracle EBS ajouté*.
   - *Créer de nouveaux alias uniquement lorsque l'utilisateur se connecte*
     Sélectionnez cette option si le rôle que vous souhaitez mapper contient plusieurs utilisateurs dont un petit nombre utilisera la plateforme de BI. La plateforme ne crée pas automatiquement d'alias ni de comptes pour les utilisateurs. À la place, elle crée des alias (et des comptes, au besoin) uniquement pour les utilisateurs lorsqu'ils se connectent pour la première fois à la plateforme de BI. Il s'agit de l'option par défaut.
6. Dans *Options de nouvel utilisateur*, indiquez le nombre d'utilisateurs créés, puis cliquez sur *Mettre à jour*.

   Sélectionnez l'une des options suivantes :

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs nommés*
     Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences Utilisateurs nommés. Les licences Utilisateur nommé sont associées à des utilisateurs particuliers qui peuvent accéder au système en saisissant un nom d'utilisateur et un mot de passe. Ainsi, les utilisateurs nommés peuvent accéder au système, quel que soit le nombre de personnes connectées. Il faut qu'une licence Utilisateurs nommés soit disponible pour chaque compte d'utilisateur créé à l'aide de cette option.

     > **Remarque**
     >
     > Le nombre de sessions ouvertes simultanément est limité à 10 pour un utilisateur nommé créé à l'aide d'une licence Utilisateur nommé. Si un tel utilisateur nommé essaie de se connecter à une 11ème session simultanée, le système affiche un message d'erreur correspondant. Vous devez libérer une des sessions existantes pour pouvoir vous connecter.
     >
     > Cependant, le nombre de sessions ouvertes simultanément n'est pas limité pour un utilisateur créé à l'aide d'une licence Processeur et d'une licence Document public.

   - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*
     Les nouveaux comptes utilisateur sont configurés de manière à utiliser des licences d'utilisateurs simultanés. Les licences d'accès simultanés spécifient le nombre d'utilisateurs pouvant se connecter en même temps à la plateforme de BI. Cette licence est tout à fait adaptée dans la mesure où elle peut accepter de nombreux utilisateurs. Par exemple, suivant la fréquence et la durée des connexions des utilisateurs à la plateforme, une licence pour 100 utilisateurs simultanés peut prendre en charge 250, 500 ou 700 utilisateurs.

   Les rôles que vous avez sélectionnés apparaissent maintenant sous forme de groupes sur la plateforme de BI.

7. Cliquez sur l'onglet *Responsabilités*.
8. Dans la zone *Services Oracle EBS actuels*, sélectionnez le serveur Oracle EBS qui contient les rôles à mapper.
9. Vous pouvez spécifier les filtres pour les utilisateurs Oracle EBS dans la zone *Rôles Oracle EBS mappés*.
   a. Sélectionnez les applications que les utilisateurs peuvent utiliser dans le cadre de leur nouveau rôle dans la liste *Application*.
   b. Sélectionnez les applications Oracle, les fonctions, les rapports ainsi que les programmes simultanés que les utilisateurs peuvent utiliser dans la liste *Responsabilité*.
   c. Sélectionnez le groupe de sécurité auquel le nouveau rôle est affecté dans le groupe Sécurité de la liste *Groupe de sécurité*.
   d. À l'aide des boutons *Ajouter* et *Supprimer* figurant sous *Rôle actuel*, vous pouvez modifier les affectations du groupe de sécurité associées au rôle.
10. Cliquez sur *Mettre à jour*.
    Les rôles seront mappés à la plateforme de BI.

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer comment le système doit les mettre à jour.

9.9.2.1.1 Mise à jour des rôles et des utilisateurs Oracle EBS

Une fois l'authentification Oracle EBS activée, il est nécessaire de planifier et d'exécuter des mises à jour régulières sur les rôles mappés qui ont été importés dans la plateforme de BI. Cela garantira que les informations des rôles Oracle EBS mis à jour sont reflétées avec précision dans la plateforme de BI.

Il existe deux options pour l'exécution et la planification des mises à jour de rôles Oracle EBS :

- Mettre à jour les rôles uniquement : cette option permet uniquement de mettre à jour les liens entre les rôles actuellement mappés qui ont été importés dans la plateforme de BI. Nous vous recommandons d'utiliser cette option si vous avez l'intention d'exécuter des mises à jour fréquentes et que vous êtes préoccupé par l'utilisation des ressources système. Aucun nouveau compte utilisateur ne sera créé si vous effectuez uniquement une mise à jour des rôles Oracle EBS.
- Mettre à jour les rôles et les alias : Cette option permet non seulement de mettre à jour les liens entre les rôles, mais aussi de créer des comptes utilisateur dans la plateforme de BI pour les alias utilisateur ajoutés à des rôles dans le système Oracle EBS.

> **ⓘ Remarque**
>
> Si vous n'avez pas spécifié de créer automatiquement des alias utilisateur pour les mises à jour lors de l'activation de l'authentification Oracle EBS, aucun compte ne sera créé pour les nouveaux alias.

9.9.2.1.2 Planification de mises à jour pour les rôles Oracle EBS

Après avoir mappé les rôles dans la plateforme de BI, vous devez indiquer comment le système doit les mettre à jour.

1. Cliquez sur l'onglet *Mise à jour de l'utilisateur*.
2. Cliquez sur *Planifier* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

   > → Conseil
   >
   > Pour une exécution et une mise à jour immédiates, cliquez sur *Mettre à jour maintenant*.

   > → Conseil
   >
   > Utilisez l'option *Mettre à jour les rôles uniquement* si vous souhaitez effectuer des mises à jour fréquentes et que vous êtes préoccupé par les ressources système. Le système met plus de temps à mettre à jour à la fois les rôles et les alias.

   La boîte de dialogue *Périodicité* s'affiche.
3. Sélectionnez une option dans la liste déroulante *Exécuter l'objet* et indiquez toutes les informations de planification demandées dans les champs correspondants.

   Lorsque vous planifiez une mise à jour, vous pouvez choisir une des périodicités récapitulées dans le tableau suivant :

Schéma de périodicité	Description
Toutes les heures	La mise à jour s'exécutera toutes les heures. Vous pouvez spécifier l'heure à laquelle l'exécution démarrera, de même que sa date de début et sa date de fin.
Tous les jours	La mise à jour s'exécutera tous les jours ou tous les N jours. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Toutes les semaines	La mise à jour s'exécutera toutes les semaines. Elle peut s'exécuter une ou plusieurs fois par semaine. Vous pouvez préciser les jours et l'heure auxquels l'exécution doit avoir lieu, ainsi qu'une date de début et une date de fin.
Tous les mois	La mise à jour s'exécutera tous les mois ou tous les N mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Nième jour du mois	La mise à jour sera exécutée un jour spécifique du mois. Vous pouvez préciser le jour du mois et l'heure auxquels l'exécution aura lieu, ainsi que sa date de début et sa date de fin.
1er lundi du mois	La mise à jour sera exécutée le premier lundi de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.

Schéma de périodicité	Description
Dernier jour du mois	La mise à jour sera exécutée le dernier jour de chaque mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Jour X de la Nième semaine du mois	La mise à jour sera exécutée le jour indiqué de la semaine indiquée du mois. Vous pouvez préciser l'heure à laquelle l'exécution aura lieu, de même que sa date de début et sa date de fin.
Calendrier	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

4. Cliquez sur *Planifier* une fois les informations de planification fournies.
   La date de la prochaine mise à jour de rôles planifiée est affichée dans l'onglet *Mise à jour de l'utilisateur*.

   > **Remarque**
   >
   > Vous pouvez annuler à tout moment la prochaine mise à jour planifiée en cliquant sur *Annuler les mises à jour planifiées* dans les sections *Mettre à jour les rôles uniquement* ou *Mettre à jour les rôles et les alias*.

9.9.3 Démappage de rôles

Afin d'empêcher certains groupes d'utilisateurs de se connecter à la plateforme de BI, vous pouvez démapper les rôles auxquels ils appartiennent.

9.9.3.1 Pour démapper un rôle

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone Gérer, cliquez sur *Authentification*.
3. Cliquez deux fois sur le nom du système ERP pour lequel vous souhaitez démapper des rôles.
   La page du système ERP affiche l'onglet *Options*.
4. Cliquez sur l'onglet *Responsabilités*.
5. Sélectionnez les *Services Oracle EBS actuel*.
6. Sous *Rôle actuel*, sélectionnez un rôle, puis cliquez sur le bouton *Supprimer*.
7. Cliquez sur *Mettre à jour*.

   Les membres de ce rôle ne pourront plus accéder à la plateforme de BI, à moins de posséder d'autres comptes ou alias.

   > **Remarque**
   >
   > Vous pouvez également supprimer des comptes individuels ou retirer des utilisateurs des rôles avant de les mapper à la plateforme de BI afin d'empêcher certains utilisateurs de se connecter.

9.9.4 Personnalisation des droits pour les groupes et utilisateurs Oracle EBS mappés

Lorsque vous mappez des rôles à la plateforme de BI, vous pouvez définir des droits ou accorder des autorisations aux groupes et utilisateurs créés.

9.9.4.1 Pour affecter des droits d'administration

Pour autoriser les utilisateurs à gérer la plateforme de BI, vous devez les désigner comme membres du groupe Administrateurs par défaut. Les membres de ce groupe reçoivent un contrôle total sur tous les aspects du système, y compris les comptes, les serveurs, les dossiers, les objets, les paramètres, etc.

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone *Organiser*, cliquez sur *Utilisateurs et groupes*.
3. Dans la colonne *Nom*, cliquez avec le bouton droit sur *Administrateurs*, puis cliquez sur *Ajouter des membres au groupe*.

   La page *Utilisateurs ou groupes disponibles* s'affiche.
4. Dans la zone *Liste des utilisateurs* ou *Liste des groupes*, sélectionnez le rôle mappé auquel vous voulez affecter les droits d'administration.
5. Cliquez sur > pour faire du rôle un sous-groupe du groupe Administrateurs, puis cliquez sur *OK*.

Les membres de ce rôle possèdent désormais les droits d'administration sur la plateforme de BI.

> **Remarque**
>
> Vous pouvez également créer un rôle dans Oracle EBS, ajouter les utilisateurs appropriés au rôle, mapper le rôle à la plateforme de BI et faire du rôle mappé un sous-groupe du groupe Administrateurs par défaut pour accorder aux membres du rôle des droits d'administration.

9.9.4.2 Pour affecter des droits de publication

Si votre système inclut des utilisateurs désignés comme créateurs de contenu dans votre organisation, vous pouvez leur accorder des autorisations pour publier des objets sur la plateforme de BI.

1. Connectez-vous en tant qu'administrateur à la Central Management Console.
2. Dans la zone *Organiser*, cliquez sur *Dossiers*.
3. Accédez au dossier dans lequel vous souhaitez autoriser les utilisateurs à ajouter des objets.
4. Cliquez sur *Gérer*, *Sécurité de niveau supérieur*, puis sur *Tous les dossiers*.
5. Cliquez sur *Ajouter des utilisateurs/groupes principaux*.

   La page Ajouter des utilisateurs/groupes principaux s'affiche.
6. Dans la liste *Utilisateurs ou groupes disponibles*, sélectionnez le groupe comprenant les membres auxquels vous souhaitez accorder des droits de publication.

7. Cliquez sur > pour permettre au groupe d'accéder au dossier, puis cliquez sur *Ajouter et affecter la sécurité*.

   La page Affecter la sécurité s'affiche.
8. Dans la liste *Niveaux d'accès disponibles*, sélectionnez le niveau d'accès voulu et cliquez sur > pour affecter explicitement ce niveau d'accès.
9. Si les options *Hériter du dossier parent* et *Hériter du groupe parent* sont activées, désélectionnez-les, puis cliquez sur *Appliquer*.
10. Cliquez sur *OK*.

Les membres du rôle ont maintenant l'autorisation d'ajouter des objets dans le dossier et tous ses sous-dossiers. Pour supprimer les autorisations attribuées, sélectionnez un groupe, puis cliquez sur *Supprimer*.

9.9.5 Configuration de la connexion unique pour SAP Crystal Reports et Oracle EBS

Par défaut, la plateforme de BI est configurée pour permettre aux utilisateurs de SAP Crystal Reports d'accéder aux données Oracle EBS à l'aide de la connexion unique.

9.9.5.1 Pour désactiver la connexion unique pour Oracle EBS et SAP Crystal Reports

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sélectionnez *crdb_oraapps*.
5. Cliquez sur *Supprimer*.
6. Cliquez sur *Enregistrer et fermer*.
7. Accédez à la page *Serveurs* de la CMC et sélectionnez *Services Crystal Reports*.
8. Cliquez sur le bouton *Redémarrer le serveur*.

9.9.5.2 Pour réactiver la connexion unique pour Oracle EBS et SAP Crystal Reports

Pour réactiver la connexion unique pour Oracle EBS et SAP Crystal Reports, procédez comme suit.

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sous *Utiliser le contexte de connexion unique pour se connecter à la base de données avec les pilotes suivants*, saisissez **`crdb_oraapps`**.

5. Cliquez sur *Ajouter*.
6. Cliquez sur *Enregistrer et fermer*.
7. Accédez à la page *Serveurs* de la CMC et sélectionnez *Services Crystal Reports*.
8. Cliquez sur le bouton *Redémarrer le serveur*.

9.10 Authentification X.509

9.10.1 Authentification X.509 pour la zone de lancement BI

9.10.1.1 Création et configuration des certificats et des fichiers de stockage de clés

> **Remarque**
>
> Un utilisateur doit exister dans la plateforme de BI pour obtenir la connexion unique via l'authentification X.509.

> **Remarque**
>
> Téléchargez et installez le Toolkit OpenSSL pour réaliser les étapes ci-dessous.

> **Remarque**
>
> Suivez toutes les étapes ci-dessous si vous devez créer un certificat CA et l'auto-signer.

> **Remarque**
>
> Si vous avez un certificat CA approuvé, voir Autorité de certification approuvée [page 410] pour la création et la configuration des certificats et des fichiers de stockage de clés.

1. Exécutez la commande pour créer deux fichiers : la clé de l'autorité de certification (ca.key) et la demande de certificat (ca.csr). `Openssl.exe req –newkey rsa:2048 –nodes –out c:\ssl\ca.csr –keyout c:\ssl\ca.key`
2. Exécutez la commande pour créer un certificat signé : ca.pem. `Openssl.exe x509 –req –trustout –signkey c:\ssl\ca.key –days 365 –in c:\ssl\ca.csr –out c:\ssl\ca.pem`
3. Créez la paire de clés de serveur, le certificat et le fichier de stockage de clés.
   a. Créez un fichier pour maintenir les numéros de série de l'autorité de certification en exécutant le code : `Echo 02 >c:\ssl\ca.srl`
   b. Accédez à `C:\Program Files\Java\jre7\bin` et utilisez le fichier keytool.exe pour créer le fichier de stockage de clés, le certificat et la clé privée.

> **Remarque**
>
> À l'emplacement du fichier Java keytool.exe, "jre7" peut varier en fonction de la version de Java.

```
Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
c:\ssl\serverkeystore.jks -storetype JKS
Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
keystore c:\ssl\serverkeystore.jks
```

> **→ N'oubliez pas**
>
> Lors de la génération du certificat, saisissez le nom d'hôte de l'ordinateur du serveur lorsqu'on vous le demandera. Sinon, vous recevrez une erreur de certificat du côté client au moment de la connexion.

c. Saisissez le mot de passe du fichier de stockage de clés.

> **→ N'oubliez pas**
>
> Vous devez modifier le fichier de demande server.csr dans un éditeur de texte et modifier "Nouvelle demande de certificat de début" par "Demande de certificat de début" et "Nouvelle demande de certificat de fin" par "Demande de certificat de fin".

4. Exécutez la commande pour créer le certificat signé : server.crt. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
5. Importez l'autorité de certification et le certificat du serveur dans le fichier de stockage de clés du serveur.

```
Keytool.exe -import -alias ca -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\ca.pem
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\server.crt
```

6. Exécutez la commande pour créer les certificats client, client.req et client.key `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> **Remarque**
>
> Copiez le fichier sslc.cnf depuis `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` sur C:\SSL et modifiez les paramètres :
>
> Dir=c:/ssl # location for everything
>
> Certificate= $dir/ca.pem # CA certificate
>
> Private_key= $dir/ca.key # private key
>
> RANDFILE= $dir/.rand # private random number file

7. Exécutez la commande pour signer le certificat client. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`

8. Importez le CA et le certificat client dans le fichier de stockage de clés approuvé à l'aide de la commande ci-dessous. La commande crée le fichier trustkeystore.jks.

```
Keytool.exe –import –alias ca –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\ca.pem
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

9. Exportez le certificat client avec le format PKCS12 de la clé privée client. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. La commande crée le fichier client.p12.
10. Exécutez la commande pour exporter le certificat CA et créer ca.crt. `Openssl.exe x509 –in c:\ssl\ca.pem –inform PEM –out c:\ssl\ca.crt –outform DER`
11. Copiez les fichiers .p12 et ca.crt sur l'ordinateur du client pour installer le certificat client et le certificat CA.

> **Remarque**
>
> Pour installer des certificats dans Mozilla Firefox, ouvrez *Outils* > *Options* > *Avancé* et sélectionnez Afficher les certificats dans l'onglet Cryptage pour importer le fichier client.p12 sous l'onglet Vos certificats et le fichier ca.crt sous l'onglet Autorités.

9.10.1.1.1 Autorité de certification approuvée

1. Créez la paire de clés de serveur, le certificat et le fichier de stockage de clés.
   a. Créez un fichier pour enregistrer les numéros de série de l'autorité de certification en exécutant le code : `Echo 02 >c:\ssl\ca.srl`
   b. Accédez à `C:\Program Files\Java\jre7\bin` et utilisez le fichier keytool.exe pour créer le fichier de stockage de clés, le certificat et la clé privée.

   > **Remarque**
   >
   > À l'emplacement du fichier keytool.exe, "jre7" peut varier en fonction de la version de Java.

   ```
   Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore
   c:\ssl\serverkeystore.jks –storetype JKS
   Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –
   keystore c:\ssl\serverkeystore.jks
   ```

   > **→ N'oubliez pas**
   >
   > Lors de la génération du certificat, saisissez le nom d'hôte de l'ordinateur du serveur lorsqu'on vous le demandera. Sinon, vous recevrez une erreur de certificat du côté client au moment de la connexion.

   c. Saisissez le mot de passe du fichier de stockage de clés.

> → N'oubliez pas
>
> Vous devez modifier le fichier de demande server.csr dans un éditeur de texte et modifier "Nouvelle demande de certificat de début" par "Demande de certificat de début" et "Nouvelle demande de certificat de fin" par "Demande de certificat de fin".

2. Exécutez la commande pour créer le certificat signé : server.crt. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
3. Importez le certificat du serveur dans le fichier de stockage de clés du serveur.

```
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -trustcacerts -file c:\ssl\server.crt
```

4. Exécutez la commande pour créer des certificats client, client.req et client.key `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> ⓘ Remarque
>
> Copiez le fichier sslc.cnf depuis `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` sur C:\SSL et modifiez les paramètres :
>
> Dir=c:/ssl # emplacement pour tout
>
> Certificate= $dir/ca.pem # certificat CA
>
> Private_key= $dir/ca.key # clé privée
>
> RANDFILE= $dir/.rand # fichier numéro aléatoire privé

5. Exécutez la commande pour signer le certificat client. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`
6. Importez le certificat client dans le fichier de stockage de clés approuvé avec la commande données ci-dessous. La commande crée le fichier trustkeystore.jks.

```
Keytool.exe -import -alias client -keystore c:\ssl\trustkeystore.jks -trustcacerts -file c:\ssl\client.pem
```

7. Exportez le certificat client avec le format PKCS12 de la clé privée client. `Openssl.exe pkcs12 -export -clcerts -in c:\ssl\client.pem -inkey c:\ssl\client.key -out c:\ssl\client.p12 -name "client certificate"`. La commande crée le fichier client.p12.
8. Copiez le fichier .p12 dans l'ordinateur du client pour l'installer.

> ⓘ Remarque
>
> Pour installer des certificats dans Mozilla Firefox, ouvrez *Outils* > *Options* > *Avancé* et sélectionnez Afficher les certificats dans l'onglet Cryptage pour importer le fichier client.p12 sous l'onglet Vos certificats et le fichier ca.crt sous l'onglet Autorités.

9.10.1.2 Configuration du serveur SSL Tomcat

9.10.1.2.1 Configuration SSL unidirectionnelle

1. Accédez à `<INSTALLDIR>\tomcat\conf\server.xml`
2. Modifiez la balise xml : `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true">`
   `<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>`

   > **Remarque**
   >
   > Le mot de passe (MotDePasse1) et l'emplacement (C:\ssl\serverkeystore.jks) du fichier de stockage de clés utilisé dans la balise xml ci-dessus sont juste des exemples. Vous pouvez utiliser le mot de passe et l'emplacement de votre choix.

3. Enregistrez le fichier et redémarrez le serveur Tomcat.

9.10.1.2.2 Configuration SSL bidirectionnelle

Configurez le serveur Tomcat pour demander l'authentification du client en suivant les étapes ci-dessous.

1. Accédez à `<INSTALLDIR>\tomcat\conf\server.xml`
2. Modifiez le serveur xml avec la balise xml donnée ci-dessous :
   `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true">`
   `<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>`

   > **Remarque**
   >
   > Le mot de passe (MotDePasse1) et l'emplacement (C:\ssl\serverkeystore.jks ou C:\ssl\trustkeystore.jks) du fichier de stockage de clés utilisé dans la balise xml ci-dessus sont juste des exemples. Vous pouvez utiliser le mot de passe et l'emplacement de votre choix.

3. Enregistrez le fichier et redémarrez le serveur Tomcat.

   > **Remarque**
   >
   > Dans Internet Explorer, désactivez l'option "Ne pas demander la sélection du certificat client si aucun certificat ou seulement un certificat existe" en accédant à *Options Internet* > *Sécurité* > *Internet local* > *Niveau personnalisé* > *Divers*

9.10.1.3 Configuration de la zone de lancement BI

9.10.1.3.1 Création d'une clé de secret partagé

La clé de secret partagé est utilisée pour établir la sécurité entre le client et le CMS. Vous devez configurer le serveur avant le client pour l'authentification sécurisée.

1. Connectez-vous à la CMC.
2. Accédez à Authentification et sélectionnez Entreprise.
3. Activez l'authentification sécurisée.
4. Cliquez sur Nouveau secret partagé.

   > **Remarque**
   >
   > La clé du secret partagé est générée et le message de téléchargement s'affiche.

5. Cliquez sur Télécharger le secret partagé.
6. Cliquez sur Enregistrer dans la boîte de dialogue de téléchargement puis cliquez sur l'un des répertoires suivants :
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

9.10.1.3.2 Transmission de la clé de secret partagé via le fichier TrustedPrincipal.conf

1. Créez un fichier texte sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory`.
2. Dans le nouveau fichier, ajoutez le texte donné ci-dessous.

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. Enregistrez le fichier et nommez-le "global.properties".

9.10.1.3.3 Modification du fichier custom.jsp

> **Remarque**
>
> Créez un utilisateur avec un nom d'ordinateur dans la CMC avant de modifier le fichier custom.jsp.

1. Accédez à

a. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* dans *com.businessobjects.webpath.InfoView.jar* pour la zone de lancement BI classique.

b. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* dans *com.businessobjects.webpath.fioriBI.jar* pour la zone de lancement BI façon Fiori.

2. Modifiez le fichier custom.jsp.

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code
request.getSession().setAttribute("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Remarque**
>
> Vous devez remplacer <Shared_Secret_Key> par la nouvelle clé disponible dans le fichier *TrustedPrincipal.conf*. Voir Création d'une clé de secret partagé [page 413] pour apprendre à créer une clé de secret partagé.

9.10.1.3.4 Création du fichier myScript.js

1. Ouvrez *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* et créez le fichier myScript.js.
2. Ajoutez à myScript.js les éléments suivants :

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Redémarrez le serveur Tomcat.

9.10.1.3.5 Configuration des fichiers de propriété personnalisés et internes BOE

1. Accédez à *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*
2. Ouvrez le fichier bilaunchpad.properties et modifiez les propriétés suivantes :

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Redémarrez le serveur Tomcat.

9.10.1.3.6 Configuration des fichiers Web.xml BOE

1. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`
2. Modifiez le fichier web.xml à cet emplacement avec le code indiqué ci-dessous :

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Ajoutez les paramètres au fichier web.xml en suivant les étapes ci-dessous :
   a. `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Ajoutez les paramètres ci-dessous :

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Veuillez répéter les étapes en accédant à `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`

> → Conseil
>
> Pour vérifier si vous avez correctement configuré l'authentification sécurisée, utilisez l'URL suivante pour accéder à l'application de la zone de lancement BI : https://[nomcms]:8443/BOE/BI/logon.jsp, [nomcms] étant le nom de l'ordinateur qui héberge le CMS.

9.10.2 Authentification X.509 pour les services Web

9.10.2.1 Services Web SOAP

9.10.2.1.1 Configuration SSL dans Tomcat

Lorsque vous utilisez des services Web, vous devez configurer SSL dans Tomcat avant de configurer la plateforme SAP Business Intelligence.

> ⓘ Remarque
>
> Un utilisateur doit exister dans la plateforme de BI pour obtenir la connexion unique via l'authentification X.509.

1. Accédez à `<INSTALLDIR>\tomcat\conf`.
2. Ouvrez server.xml dans un éditeur XML et modifiez la balise XML :

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```
3. Enregistrez le fichier.

   > ⓘ Remarque
   >
   > Le mot de passe et l'emplacement des fichiers mentionnés ci-dessus sont juste des exemples. Vous pouvez utiliser le mot de passe et l'emplacement de votre choix.

   > ⓘ Remarque
   >
   > Pour en savoir plus, voir Création et configuration des certificats et des fichiers de stockage de clés [page 408] sur la création et la configuration des fichiers de stockage de clés.

9.10.2.1.2 Configuration du fichier axis2.xml

> **Remarque**
>
> Sur Linux ou Unix, assurez-vous que l'utilisateur de l'installation BI du système d'exploitation dispose des droits récursif 755 sur `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje` avant de réaliser les étapes suivantes. Les droits peuvent être octroyés à l'aide de la commande `chmod -R 755`

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
2. Ouvrez le fichier axis2.xml dans n'importe quel éditeur XML.
3. Mettez à jour la balise xml avec le nouveau numéro de port pour autoriser une connexion sécurisée.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Remarque**
>
> La configuration par défaut suppose que AxisServlet reçoit seulement des demandes via HTTP. Pour autoriser HTTPS, vous devez configurer AxisServletListener avec le nom "HTTPS" et spécifier le paramètre du port sur chaque récepteur. En outre, vous pouvez ajouter ou supprimer plusieurs numéros de port en mettant à jour les balises xml.

4. Enregistrez axis2.xml.
5. Redémarrez le serveur Tomcat.
6. Utilisez le navigateur de votre choix et accédez à https://<IP address>:<https port>/dswsbobje/services/listServices pour valider la connexion sécurisée. Une fois que vous avez accédé au lien, trustedLoginWithX509 s'affiche sous l'onglet Session.

9.10.2.1.3 Génération de la valeur d'un secret partagé

1. Lancez la Central Management Console
2. Ouvrez *Authentification* > *Entreprise.*
3. Sous *Authentification sécurisée* cochez la case *L'authentification sécurisée est activée*.
4. Cliquez sur *Nouveau secret partagé*. La clé du secret partagé est générée.
5. Cliquez sur *Télécharger le secret partagé* puis sur *Mettre à jour*.
6. Sous Windows, copiez le fichier téléchargé TrustedPrincipal.conf sur `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`.

> **Remarque**
>
> Vous pouvez afficher la valeur du secret partagé en ouvrant TrustedPrincipal.conf dans l'éditeur XML de votre choix.

9.10.2.1.4 Configuration du fichier web.xml

1. Accédez à `<INSTALLDIR>\tomcat\webapps\dswsbobje\WEB-INF.`
2. Ouvrez web.xml dans un éditeur XML et mettez à jour la balise XML avec le nom de l'ordinateur de l'hôte du CMS.

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. Ajoutez la balise XML ci-dessous avec la valeur du secret partagé. Pour en savoir plus sur la génération de la valeur d'un secret partagé, consultez Génération de la valeur d'un secret partagé [page 417].

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. Enregistrez le fichier web.xml.

> **Remarque**
>
> Les configurations réalisées dans le fichier axis2.xml seront ignorées si vous effectuez une mise à niveau à partir d'une version inférieure à BI 4.2 SP04.

9.10.2.2 Services Web RESTful

> **Remarque**
>
> Un utilisateur doit exister dans la plateforme de BI pour obtenir la connexion unique via l'authentification X.509.

Consultez la rubrique Configuration HTTPS/SSL dans le *Guide d'administration de la plateforme de Business Intelligence* afin d'établir une authentification sécurisée pour les services Web RESTful.

Pour établir une authentification sécurisée à l'aide de certificats X.509, vous devez générer une clé de secret partagé. Pour plus d'informations, reportez-vous à la rubrique Génération de la valeur d'un secret partagé dans le *Guide d'administration de la plateforme de Business Intelligence*.

Pour plus de détails sur le point de terminaison SDK REST, vous pouvez également vous référer à *Référence d'API* > *Authentification* > */v1//logon/trustedx509* dans le *Guide du développeur des services Web RESTful de la plateforme de Business Intelligence*.

9.10.2.2.1 Authentification X.509 pour les services Web RESTful Web sur Tomcat

Dans la cryptographie à clé publique, X.509 est une norme qui définit les exigences liées à un certificat numérique sécurisé. Un certificat X.509 vérifie la possession de la clé publique par un utilisateur ou une identité de services.

Vous pouvez désormais activer l'authentification X.509 pour les services Web RESTful sur le serveur d'applications Tomcat en suivant les étapes ci-dessous :

1. Activez le SSL sur Tomcat. Pour en savoir plus, voir Configuration SSL dans Tomcat [page 416].
2. Générez une clé de secret partagé. Pour en savoir plus, voir Génération de la valeur d'un secret partagé [page 417].
3. Ouvrez le fichier clé de secret partagé dans un éditeur de texte.
4. Copiez la clé de secret partagé.
5. Modifiez le fichier *biprws.properties*.
   a. Accédez à `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default`.
   b. Ouvrez le fichier *biprws.properties* dans un éditeur de texte.
   c. Recherchez *Trusted_Auth_Shared_Secret=*.
   d. Collez la clé de secret partagé sur la valeur *Trusted_Auth_Shared_Secret=*.
   e. Enregistrez le fichier *biprws.properties*.

9.10.3 Authentification X.509 pour la CMC

> **Remarque**
>
> Un utilisateur doit exister dans la plateforme de BI pour obtenir la connexion unique via l'authentification X.509.

Vous pouvez obtenir la connexion unique via l'authentification X.509 en suivant ces étapes :

1. Création et configuration des certificats et des fichiers de stockage de clés [page 408]
2. Configuration SSL unidirectionnelle [page 412]
3. Configuration SSL bidirectionnelle [page 412]
4. Création d'une clé de secret partagé [page 413]
5. Transmission de la clé de secret partagé via le fichier TrustedPrincipal.conf [page 413]
6. Modification du fichier Custom.jsp (pour la CMC) [page 420]
7. Création du fichier myScript.js (pour la CMC) [page 420]

8. Configuration des fichiers de propriété personnalisés et internes BOE (pour la CMC) [page 421]
9. Configuration du fichier Web.xml BOE (pour la CMC) [page 421]

9.10.3.1 Modification du fichier Custom.jsp (pour la CMC)

> **Remarque**
>
> Créez un utilisateur avec un nom d'ordinateur dans la CMC avant de modifier le fichier custom.jsp. Si un utilisateur existe sur un ordinateur, vous pouvez directement passer aux étapes suivantes.

1. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` dans com.businessobjects.webpath.InfoView.jar.
2. Modifiez le fichier custom.jsp.

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code request.getSession().setAttribute("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Remarque**
>
> Vous devez remplacer la valeur du secret partagé dans ce code par la nouvelle clé, et l'utilisateur par le nom d'ordinateur créé dans la CMC.

9.10.3.2 Création du fichier myScript.js (pour la CMC)

1. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources and create myScript.js`.
2. Ajoutez à myScript.js les éléments suivants :

```
function goToLogonPage()
{
window.location = "logon.jsp";
```

```
}
```

3. Redémarrez le serveur Tomcat.

9.10.3.3 Configuration des fichiers de propriété personnalisés et internes BOE (pour la CMC)

1. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Ouvrez le fichier CmcApp.properties et ajoutez les paramètres :

   ```
   sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter,
   trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela,
   trustedX509, sapSSO, sitemindera
   ```

3. Redémarrez le serveur Tomcat.

9.10.3.4 Configuration du fichier Web.xml BOE (pour la CMC)

1. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Modifiez le fichier web.xml à cet emplacement avec le code indiqué ci-dessous :

   ```
   <init-param>
   <param-name>extendedFrameworkExports</param-name>
   <param-
   value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
   idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
   ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
   bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
   value>
   </init-param>
   ```

3. Ajoutez les paramètres au fichier web.xml en suivant les étapes ci-dessous :
   a. Accédez à `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Ajoutez les paramètres ci-dessous :

      ```
      <init-param>
      <param-name>trusted.auth.shared.secret</param-name>
      <param-value>Shared_Secret_Key</param-value>
      </init-param>
      ```

   c. Veuillez répéter les étapes en accédant à `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`

> **Remarque**
>
> Pour vérifier si vous avez correctement configuré l'authentification sécurisée, utilisez l'URL suivante pour accéder à l'application de la zone de lancement BI : https://[nomcms]:8443/BOE/BI/logon.jsp, [nomcms] étant le nom de l'ordinateur qui héberge le CMS.

9.11 Authentification OpenID Connect

Vous pouvez activer l'authentification OpenID Connect.

L'authentification OpenID Connect fonctionne sur la base du serveur d'authentification (OAuth). Comme pour la prise en charge de Cloud Drive, l'authentification OpenID Connect repose également sur la configuration du serveur d'authentification. Pour en savoir plus sur la configuration du serveur d'authentification, voir Configuration du serveur d'autorisation [page 765].

L'authentification OpenID Connect est développée en plus de l'authentification Enterprise.

Comme dans le cas de l'authentification SAML, les utilisateurs doivent être importés à l'avance dans la plateforme de BI en tant qu'utilisateurs Enterprise (secEnterprise).

> **Remarque**
>
> Lors de l'importation d'utilisateurs, vous devez vous assurer que l'ID d'adresse électronique de l'utilisateur est également inclus.

Contrairement à l'authentification SAML, ce qui suit s'applique pour l'authentification OpenID Connect :

- Toutes les configurations doivent être effectuées dans le backend de la plateforme de BI et non dans la couche du serveur d'applications.
- Elle ne dépend pas de l'authentification sécurisée.

L'authentification OpenID Connect est prise en charge uniquement pour la zone de lancement BI et OpenDocument.

9.11.1 Activation de l'authentification OpenID Connect

L'authentification OpenID Connect est prise en charge uniquement pour la zone de lancement BI et OpenDocument.

Pour plus d'informations sur l'activation de l'authentification OpenID Connect, voir Paramètres d'authentification Enterprise [page 245]. Après avoir activé l'authentification OpenID Connect au niveau du plugin d'authentification Enterprise dans le backend, vous devez activer la même couche d'application pour les applications prises en charge (par exemple, le fichier `FioriBI.properties` pour la zone de lancement et le fichier `OpenDocument.properties` pour les applications OpenDocument sous `WEB-INF/config/custom`.

Pour activer le workflow d'authentification SSO, définissez `logon.webssoauthentication.framework` sur `OpenId`.

Définissez `openid.restful.url` sur l'URL des services Web RESTful de l'infrastructure (par exemple, `https://<server>:8443/biprws`).

Vous pouvez vous connecter à la zone de lancement BI via OpenID à l'aide de l'URL `…/BO/BI`. Toutefois, une fois que vous vous connectez à l'aide de l'authentification OpenID Connect à la zone de lancement BI, vous pouvez noter que le chemin de contexte d'un espace réservé "WEBSSO" est ajouté à l'URL. Cela restera sur le chemin de l'URL après la déconnexion. Si vous voulez à nouveau vous connecter à partir de la même fenêtre à l'aide de la même URL, vous devez supprimer "WEBSSO" de l'URL du navigateur.

10 Référence de la source de données

10.1 Mappage des références de connexion étendu

Dans BI 4.2.X et les versions antérieures, un administrateur ne pouvait sauvegarder qu'un seul ensemble de références de connexion à la base de données pour chaque utilisateur dans la CMC.

Cette fonctionnalité requiert que l'administrateur conserve les mêmes références de connexion pour toutes les différentes bases de données. À compter de BI 4.3, vous pouvez sauvegarder plusieurs ensembles de références de connexion à la base de données pour chaque utilisateur via des références de source de données.

> **Remarque**
>
> La fonction de mappage de référence étendue introduite dans SAP BusinessObjects Business Intelligence Platform 4.3 est prise en charge uniquement dans l'outil de conception d'information. Le mappage de référence étendu n'est pas pris en charge dans l'outil de conception d'univers.

Référence de la source de données dans la CMC

Dans la CMC, un administrateur crée une référence de la source de données dans la plateforme de BI. Cette référence de la source de données est ensuite utilisée dans les propriétés de l'utilisateur où l'administrateur définit un ensemble de références de connexion à la base de données. Cette référence de la source de données est ensuite utilisée dans le cadre du mappage des références de connexion qui est un mode d'authentification disponible dans les connexions.

L'administrateur a à sa disposition une option pour sélectionner la référence de la source de données de son choix si le mappage des références de connexion est sélectionné comme mode d'authentification. De la même manière, un administrateur peut créer plusieurs références de source de données si plusieurs bases de données se connectent à la plateforme de BI et définir des références de connexion uniques pour chaque utilisateur.

> **Remarque**
>
> Lorsque vous importez des utilisateurs via un fichier CSV, promouvez les utilisateurs à l'aide de l'outil de gestion des promotions ou, lorsque vous effectuez une sélection pour synchroniser les références de connexion à la source de données lors de la connexion aux types d'authentification Enterprise, LDAP, Windows AD, la plateforme de BI affecte les références de connexion à la base de données à la référence de la source de données par défaut.

Référence de la source de données dans la zone de lancement BI

Les références aux sources de données sont également disponibles dans la zone de lancement BI, où vous pouvez mettre à jour et mapper vos références de connexion utilisateur.

> ⓘ Remarque
>
> Vous ne pouvez pas modifier les détails *de référence de la source de données*, mais vous pouvez modifier les champs *Nom du compte*, *Mot de passe* et *Confirmer le mot de passe*.

Fonctionnement

Supposons ce qui suit :

- Deux références de la source de données sont disponibles sur la plateforme de BI, par exemple, DSR1 pour votre base de données des ventes et DSR2 pour votre base de données financières.
- Chaque référence de la source de données a des références de connexion à la base de données définies dans les propriétés utilisateur de l'Utilisateur A
- Deux connexions, CN1 et CN2, sont configurées pour utiliser le mappage des références de connexion comme mode d'authentification.
- DSR1 est associé à la connexion CN1 et DSR2 est associé à CN2.

Désormais, si un Utilisateur A tente d'actualiser un rapport qui nécessite l'accès à la base de données des ventes, la plateforme de BI recherche DSR1 dans les propriétés de l'utilisateur et utilise les références de connexion à la base de données définies par rapport à DSR1 pour établir une connexion.

Pour utiliser une référence de la source de données, vous devez effectuer les tâches suivantes.

1. Création d'une référence de la source de données [page 424]
2. Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la CMC [page 425]
3. Association d'une référence de la source de données à la connexion OLAP [page 427]

> ⓘ Remarque
>
> Il est également possible de configurer le mappage des références de connexion pour les connexions relationnelles et les connexions OLAP dans l'outil de conception d'information.

10.1.1 Création d'une référence de la source de données

Une référence de la source de données agit comme une variable qu'un administrateur crée sur la plateforme de BI pour enregistrer un ensemble unique de références de connexion à la base de données pour chaque utilisateur. Suivez les étapes ci-dessous pour créer une référence de la source de données.

1. Connectez-vous à la CMC.

2. Sous Définir, accédez à Références de la source de données.
3. Sélectionnez l'icône (Créer une référence de la source de données).
4. Ajoutez le titre de votre référence de la source de données et une description.
5. Sélectionnez OK.

Vous avez créé avec succès une référence de la source de données.

10.1.2 Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la CMC

Une référence de la source de données doit avoir une référence de connexion à une base de données définie dans les propriétés utilisateur pour permettre à l'utilisateur de se connecter à une base de données. Pour définir les références de connexion à la base de données, procédez comme suit :

1. Connectez-vous à la CMC.
2. Accédez à *Utilisateurs et groupes*.
3. Ouvrez le menu contextuel d'un utilisateur dans *Liste des utilisateurs*.
4. Accédez à *Propriétés* et sélectionnez *Ajouter* sous *Références de connexion à la source de données*.
5. Sélectionnez la référence de la source de données préférée.
6. Saisissez les valeurs pour *Nom du compte*, *Mot de passe* et *Confirmer le mot de passe*.
7. Répétez le processus à partir de l'étape 4 pour ajouter une autre référence de la source de données.
8. Sélectionnez *Enregistrer et fermer*.

   Vous avez défini avec succès les références de connexion à la base de données pour une référence de la source de données.

10.1.3 Définition des références de connexion à la base de données par rapport à une référence de la source de données pour un utilisateur dans la zone de lancement BI

Une référence de la source de données doit avoir une référence de connexion à une base de données définie dans les propriétés utilisateur pour permettre à l'utilisateur de se connecter à une base de données.

Les références aux sources de données sont désormais disponibles dans la zone de lancement BI, où vous pouvez également mettre à jour et mapper vos références de connexion utilisateur. Les références de connexion à la base de données sont synchronisées entre la CMC et la zone de lancement BI.

Suivez les étapes ci-dessous pour définir les références de connexion à la base de données dans la zone de lancement BI.

1. Connectez-vous à la zone de lancement BI

2. Ouvrez (Paramètres utilisateur), cliquez sur l'option (*Paramètres*) dans la liste déroulante.

   La fenêtre *Paramètres* s'affiche.
3. Cliquez sur *Compte utilisateur (administrateur)*.

   La page Compte utilisateur s'affiche avec deux onglets : *Informations de compte*, *Références de connexion à la base de données* et *Jetons d'autorisation*.
4. Cliquez sur *Références de connexion à la base de données*.

   Vous pouvez afficher les données synchronisées de l'utilisateur à partir de la CMC affichée ici.

   > **Remarque**
   >
   > Vous ne pouvez pas modifier les détails de la *Référence de la source de données*.
   >
   > Vous pouvez cependant modifier les champs *Nom du compte*, *Mot de passe* et *Confirmer le mot de passe*.

   Lorsque vous modifiez votre mot de passe, un message flottant s'affiche à l'écran *Les modifications apportées à certaines préférences prendront effet après le rechargement de la page*.
5. Cliquez sur *Enregistrer* et *Fermer* pour enregistrer les modifications des références de connexion mappées.

10.1.4 Définition des références de connexion à une base de données par rapport à une référence de la source de données pour un groupe

Une référence de la source de données doit avoir une référence de connexion à une base de données définie dans les propriétés utilisateur pour permettre à l'utilisateur de se connecter à une base de données.

> **Remarque**
>
> Cette tâche ne met pas à jour les références de la source de données pour les membres des sous-groupes. Vous pouvez suivre les mêmes étapes pour le sous-groupe pour mettre à jour les références de la source de données pour ses membres.

Suivez les étapes ci-dessous pour définir les références de connexion à la base de données :

1. Connectez-vous à la CMC.
2. Accédez à *Utilisateurs et groupes*.
3. Ouvrez le menu contextuel d'un groupe d'utilisateurs et sélectionnez *Responsable du compte*.
4. Cochez la case qui apparaît en regard de *Références de connexion à la base de données*, puis sélectionnez *Ajouter*.
5. Saisissez les valeurs dans les champs requis.
6. Sélectionnez *Enregistrer et fermer*.

Vous avez défini avec succès une nouvelle référence de la source de données avec les références de connexion à la base de données pour les membres du groupe d'utilisateurs. Vous pouvez accéder aux *Propriétés* de n'importe quel utilisateur de ce groupe d'utilisateurs pour vérifier la référence de la source de données que vous venez de mettre à jour.

10.1.5 Association d'une référence de la source de données à la connexion OLAP

Un administrateur a à sa disposition une option pour sélectionner la référence de la source de données de son choix si le mappage des références de connexion est sélectionné comme mode d'authentification pour une connexion.

Suivez les étapes ci-dessous pour associer une référence de la source de données à une connexion.

1. Connectez-vous à la CMC.
2. Accédez à *Connexions OLAP*.
3. Ouvrez une connexion existante ou créez-en une.
4. Dans le champ *Authentification*, sélectionnez *Mappage des références de connexion*.
   Le champ *Référence de la source de données* s'affiche.
5. Sélectionnez une référence de la source de données.
6. Saisissez les autres détails requis et sélectionnez *Enregistrer*.

Vous avez réussi à associer une référence de la source de données à une connexion OLAP.

11 Administration du serveur

11.1 Utilisation de la zone de gestion Serveurs de la CMC

La zone de gestion Serveurs de la CMC constitue votre principal outil pour les tâches de gestion des serveurs. Elle fournit la liste de tous les serveurs de votre déploiement. Pour la plupart des tâches de gestion et de configuration, vous devez sélectionner un serveur dans la liste et choisir une commande dans le menu Gérer ou Action.

A propos de l'arborescence

L'arborescence de navigation dans la partie gauche de la zone de gestion Serveurs permet de visualiser la liste des serveurs de différentes manières. Sélectionnez des éléments dans l'arborescence de navigation pour modifier les informations affichées dans le volet *Détails*.

Option de l'arborescence de navigation	Description
Liste des serveurs	Affiche la liste complète des serveurs du déploiement.
Liste des groupes de serveurs	Affiche une liste horizontale de tous les groupes de serveurs disponibles dans le volet Détails. Sélectionnez cette option si vous souhaitez configurer les paramètres ou la sécurité d'un groupe de serveurs.
Groupes de serveurs	Répertorie les groupes de serveurs et les serveurs appartenant à chaque groupe. Lorsque vous sélectionnez un groupe de serveurs, les serveurs et groupes de serveurs correspondants sont affichés dans le volet Détails d'une vue hiérarchique.
Noeuds	Affiche la liste des nœuds de votre déploiement. Les nœuds sont configurés dans le CCM. Vous pouvez sélectionner un nœud en cliquant dessus pour visualiser ou gérer les serveurs qu'il contient.

Option de l'arborescence de navigation	Description
Catégories de service	Affiche la liste des types de service pouvant faire partie de votre déploiement. Les catégories de services sont divisées en services principaux de la plateforme de BI et en services associés à des composants SAP BusinessObjects spécifiques. Les catégories de service comprennent : • *Services de connectivité* • *Services principaux* • *Services Crystal Reports* • *Services de fédération de données* • *Services de gestion des promotions* • *Services Analysis* • *Services Web Intelligence* Sélectionnez une catégorie de service dans la liste de navigation pour visualiser ou gérer les serveurs appartenant à cette catégorie. **Remarque** Un serveur peut héberger des services appartenant à plusieurs catégories de services. Par conséquent, un serveur peut apparaître dans plusieurs catégories de services.
Statut du serveur	Affiche les serveurs en fonction de leur état actuel. Cet outil s'avère très utile pour vérifier quels sont les serveurs en cours d'exécution ou arrêtés. Si vous êtes confronté à un ralentissement des performances système, vous pouvez utiliser la liste *Statut du serveur* pour déterminer rapidement si certains de vos serveurs présentent un état anormal. Les états de serveur possibles sont les suivants : • *Arrêté* • *Démarrage en cours* • *Initialisation en cours* • *Exécution en cours* • *Arrêt en cours* • *Exécution avec des erreurs* • *Échec* • *Attente des ressources*

A propos du volet Détails

Selon les options que vous avez sélectionnées dans l'arborescence, le volet *Détails* situé à droite de la zone de gestion Serveurs affiche une liste des serveurs, groupes de serveurs, états, catégories ou nœuds. Le tableau suivant décrit les informations répertoriées pour les serveurs dans le volet *Détails*.

> **Remarque**
>
> Pour les nœuds, groupes de serveurs, catégories et états, le volet *Détails* affiche généralement les noms et les descriptions.

Colonne du volet Détails	Description
Nom du serveur ou *Nom*	Affiche le nom du serveur.
État	Affiche le statut actuel du serveur. Vous pouvez effectuer un tri par état de serveur à l'aide de la liste *Statut du serveur* dans l'arborescence. Les états de serveur possibles sont les suivants : • *Arrêté* • *Démarrage en cours* • *Initialisation en cours* • *Exécution en cours* • *Arrêt en cours* • *Exécution avec des erreurs* • *Échec* • *Attente des ressources*
Activé	Indique si le serveur est activé ou désactivé.
Périmé	Si le serveur est marqué comme *Périmé*, un redémarrage est nécessaire. Par exemple, si vous modifiez certains paramètres du serveur dans l'écran *Propriétés* du serveur, vous devrez peut-être redémarrer le serveur pour prendre en compte les modifications.
Type	Affiche le type de serveur.
Nom d'hôte	Affiche le nom d'hôte du serveur.
Santé	Indique la santé globale du serveur. Les états de serveur possibles sont les suivants : • *Vert* (sain) • *Orange* (attention) • *Rouge* (danger) L'état de santé d'un serveur dépend directement du statut de la veille du serveur. Par exemple, l'état de santé du Central Management Server dépend du statut de `<NODENAME>.CentralManagementServer Watch`. Vous pouvez accéder aux détails des veilles sur la page *Suivi* dans la CMC. Dans l'onglet *Liste de veilles*, sélectionnez la veille et cliquez sur *Modifier*. La *Règle de mise en garde* et la *Règle de danger* pour la veille s'affichent, qui sont mappées à l'état de santé orange et rouge, respectivement.
PID	Affiche le numéro d'identification unique du processus.

Colonne du volet Détails	Description
Description	Affiche une description du serveur. Vous pouvez modifier cette description dans la page *Etat du serveur* du serveur.
Date de modification	Affiche la date de la dernière modification du serveur ou du dernier changement d'état du serveur. Cette colonne est très utile pour vérifier le statut des serveurs récemment modifiés.

11.2 Gestion des serveurs à l'aide de scripts sous Windows

Le fichier exécutable `ccm.exe` vous permet de démarrer, arrêter, redémarrer, activer et désactiver les serveurs de votre déploiement Windows à partir de la ligne de commande.

Informations associées

ccm.exe [page 1121]

11.3 Gestion des serveurs sous Unix

Le fichier exécutable `ccm.sh` vous permet de démarrer, arrêter, redémarrer, activer et désactiver les serveurs de votre déploiement Unix à partir de la ligne de commande.

Informations associées

ccm.sh [page 1113]

11.4 Affichage et modification du statut d'un serveur

11.4.1 Visualisation de l'état des serveurs

Le statut d'un serveur correspond à son état de fonctionnement actuel : il peut être en cours d'exécution, de démarrage ou d'arrêt, arrêté, en échec, en cours d'initialisation, démarré avec des erreurs ou en attente de ressources. Pour pouvoir répondre à une requête de la plateforme de BI, le serveur doit être en cours

d'exécution et activé. Bien qu'il s'exécute toujours en tant que processus, un serveur désactivé ne peut accepter aucune requête des autres composants de la plateforme de BI. Un serveur arrêté n'est plus considéré comme un processus en cours d'exécution.

Cette section explique comment modifier l'état des serveurs à l'aide de la CMC.

Informations associées

Pour visualiser le statut d'un serveur [page 432]
Affichage de l'état des services [page 432]
Démarrage, arrêt et redémarrage d'un serveur [page 433]
Activation et désactivation de serveurs [page 436]
Arrêt d'un Central Management Server [page 435]
Pour démarrer les serveurs automatiquement [page 435]

11.4.1.1 Pour visualiser le statut d'un serveur

1. Accédez à la zone de gestion *Serveurs* de la CMC.

   Le volet *Détails* affiche les catégories de service de votre déploiement.
2. Pour afficher la liste des serveurs d'un groupe de serveurs, d'un nœud ou d'une catégorie de service, cliquez sur l'élément concerné dans l'arborescence de navigation.
   Le volet *Détails* affiche la liste des serveurs votre déploiement. La colonne *ETAT* indique le statut pour chaque serveur de la liste.
3. Si vous souhaitez visualiser la liste de tous les serveurs affichant un statut donné, développez l'option *Statut du serveur* dans l'arborescence de navigation et sélectionnez le statut de votre choix.

   Une liste des serveurs ayant le statut sélectionné s'affiche dans le volet Détails.

   > **Remarque**
   >
   > Ceci peut s'avérer particulièrement utile lorsque vous devez visualiser rapidement une liste des serveurs qui ne démarrent pas correctement ou se sont arrêtés de manière inattendue.

11.4.1.2 Affichage de l'état des services

Si un service échoue, l'état du serveur hôte est défini sur *Exécution avec des erreurs* (c'est-à-dire qu'au moins un service a démarré correctement) ou *Échec* (c'est-à-dire qu'aucun des services n'a démarré correctement). Vous pouvez afficher l'état des serveurs dans la CMC et le CCM. Vous pouvez cependant afficher le statut de chaque service dans la page *Propriétés* du serveur dans la CMC.

1. Accédez à la zone de gestion *Serveurs* de la CMC.

   Le volet *Détails* affiche les catégories de service de votre déploiement.

2. Pour afficher la liste des serveurs d'un groupe de serveurs, d'un nœud ou d'une catégorie de service, cliquez sur l'élément concerné dans l'arborescence de navigation.
   Le volet *Détails* affiche la liste des serveurs votre déploiement.
3. Cliquez deux fois sur une connexion pour ouvrir la page *Propriétés* correspondante.

   La page *Propriétés* affiche les propriétés du serveur et des services qu'il héberge. Des messages d'erreur sont également affichés pour les services ayant échoué.

Informations associées

Visualisation de l'état des serveurs [page 431]

11.4.2 Démarrage, arrêt et redémarrage d'un serveur

Le démarrage, l'arrêt et le redémarrage des serveurs sont autant d'actions courantes que vous réalisez lorsque vous configurez des serveurs ou les déconnectez. Par exemple, si vous souhaitez modifier le nom d'un serveur, vous devez arrêter ce dernier au préalable. Une fois les modifications apportées, il suffit de le redémarrer pour que les modifications soient prises en compte. Si vous modifiez les paramètres de configuration d'un serveur, la CMC affiche un message d'invite lorsque vous devez redémarrer le serveur.

La suite de cette section présente les cas où un changement de configuration nécessite l'arrêt ou le redémarrage du serveur. Dans la mesure où ces tâches sont particulièrement fréquentes, vous trouverez tout d'abord l'explication des concepts et des différences, puis les procédures générales à respecter.

Action	Description
Arrêt d'un serveur	Vous pouvez être dans l'obligation d'arrêter les serveurs de la plateforme de BI pour pouvoir modifier certaines propriétés et certains paramètres.
Démarrage d'un serveur	Si vous avez arrêté un serveur afin de le configurer, vous devez le redémarrer pour que vos modifications s'appliquent et que le serveur recommence à traiter les demandes.
Redémarrage d'un serveur	Le redémarrage d'un serveur regroupe deux étapes : son arrêt complet et son redémarrage. Si vous devez redémarrer un serveur après avoir modifié l'un de ses paramètres, vous y serez invité par la CMC.
Lancement automatique d'un serveur	Vous pouvez configurer les serveurs de sorte qu'ils démarrent automatiquement lors du démarrage du Server Intelligence Agent.

Action	Description
Forcer l'arrêt	Arrête immédiatement le serveur (un serveur s'arrête dès lors que toutes les activités de traitement en cours sont terminées). Ne forcez à se terminer un serveur que lorsque l'arrêt du serveur a échoué et que vous devez arrêter le serveur immédiatement.

→ Conseil

Lorsque vous arrêtez (ou redémarrez) un serveur, vous abandonnez le processus du serveur et, ce faisant, arrêtez complètement ce dernier. Avant d'arrêter un serveur, il est recommandé de

- Désactiver le serveur pour qu'il puisse finir de traiter les travaux en cours, et
- S'assurer qu'il ne reste aucun événement d'audit dans la file. Pour visualiser le nombre d'événements d'audit restant dans la file, accédez à l'écran *Métriques* du serveur et visualisez la métrique *Nombre actuel d'événements d'audit en attente*.

Informations associées

Activation et désactivation de serveurs [page 436]

11.4.2.1 Pour démarrer, arrêter ou redémarrer des serveurs à l'aide de la CMC

1. Accédez à la zone de gestion *Serveurs* de la CMC.

   Le volet *Détails* affiche les catégories de service de votre déploiement.
2. Pour afficher une liste des serveurs d'un groupe de serveurs, d'un nœud ou d'une catégorie de service particuliers, sélectionnez cet élément dans le volet de navigation.
   Le volet *Détails* affiche une liste de serveurs.
3. Si vous souhaitez visualiser la liste de tous les serveurs affichant un statut donné, développez l'option *Statut du serveur* dans l'arborescence de navigation et sélectionnez le statut de votre choix.

   Une liste de serveurs ayant le statut sélectionné s'affiche dans le volet *Détails*.

   ⓘ Remarque

   Ceci peut s'avérer particulièrement utile lorsque vous devez visualiser rapidement une liste des serveurs qui ne démarrent pas correctement ou se sont arrêtés de manière inattendue.
4. Cliquez avec le bouton droit de la souris sur le serveur dont vous souhaitez modifier le statut et, selon l'action à effectuer, sur*Démarrer le serveur*, *Redémarrer le serveur*, *Arrêter le serveur* ou *Forcer l'arrêt*.

11.4.2.2 Pour démarrer, arrêter ou redémarrer un serveur Windows à l'aide du CCM

1. Dans le CCM, cliquez sur le bouton *Gérer les serveurs* de la barre d'outils.
2. Lorsque vous y êtes invité, connectez-vous à votre CMS avec un compte d'administrateur.
3. Dans la boîte de dialogue *Gérer les serveurs*, sélectionnez le serveur que vous voulez démarrer, arrêter ou redémarrer.
4. Cliquez sur *Démarrer*, *Arrêter*, *Redémarrer* ou *Forcer l'arrêt*.
5. Cliquez sur *Fermer* pour revenir au CCM.

11.4.2.3 Pour démarrer les serveurs automatiquement

Par défaut, les serveurs de votre déploiement sont démarrés automatiquement au démarrage du Server Intelligence Agent. Cette procédure indique où définir l'option de démarrage automatique.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur que vous souhaitez lancer automatiquement.
   L'écran *Propriétés* s'affiche.
3. Dans *Paramètres courants*, cochez la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* puis cliquez sur *Enregistrer* ou *Enregistrer et fermer*.

> ⓘ Remarque
>
> Si la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* n'est pas cochée pour chaque CMS du cluster, vous devez utiliser le CCM pour redémarrer le système. Après avoir utilisé le CCM pour arrêter le SIA, cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*. Dans l'onglet *Démarrage*, cliquez sur *Propriétés* pour ouvrir la page Propriétés du serveur du CMS. Sélectionnez *Démarrage automatique*, puis cliquez sur *OK* pour fermer la page Propriétés du serveur, puis cliquez à nouveau sur *OK*. Redémarrez le SIA. L'option *Démarrage automatique* est disponible uniquement si la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* est décochée pour tous les CMS du cluster.

11.4.3 Arrêt d'un Central Management Server

Si votre installation de la plateforme de BI comporte plusieurs CMS (Central Management Servers) actifs, vous pouvez fermer un seul CMS sans perdre de données, ni affecter la fonctionnalité du système. Un autre CMS du nœud récupérera la charge du serveur arrêté. La mise en cluster de plusieurs CMS permet d'effectuer la maintenance de chaque Central Management Server à tour de rôle sans arrêter la plateforme de BI.

Toutefois, si votre déploiement de la plateforme de BI ne comporte qu'un seul CMS, son arrêt entraîne l'indisponibilité de la plateforme BI pour les utilisateurs et interrompt le traitement des rapports et des programmes. Pour éviter ce problème, le Server Intelligence Agent de chaque nœud vérifie si au moins un CMS s'exécute en permanence. Vous pouvez arrêter un CMS en arrêtant son SIA, mais avant d'arrêter le SIA,

vous devez désactiver les serveurs de traitement via la CMC afin qu'ils terminent les travaux en cours avant l'arrêt de la plateforme de BI, étant donné que tous les autres serveurs du nœud vont également être arrêtés.

> ⓘ Remarque
>
> Dans certaines situations, vous pouvez être amené à redémarrer le système à partir du CCM alors que le CMS a été arrêté. Par exemple, si vous arrêtez tous les CMS d'un nœud et que la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* est décochée pour tous les CMS du cluster lorsque le SIA démarre, vous devez utiliser le CCM pour redémarrer le système. Dans le CCM, cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*. Dans l'onglet *Démarrage*, cliquez sur *Propriétés* pour ouvrir la page Propriétés du serveur du CMS. Sélectionnez *Démarrage automatique*, puis cliquez sur *OK* pour fermer la page Propriétés du serveur, puis cliquez à nouveau sur *OK*. Redémarrez le SIA. L'option *Démarrage automatique* est disponible uniquement si la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* est décochée pour tous les CMS du cluster.

Si vous souhaitez configurer votre système de manière à pouvoir démarrer et arrêter le CMS dans le cluster sans démarrer ou arrêter les autres serveurs, mettez le CMS sur un nœud séparé. Créez un nœud et clonez le CMS sur ce nœud. Une fois le CMS sur son propre nœud, vous pouvez facilement fermer ce nœud sans affecter les autres serveurs.

Informations associées

Utilisation des nœuds [page 480]
Clonage des serveurs [page 438]
Mise en cluster de Central Management Servers [page 441]

11.4.4 Activation et désactivation de serveurs

Lorsque vous désactivez un serveur de la plateforme de BI, vous l'empêchez de recevoir de nouvelles requêtes de la plateforme de BI et d'y répondre, mais vous n'arrêtez pas réellement le processus du serveur. Cela s'avère utile lorsque vous souhaitez laisser un serveur terminer le traitement des requêtes en cours avant de l'arrêter complètement.

Supposons, par exemple, que vous ayez à arrêter un Job Server avant de redémarrer l'ordinateur sur laquelle il s'exécute. Vous voulez toutefois laisser le serveur mener à bien toutes les requêtes figurant dans sa file d'attente. Vous commencez alors par désactiver le Job Server afin qu'il n'accepte plus aucune autre requête. Accédez ensuite à la Central Management Console pour savoir à quel moment le serveur termine les tâches en cours. (Dans la zone de gestion des *serveurs*, cliquez avec le bouton droit de la souris sur le serveur et sélectionnez *Métriques*.) Puis, une fois le traitement des requêtes en cours terminé, vous pouvez arrêter le serveur en toute sécurité.

> ⓘ Remarque
>
> Le CMS doit être en cours d'exécution pour que vous puissiez activer et/ou désactiver d'autres serveurs.

> **Remarque**
>
> Un CMS ne peut pas être activé ni désactivé.

11.4.4.1 Pour activer et désactiver des serveurs à l'aide de la CMC

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Avec le bouton droit de la souris, cliquez sur le serveur dont vous souhaitez modifier le statut et, selon l'action à effectuer, cliquez sur *Activer le serveur* ou *Désactiver le serveur*.

11.4.4.2 Pour activer ou désactiver un serveur Windows à l'aide du CCM

1. Dans le CCM, cliquez sur *Gérer les serveurs*.
2. Lorsque vous y êtes invité, connectez-vous à votre CMS à l'aide des références de connexion qui vous confèrent des droits d'administration sur la plateforme de BI.
3. Dans la boîte de dialogue *Gérer les serveurs*, sélectionnez le serveur que vous voulez activer ou désactiver.
4. Cliquez sur *Activer* ou sur *Désactiver*.
5. Cliquez sur *Fermer* pour revenir au CCM.

11.5 Ajout, clonage ou suppression de serveurs

11.5.1 Ajout, clonage et suppression de serveurs

Si vous souhaitez ajouter du matériel à la plateforme de BI en installant des composants serveur sur des ordinateurs supplémentaires, exécutez le programme d'installation de la plateforme de BI sur ces ordinateurs. Le programme d'installation vous permet de procéder à une installation personnalisée. Durant l'installation personnalisée, spécifiez le CMS pour votre déploiement existant, puis sélectionnez les composants que vous souhaitez installer sur l'ordinateur local. Pour des informations détaillées sur les options d'installation personnalisée, voir le *Guide d'installation de la plateforme SAP BI*.

11.5.1.1 Ajout d'un serveur

Vous pouvez exécuter plusieurs instances du même serveur de plateforme de BI sur la même machine. Pour ajouter un serveur :

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Dans le menu *Gérer*, cliquez sur *Nouveau* > *Nouveau serveur*.
   La boîte de dialogue *Créer un serveur* s'affiche.
3. Sélectionnez la *Catégorie de service*.
4. Sélectionnez le type de service dont vous avez besoin dans la liste *Sélectionner le service*, puis cliquez sur *Suivant*.
5. Pour ajouter un service supplémentaire au serveur, sélectionnez le service dans la liste *Services supplémentaires disponibles*, puis cliquez sur >.

   > **Remarque**
   >
   > Les services supplémentaires ne sont pas disponibles pour tous les types de serveur.

6. Après avoir ajouté les services supplémentaires souhaités, cliquez sur *Suivant*.
7. Si votre architecture de plateforme de BI est composée de plusieurs nœuds, sélectionnez celui où vous voulez ajouter le nouveau serveur dans la liste *Nœud*.
8. Saisissez le nom du serveur dans zone *Nom*.

   Chaque serveur du système doit disposer d'un nom unique. La convention d'appellation par défaut est `<NOMNOEUD>.<typeserveur>` (un numéro est ajouté s'il existe plusieurs serveurs du même type sur l'ordinateur hôte).
9. Pour inclure une description du serveur, saisissez-en une dans la zone *Description*.
10. Si vous ajoutez un nouveau CMS (Central Management Server), spécifiez un numéro de port dans le champ *Port du serveur de noms*.
11. Cliquez sur *Créer*.
    Le nouveau serveur figure désormais dans la liste des serveurs, dans la zone *Serveurs* de la CMC, mais il n'est ni démarré, ni activé.
12. Utilisez la CMC pour démarrer puis activer le nouveau serveur lorsque vous souhaitez qu'il commence à répondre aux requêtes de la plateforme de BI.

11.5.1.2 Clonage des serveurs

Si vous voulez ajouter une instance de serveur à votre déploiement, vous pouvez cloner un serveur existant. Le serveur cloné conserve les paramètres de configuration du serveur d'origine, à l'exception des paramètres courants et des paramètres de ligne de commande. Cette fonctionnalité peut être particulièrement utile si vous développez votre déploiement et souhaitez créer des instances de serveur utilisant presque tous les paramètres de configuration d'un serveur existant.

Le clonage simplifie également la procédure de déplacement des serveurs d'un nœud à l'autre. Si vous souhaitez déplacer un CMS existant vers un autre nœud, vous pouvez le cloner sur le nouveau nœud. Le CMS cloné apparaît sur le nouveau nœud et conserve tous les paramètres de configuration du CMS d'origine, à l'exception des paramètres courants et des paramètres de ligne de commande.

Certains aspects sont toutefois à prendre en considération lorsque vous clonez des serveurs. Vous ne souhaitez peut-être pas cloner tous les paramètres ; il est donc conseillé de toujours vérifier le serveur cloné afin de s'assurer que sa configuration est appropriée à vos besoins.

> **Remarque**
>
> Avant de cloner des serveurs, assurez-vous que tous les ordinateurs de votre déploiement disposent de la même version de la plateforme de BI (et au besoin des éventuelles mises à jour).

> **Remarque**
>
> Il est possible de cloner des serveurs à partir de n'importe quel ordinateur. Toutefois, vous ne pouvez cloner des serveurs que sur les ordinateurs où sont installées les données binaires requises pour le serveur.

> **Remarque**
>
> Lorsque vous clonez un serveur, le nouveau serveur n'utilise pas obligatoirement les mêmes références de système d'exploitation. Le compte utilisateur est contrôlé par le Server Intelligence Agent sous lequel le serveur est exécuté.

11.5.1.2.1 Utilisation des espaces réservés pour les paramètres de serveur

Les espaces réservés sont des variables au niveau des nœuds, utilisées par les serveurs exécutés sur le nœud. Les espaces réservés sont répertoriés sur une page dédiée de la CMC (Central Management Console). Lorsque vous cliquez deux fois sur un des noms répertoriés sous *Serveurs* dans la CMC, un lien vers les « Espaces réservés » s'affiche dans le volet de navigation gauche. La page *Espaces réservés* dresse la liste de tous les noms d'espace réservé disponibles et de leurs valeurs associées pour le serveur sélectionné. Les espaces réservés contiennent des valeurs en lecture seule et leurs noms commencent et finissent par le signe pour cent %.

> **Remarque**
>
> Vous pouvez toujours remplacer un espace réservé par une chaîne spécifique dans la page *Propriétés du serveur* de la CMC.

Exemple

Les espaces réservés sont utiles dans le cas de clonage de serveurs. Par exemple, la plateforme de BI est installée sur l'ordinateur à plusieurs lecteurs A, sous `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. L'espace réservé `%DefaultAuditingDir%` sera donc `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

Sur l'ordinateur B, il n'y a qu'un seul lecteur de disque (pas de lecteur D) et la plateforme de BI est installée à l'emplacement `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. Dans ce cas, l'espace réservé `%DefaultAuditingDir%` sera `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`

Si vous cloner l'Event Server de l'ordinateur A vers l'ordinateur B en utilisant des espaces réservés pour le répertoire temporaire d'audit, les espaces réservés seront automatiquement résolus et l'Event Server

fonctionnera correctement. Si vous n'utilisez pas d'espaces réservés, l'Event Server échouera à moins que vous ne remplaciez manuellement le paramètre du répertoire temporaire d'audit.

11.5.1.2.2 Pour cloner un serveur

1. Sur l'ordinateur sur lequel vous voulez ajouter le serveur cloné, accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez avec le bouton droit de la souris sur le serveur que vous souhaitez cloner et sélectionnez *Cloner un serveur*.
   La boîte de dialogue *Cloner un serveur* s'affiche.
3. Saisissez un nom pour le serveur (ou utilisez le nom par défaut) dans le champ *Nom du nouveau serveur*.
4. Si vous clonez un CMS (Central Management Server), spécifiez un numéro de port dans le champ *Port du serveur de noms*.
5. Dans la liste *Cloner sur le nœud*, choisissez le nœud sur lequel ajouter le serveur cloné, puis cliquez sur *OK*.
   Le nouveau serveur apparaît dans la zone de gestion des *serveurs* de la CMC.

11.5.1.3 Suppression d'un serveur

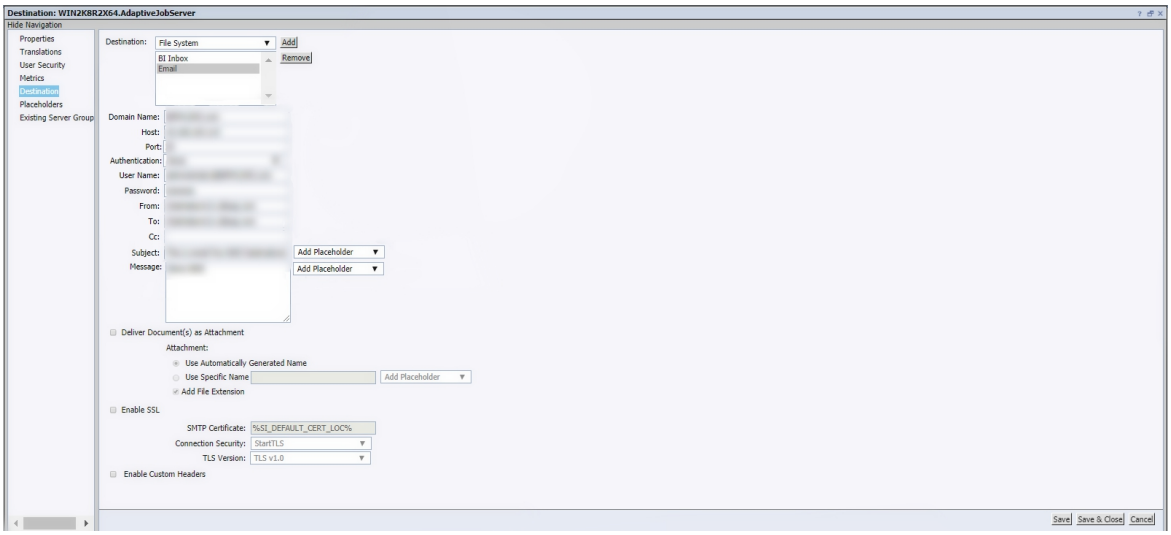
1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Arrêtez le serveur que vous voulez supprimer.
3. Cliquez avec le bouton droit de la souris sur ce serveur, puis sélectionnez *Supprimer*.
4. Lorsque le système vous invite à confirmer votre choix, cliquez sur *OK*.

11.6 Ajout d'en-têtes Internet personnalisés

L'en-tête Internet d'un courrier électronique inclut les informations concernant l'utilisateur ayant rédigé le message, le serveur électronique via lequel le message a été transmis ainsi que l'outil ou le logiciel utilisé pour rédiger le message. Vous pouvez maintenant ajouter des en-têtes Internet personnalisés aux courriers électroniques planifiés à partir de la plateforme SAP BusinessObjects BI. Suivez les étapes ci-dessous pour ajouter des en-têtes personnalisés :

1. Connectez à la *CMC*.
2. Accédez à *Serveurs*, puis à *Liste de serveurs*.
3. Ouvrez le menu contextuel *Adaptive Job Server* et sélectionnez *Destinations*.

4. Dans l'assistant *Destination*, sélectionnez *Courrier électronique* et ajoutez les informations requises pour chaque zone comme ci-dessous :



5. Cochez la case *Activer les en-têtes personnalisés* et ajoutez les en-têtes Internet dans la zone vierge comme illustré ci-après :

6. Choisissez *Enregistrer et fermer*.

Les courriers électroniques avec des documents planifiés contiennent maintenant les en-têtes Internet.

> **Remarque**
>
> - Lors de la planification, sélectionnez *Utiliser les paramètres par défaut* pour ajouter des en-têtes Internet personnalisés dans les courriers électroniques planifiés.
> - Chaque *Adaptive Job Server* doit être configuré pour assurer l'ajout des en-têtes personnalisés dans chaque courrier électronique.

11.7 Mise en cluster de Central Management Servers

11.7.1 Mise en cluster de Central Management Servers

Si vous disposez d'une mise en œuvre importante ou stratégique de la plateforme SAP BusinessObjects Business Intelligence, vous souhaiterez probablement exécuter plusieurs ordinateurs CMS ensemble au sein d'un cluster. Un cluster est constitué d'au moins deux serveurs CMS travaillant ensemble sur une base de données système du CMS. En cas de défaillance de l'un des ordinateurs du cluster, le transfert se fait automatiquement vers un autre CMS afin d'assurer la prise en charge des requêtes de la plateforme de BI. Cette prise en charge "haute disponibilité" vous aide à garantir que les utilisateurs de la plateforme de BI peuvent continuer à accéder aux informations en cas de défaillance d'un équipement.

Cette section vous explique comment ajouter un nouveau membre de cluster de CMS à un système de production pleinement fonctionnel. Lorsque vous ajoutez un CMS à un cluster existant, vous demandez au

nouveau CMS de se connecter à la base de données système actuelle du CMS et de répartir la charge de traitement entre les serveurs CMS existants. Pour en savoir plus sur le CMS actuel, accédez à la zone de gestion *Serveurs* de la CMC.

Avant de procéder à la mise en cluster des ordinateurs du CMS, vous devez vous assurer que chaque CMS est installé sur un système qui présente la configuration requise (y compris les niveaux de version et de correctif requis) pour le système d'exploitation, le serveur de base de données, le mode d'accès aux bases de données, le pilote de base de données et le client de base de données indiqués dans le document Product Availability Matrix (matrice de disponibilité des produits).

Vous devez également respecter les exigences suivantes en matière de mise en cluster.

- Pour des performances optimales, le serveur de base de données qui héberge la base de données système doit être capable de traiter des requêtes simples très rapidement. Le CMS communique fréquemment avec la base de données système et lui adresse de nombreuses requêtes simples. Si le serveur de base de données est incapable de traiter ces requêtes à temps, les performances de la plateforme de BI s'en trouveront fortement réduites.
- Pour des performances optimales, exécutez chaque membre du cluster de CMS sur une machine disposant de la même quantité de mémoire et du même type de processeur.
- Configurez chaque ordinateur de manière identique :
  - Installez le même système d'exploitation, y compris les mêmes versions de Service Pack et de correctifs.
  - Installez la même version de la plateforme de BI (correctifs compris, le cas échéant).
  - Assurez-vous que chaque CMS soit connecté à la base de données système CMS de la même manière : c'est-à-dire avec des pilotes ODBC ou natifs. Veillez à ce que les pilotes soient identiques sur chaque ordinateur et à ce que leur version soit prise en charge.
  - Vérifiez que chaque CMS utilise le même client de base de données pour se connecter à sa base de données système et qu'il s'agit d'une version prise en charge.
  - Vérifiez que chaque CMS utilise le même compte utilisateur de base de données et le même mot de passe pour se connecter à la base de données système. Ce compte doit posséder les droits de création, suppression et mise à jour sur la base de données système.
  - Assurez-vous que les nœuds sur lesquels se trouve chaque CMS sont exécutés sous le même compte de système d'exploitation. (Sous Windows, le compte par défaut est "LocalSystem".)
  - Vérifiez que la date et l'heure sont correctes sur chaque ordinateur (y compris les paramètres relatifs à l'heure d'été).
  - Assurez-vous que tous les ordinateurs du cluster (notamment ceux qui hébergent le CMS) sont définis sur la même heure système. Pour obtenir les meilleurs résultats, synchronisez les ordinateurs avec un serveur de temps (tel que `time.nist.gov`) ou une solution de surveillance centrale.
  - Assurez-vous d'avoir installé les mêmes fichiers WAR sur tous les serveurs d'applications Web du cluster. Pour en savoir plus sur le déploiement des fichiers WAR, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*.
- Assurez-vous que tous les CMS du cluster sont situés sur le même réseau local.
- Les threads hors-bande (-oobthreads) sont utilisés par les pings et notifications de mise en cluster. Comme les deux opérations sont rapides (les notifications sont asynchrones), la plateforme de BI n'a plus besoin de plusieurs threads hors-bande, un seul est créé.
  Si votre cluster comporte plus de huit serveurs CMS, vérifiez que la ligne de commande de chaque CMS comprend l'option `-oobthreads <numCMS>`, `<numCMS>` correspondant au nombre de serveurs CMS du cluster. Cette option garantit que le cluster peut gérer des charges importantes. Pour en savoir plus sur la

configuration des lignes de commande des serveurs, voir l'annexe Lignes de commande des serveurs du *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.

- L'activation de l'audit sur un seul CMS donne les mêmes résultats qu'une configuration dans un environnement en clusters. Vous pouvez également modifier les détails de la base de données d'audit dans la page Paramètres d'audit de la CMC. Les exigences requises pour la base de données d'audit sont identiques à celles de la base de données système en termes de serveurs, de clients, de modes d'accès, de pilotes et d'ID utilisateur.

> → Conseil
>
> Par défaut, le nom d'un cluster correspond au nom d'hôte de l'ordinateur du premier CMS que vous installez.

Informations associées

Modification du nom d'un cluster de CMS [page 445]

11.7.1.1 Ajout d'un CMS à un cluster

Il existe plusieurs façons d'ajouter un nouveau membre à un cluster de CMS. Suivez la procédure appropriée :

- Vous pouvez installer un nouveau nœud avec un CMS sur un nouvel ordinateur.
- Si vous possédez déjà un nœud avec des fichiers binaires de CMS, vous pouvez ajouter un nouveau serveur CMS à partir de la CMC.
- Si vous possédez déjà un nœud avec les fichiers binaires de CMS, vous pouvez également ajouter un nouveau serveur CMS en clonant un serveur CMS existant.

> ⓘ Remarque
>
> Réalisez une copie de sauvegarde de la base de données système du CMS, de la configuration du serveur et du contenu de vos Input et Output File Repositories avant d'apporter une quelconque modification. Si nécessaire, contactez l'administrateur de votre base de données.

Informations associées

Ajout d'un nœud à un cluster [page 444]
Ajout d'un serveur [page 437]
Clonage des serveurs [page 438]
Présentation de la sauvegarde et de la restauration [page 565]

11.7.1.2 Ajout d'un nœud à un cluster

Lorsque vous ajoutez un nœud (un nœud est un ensemble de serveurs de la plateforme de BI gérés par un unique Server Intelligence Agent), vous êtes invité à créer un CMS ou à mettre en cluster le nœud vers un CMS existant.

Si vous souhaitez ajouter un nœud à un cluster sur un CMS existant, vous pouvez également utiliser le programme d'installation. Exécutez le programme d'installation de la plateforme de BI sur l'ordinateur où vous souhaitez installer le nouveau membre du cluster de CMS. Le programme d'installation vous permet de procéder à une installation personnalisée. Au cours de l'installation personnalisée, indiquez le nom du CMS existant dont vous souhaitez développer le système, puis sélectionnez les composants à installer sur l'ordinateur local. Dans ce cas, indiquez le nom du CMS en cours d'exécution sur votre système existant, choisissez d'installer un nouveau CMS sur l'ordinateur local et fournissez au programme d'installation les informations nécessaires pour qu'il se connecte à la base de données du CMS existant. Lorsque le programme d'installation installe le nouveau CMS sur l'ordinateur local, il ajoute automatiquement le serveur au cluster existant.

> **Remarque**
>
> Avant de mettre en cluster un nouveau nœud sur un CMS existant, si le nouveau nœud est un nouveau serveur, assurez-vous que l'installation de la plateforme de BI sur ce serveur se trouve au même niveau de correctif que l'environnement de la plateforme de BI existante.

> **Remarque**
>
> Les licences Edge BI et Crystal Server n'autorisent pas la mise en cluster ou le déploiement de nœuds multiples. Toutefois, à partir de Edge BI 4.3 SP2 et Crystal Server 2020 SP2, si Edge BI et Crystal Server sont déployés sous Linux, le nœud One Windows avec les services Crystal Reports 2020 est autorisé. Pour en savoir plus, voir Comment distribuer les services SAP Crystal Reports 2020 sur un serveur Windows.

Informations associées

Utilisation des nœuds [page 480]

11.7.1.3 Ajout de clusters aux fichiers de propriétés d'application Web

Si vous avez ajouté des CMS supplémentaires à votre déploiement, ces informations sont alors saisies dans le fichier `clusterinfo.1400.properties` disponible à l'emplacement `C:/Users/<you_user>/.businessobjects`. Le fichier est généré ou mis à jour lorsque vous redémarrez le SIA.

> **Remarque**
>
> Dans un déploiement Tomcat autonome, le fichier `clusterinfo.1400.properties` est généré seulement lorsque vous vous connectez avec l'un des noms du CMS. Lorsque vous mettez à jour le cluster,

le fichier dans un déploiement Tomcat autonome n'est pas mis à jour. Vous devez copier le fichier depuis votre CMS sur votre ordinateur Tomcat.

11.7.1.4 Modification du nom d'un cluster de CMS

Cette procédure vous permet de modifier le nom d'un cluster déjà installé. Une fois le nom du cluster de CMS modifié, le Server Intelligence Agent reconfigure automatiquement chaque serveur SAP Business Objects afin qu'il soit enregistré auprès du cluster, plutôt qu'auprès d'un CMS donné.

> **Remarque**
>
> Pour les administrateurs expérimentés de la plateforme de BI, notez que vous ne pouvez plus utiliser l'option `-ns` sur la ligne de commande du serveur pour configurer le CMS avec lequel un serveur doit s'enregistrer. Cette procédure est désormais gérée automatiquement par le SIA.

11.7.1.4.1 Pour modifier le nom d'un cluster sous Windows

1. Utilisez le CCM pour arrêter le Server Intelligence Agent pour le nœud contenant le Central Management Server membre du cluster dont vous voulez modifier le nom.
2. Cliquez avec le bouton droit sur le Server Intelligence Agent et choisissez *Propriétés*.
3. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet *Configuration*.
4. Cochez la case *Changer nom de cluster en*.
5. Saisissez le nouveau nom du cluster.
6. Cliquez sur *OK*, puis redémarrez le Server Intelligence Agent.

   Le nom du cluster de CMS a changé. Tous les autres membres de cluster de CMS sont dynamiquement informés du nouveau nom de cluster (cependant cela peut prendre quelques minutes avant que vos modifications n'arrivent aux membres du cluster).
7. Accédez à la zone de gestion *Serveurs* de la CMC et vérifiez que tous vos serveurs restent activés. Si nécessaire, activez les serveurs qui ont éventuellement été désactivés à la suite de vos modifications.

11.7.1.4.2 Pour modifier le nom d'un cluster sous UNIX

Utilisez le script `cmsdbsetup.sh`. Pour en savoir plus, voir la rubrique relative aux « scripts Unix » dans le chapitre Administration de la ligne de commande du *Guide d'administration de la plateforme de BI*.

Informations associées

Scripts UNIX [page 1113]

11.8 Gestion des groupes de serveurs

Les groupes de serveurs peuvent servir à organiser et gérer les serveurs de plateforme de BI sur votre système. Il est possible de sélectionner un serveur ou groupe de serveurs donné par publication (et non par utilisateur) et de regrouper des serveurs par région ou type.

Le regroupement de serveurs par région permet de configurer facilement des paramètres de traitement par défaut, des planifications récurrentes et des destinations de planification pour les utilisateurs qui travaillent dans un bureau régional spécifique. Vous pouvez associer un objet de rapport (un rapport Crystal ou un document Web Intelligence) à un groupe de serveurs unique de manière à ce que l'objet soit toujours traité par les mêmes serveurs. Il est aussi possible d'associer des objets de rapports planifiés à un groupe de serveurs donné pour s'assurer que les objets planifiés seront envoyés aux imprimantes ou serveurs de fichiers appropriés. Les groupes de serveurs se révèlent particulièrement utiles pour la maintenance des systèmes qui couvrent plusieurs emplacements et plusieurs fuseaux horaires.

Les groupes de serveurs se révèlent particulièrement utiles pour la maintenance des systèmes qui couvrent plusieurs emplacements et plusieurs fuseaux horaires. Vous pouvez, par exemple, utiliser des groupes de serveurs pour personnaliser votre système de plateforme de BI pour les rapports affichés dans différents endroits et pour différents types de rapports. Lorsque vous organisez vos serveurs par région, vous pouvez effectuer les actions suivantes pour les groupes de serveurs :

- Configurer des paramètres de traitement par défaut
- Configurer des planifications récurrentes
- Configurer des destinations de planification pour les utilisateurs qui travaillent dans un bureau régional spécifique.
- Associer un objet de rapport (tel qu'un rapport Crystal ou un document Web Intelligence) à un groupe de serveurs unique de manière à ce que l'objet soit toujours traité par les mêmes serveurs.
- Associer des objets planifiés à un groupe de serveurs particulier, afin de garantir que les objets planifiés soient envoyés sur les imprimantes correctes, les serveurs de fichiers corrects, etc.

Regroupez des serveurs par type lors de la configuration des objets à traiter par les serveurs optimisés pour ces objets.

Après la création des groupes de serveurs, configurez les objets pour qu'ils utilisent des groupes de serveurs spécifiques pour la planification ou la visualisation et la modification de rapports. Utilisez l'arborescence de navigation de la zone de gestion *Serveurs* de la CMC pour visualiser les groupes de serveurs. L'option *Liste des groupes de serveurs* affiche la liste des groupes de serveurs dans le volet *Détails*. L'option *Groupes de serveurs* permet de visualiser les serveurs appartenant au groupe.

Exemple : Regroupement des serveurs de traitement par type

Par exemple, les serveurs de traitement doivent communiquer fréquemment avec la base de données contenant les données des rapports publiés. Le fait de placer les serveurs de traitement près du serveur de base de données auquel ils doivent accéder améliore les performances du système et réduit au minimum le trafic réseau. Par conséquent, si de nombreux rapports doivent être exécutés par rapport à une base de données DB2, vous pouvez créer un groupe de serveurs de traitement qui traitent les rapports uniquement par rapport au serveur de base de données DB2. Pour améliorer les performances du système lors de la

visualisation des rapports, vous pouvez configurer les rapports de manière à toujours utiliser ce groupe de serveurs de traitement pour la visualisation.

11.8.1 Création d'un groupe de serveurs

Pour créer un groupe de serveurs, vous devez spécifier le nom et la description du groupe, puis ajouter des serveurs à ce groupe.

11.8.1.1 Pour créer un groupe de serveurs non exclusif

Les groupes de serveurs non exclusifs peuvent contenir des serveurs ou des groupes de serveurs qui font partie d'un autre groupe de serveurs non exclusif ou du pool courant du serveur.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Choisissez *Gérer* > *Nouveau* > *Créer des groupes de serveurs*.

   La boîte de dialogue *Créer des groupes de serveurs* s'affiche.
3. Dans le champ *Nom*, saisissez un nom pour le nouveau groupe de serveurs.
4. Si vous souhaitez ajouter des informations concernant le groupe de serveurs, saisissez-les dans le champ *Description*.
5. Cliquez sur *OK*.
6. Dans la zone de gestion *Serveurs* , cliquez sur *Groupes de serveurs* dans l'arborescence de navigation et sélectionnez le nouveau groupe de serveurs.
7. Choisissez *Ajouter des membres* à partir du menu *Actions*.
8. Sélectionnez les serveurs que vous souhaitez ajouter à ce groupe, puis cliquez sur la flèche >.

   > → Conseil
   >
   > Utilisez la combinaison `CTRL` + `+clic` pour sélectionner plusieurs serveurs.

   > ⓘ Remarque
   >
   > Les serveurs listés comprennent uniquement les serveurs qui ne font pas partie d'un autre groupe de serveurs exclusifs.
9. Cliquez sur *OK*.

   La zone de gestion *Serveurs* s'affiche de nouveau et répertorie maintenant tous les serveurs que vous avez ajoutés au groupe. Vous pouvez à présent modifier le statut, afficher les performances des serveurs et modifier les propriétés des serveurs du groupe.

11.8.1.2 Pour créer un groupe de serveurs exclusif

Les groupes de serveurs exclusifs contiennent des serveurs ou des groupes de serveurs qui ne font pas partie d'un autre groupe de serveurs ou du pool courant du serveur. Lorsqu'un groupe de serveurs est créé comme

groupe de serveurs exclusif, les serveurs faisant partie de ce groupe ne peuvent pas être affectés à aucun autre groupe de serveurs (exclusif ou non exclusif) et les serveurs ajoutés à un groupe de serveurs exclusifs sont exclus du pool courant. Vous pouvez ainsi créer des groupes de serveurs isolés du chargement général du système BI.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Choisissez *Gérer* > *Nouveau* > *Créer des groupes de serveurs*.

   La boîte de dialogue *Créer des groupes de serveurs* s'affiche.
3. Dans le champ *Nom*, saisissez un nom pour le nouveau groupe de serveurs.
4. Si vous souhaitez ajouter des informations concernant le groupe de serveurs, saisissez-les dans le champ *Description*.
5. Cochez la case *Groupe de serveurs exclusif*.

   > **Remarque**
   >
   > Il est possible de créer un groupe de serveurs exclusif uniquement au niveau racine. Dans le cas d'un nœud enfant, vous pouvez créer un groupe de serveurs exclusif uniquement si le groupe de serveurs racine ou parent est exclusif.
   >
   > > **Exemple**
   > >
   > > Prenons l'exemple du scénario suivant pour mieux comprendre les groupes de serveurs exclusifs.
   > >
   > > Deux Job Servers : JS1 et JS2 font partie du pool courant de serveur.
   > >
   > > Vous créez un groupe de serveurs exclusif : SG1.
   > >
   > > Vous ajoutez JS1 à SG1.
   > >
   > > Vous planifiez le document en sélectionnant l'option *Utiliser uniquement les serveurs dans le groupe sélectionné*.
   > >
   > > En partant du principe que JS1 et JS2 ont déjà des travaux en cours d'exécution.
   > >
   > > **Résultat :** JS1 est déjà chargé avec des travaux qui doivent être traités. Cependant, JS1 faisant désormais partie de SG1, JS1 reçoit uniquement les requêtes de traitement de workflows affectés à SG1. En d'autres termes, JS1 est libéré du chargement du système général.
6. Cliquez sur *OK*.
7. Dans la zone de gestion *Serveurs* , cliquez sur *Groupes de serveurs* dans l'arborescence de navigation et sélectionnez le nouveau groupe de serveurs.
8. Choisissez *Ajouter des membres* à partir du menu *Actions*.
9. Sélectionnez les serveurs que vous souhaitez ajouter à ce groupe, puis cliquez sur la flèche >.

   > **Conseil**
   >
   > Utilisez la combinaison `CTRL` + `+clic` pour sélectionner plusieurs serveurs.

   > **Remarque**
   >
   > Les serveurs listés comprennent uniquement les serveurs qui ne font pas déjà partie d'autres groupes de serveurs ou du pool courant de serveur.

10. Cliquez sur *OK*.

    La zone de gestion *Serveurs* s'affiche de nouveau et répertorie maintenant tous les serveurs que vous avez ajoutés au groupe. Vous pouvez à présent modifier le statut, afficher les performances des serveurs et modifier les propriétés des serveurs du groupe.

11.8.2 Conversion d'un groupe de serveurs exclusif en groupe de serveurs non exclusif et vice versa.

11.8.2.1 Conversion d'un groupe de serveurs exclusif en groupe de serveurs non exclusif

Vous pouvez désormais modifier un groupe de serveurs exclusif existant afin de le rendre non exclusif.

Pour convertir un groupe de serveurs exclusif de niveau racine en groupe de serveurs non exclusif, agissez comme suit :

1. Cliquez avec le bouton droit sur le groupe de serveurs exclusif à convertir, puis sélectionnez *Propriétés* dans la liste déroulante.

   La boîte de dialogue *Propriétés* s'ouvre. Remarquez que la case *Groupe de serveurs exclusif* est cochée.
2. Décochez la case *Groupe de serveurs exclusif*.

   Un message d'avertissement apparaît.
3. Cliquez sur *OK* pour confirmer la conversion.
4. Cliquez sur *Enregistrer et fermer*.

   Vous venez de convertir un groupe de serveurs exclusif en groupe de serveurs non exclusif.

   > ⓘ Remarque
   >
   > Seul un groupe de serveurs exclusif de niveau racine peut être converti en groupe de serveurs non exclusif.

11.8.2.2 Conversion d'un groupe de serveurs non exclusif en groupe de serveurs exclusif

Vous pouvez désormais modifier un groupe de serveurs non exclusif existant afin de le rendre exclusif.

Pour convertir un groupe de serveurs non exclusif qui contient des serveurs et des groupes de serveurs **indépendants**, procédez comme suit :

1. Cliquez avec le bouton droit sur le groupe de serveurs non exclusif à convertir, puis sélectionnez *Propriétés* dans la liste déroulante.

La boîte de dialogue *Propriétés* s'ouvre. Remarquez que la case *Groupe de serveurs exclusif* n'est pas cochée.

2. Cochez la case *Groupe de serveurs exclusif*.

   Un message de réussite s'affiche.

3. Cliquez sur *OK*.
4. Cliquez sur *Enregistrer et fermer*.

   Vous venez de convertir un groupe de serveurs non exclusif en groupe de serveurs exclusif.

> ⓘ Remarque
>
> La conversion est possible uniquement pour un groupe de serveurs non exclusif comportant des serveurs et des groupes de serveurs indépendants. Les serveurs et les groupes de serveurs indépendants correspondent aux serveurs et groupes de serveurs ne faisant partie d'aucun autre groupe de serveurs.

11.8.3 Utilisation des sous-groupes de serveurs

Les sous-groupes de serveurs vous permettent de mieux organiser vos serveurs. Un sous-groupe est simplement un groupe de serveurs qui fait partie d'un autre groupe de serveurs.

Par exemple, si vous groupez des serveurs par région et par pays, chaque groupe régional devient un sous-groupe d'un groupe national. Pour organiser des serveurs de cette façon, créez tout d'abord un groupe pour chaque région et ajoutez les serveurs appropriés à chaque groupe régional. Puis créez un groupe pour chaque pays et ajoutez chaque groupe régional au groupe national correspondant.

Il existe deux façons de configurer les sous-groupes : vous pouvez modifier les sous-groupes d'un serveur ou rendre un groupe de serveurs membre d'un autre. Le résultat est le même, choisissez donc la méthode qui s'avère la plus pratique.

11.8.3.1 Pour ajouter des sous-groupes à un groupe de serveurs

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez sur *Groupes de serveurs* dans l'arborescence de navigation et sélectionnez le groupe de serveurs auquel vous souhaitez ajouter des sous-groupes.

   Ce groupe est le groupe parent.

3. Choisissez *Ajouter des membres* à partir du menu *Actions*.
4. Cliquez sur *Groupes de serveurs* dans l'arborescence de navigation, sélectionnez les groupes de serveurs que vous souhaitez ajouter à ce groupe, puis cliquez sur la flèche >.

> → Conseil
>
> Utilisez la combinaison `CTRL` + `+clic` pour sélectionner plusieurs groupes de serveurs.

5. Cliquez sur *OK*.

   La zone de gestion *Serveurs* s'affiche de nouveau et répertorie maintenant tous les groupes de serveurs que vous avez ajoutés au groupe parent.

11.8.3.2 Pour qu'un groupe de serveurs soit membre d'un autre groupe

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez sur le groupe que vous souhaitez ajouter à un autre groupe.

   > ⓘ Remarque
   >
   > Pour le niveau racine, tous les groupes de serveurs exclusifs sont répertoriés sous *Groupes de serveurs disponibles*. Vous pouvez uniquement sélectionner un groupe de serveurs exclusif et le déplacer vers *Membre des groupes de serveurs*, puisqu'un groupe de serveurs exclusif ne peut avoir qu'un seul groupe de serveurs parent.
   >
   > Les groupes de serveurs exclusifs de niveau enfant ne répertorient aucun groupe de serveurs sous *Groupes de serveurs disponibles*, puisqu'un groupe de serveurs exclusif enfant ne peut avoir qu'un seul parent.

3. Choisissez *Ajouter à un groupe de serveurs* dans le menu *Actions*.
4. Dans la liste *Groupes de serveurs disponibles*, sélectionnez les autres groupes auxquels vous souhaitez ajouter le groupe, puis cliquez sur >.

   > → Conseil
   >
   > Utilisez la combinaison `CTRL` + `+ clic` pour sélectionner plusieurs groupes de serveurs.

5. Cliquez sur *OK*.

11.8.4 Modification de l'appartenance d'un serveur à un groupe

Vous pouvez modifier l'appartenance d'un serveur à un groupe en ajoutant ou en supprimant le serveur d'un groupe ou sous-groupe préalablement créé sur le système.

Par exemple, supposons que vous ayez créé des groupes de serveurs pour un certain nombre de régions. Vous pouvez souhaiter utiliser un seul et même CMS (Central Management Server) pour plusieurs régions. Au lieu d'ajouter le CMS individuellement à chaque groupe de serveurs régional, vous pouvez cliquer sur le lien *Membre de* du serveur pour l'ajouter aux trois régions en même temps.

11.8.4.1 Pour modifier l'appartenance d'un serveur à un groupe

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez avec le bouton droit de la souris sur le serveur dont vous souhaitez modifier les informations d'appartenance et sélectionnez *Groupes de serveurs existants*.
   Dans le panneau Détails, la liste *Groupes de serveurs disponibles* affiche les groupes auxquels vous pouvez ajouter le serveur. La liste *Membre des groupes de serveurs* affiche tous les groupes de serveurs auquel le serveur appartient actuellement.

   > **Remarque**
   >
   > Pour le niveau racine, tous les groupes de serveurs exclusifs sont répertoriés sous *Groupes de serveurs disponibles*. Vous pouvez uniquement sélectionner un groupe de serveurs exclusif et le déplacer vers *Membre des groupes de serveurs*, puisqu'un groupe de serveurs exclusif ne peut avoir qu'un seul groupe de serveurs parent. Après avoir sélectionné un groupe de serveurs exclusif dans la liste *Groupes de serveurs disponibles* et l'avoir déplacé dans *Membre des groupes de serveurs*, le groupe de serveurs exclusif est déplacé de son groupe de serveurs racine vers un nouveau groupe auquel il est mappé.
   >
   > Pour les groupes de serveurs enfants, les groupes de serveurs parents existants sont affichés sous *Membre des groupes de serveurs* et les autres groupes de serveurs exclusifs sont répertoriés sous *Groupes de serveurs disponibles*. Il est possible de modifier le mappage d'un groupe de serveurs enfant d'un groupe parent exclusif à un autre.
3. Pour modifier les groupes auxquels le serveur appartient, utilisez les flèches pour déplacer les groupes de serveurs entre les listes, puis cliquez sur *OK*.

> **Remarque**
>
> L'option *Supprimer d'un groupe de serveurs* est répertoriée uniquement pour les groupes de serveurs exclusifs de niveau enfant. Une fois qu'un groupe de serveurs exclusif de niveau enfant est supprimé du groupe de serveurs parent, il conserve son exclusivité et peut être déplacé au niveau racine.
>
> Les groupes de serveurs apparaissent dans la zone de lancement de BI si les droits de sécurité utilisateur sont octroyés par l'administrateur depuis la CMC pour des groupes de serveurs spécifiques.

11.8.5 Accès en administration à un serveur ou à un groupe de serveurs accordé aux utilisateurs

L'octroi de l'accès en administration à des utilisateurs leur permet d'effectuer des tâches sur les serveurs ou groupes de serveurs, telles que le démarrage et l'arrêt des serveurs.

Selon les configurations système et la politique de sécurité, la gestion des serveurs peut être exclusivement réservée à l'administrateur de la plateforme de BI ou l'accès en administration peut être accordé à d'autres utilisateurs qui utilisent ces serveurs. De nombreuses organisations disposent d'un groupe de professionnels de l'informatique qui se consacre à la gestion des serveurs. Si votre équipe chargée de la gestion des serveurs doit régulièrement réaliser des tâches de maintenance qui l'amènent à arrêter et à démarrer les serveurs, vous devez lui accorder des droits en administration sur les serveurs. Vous souhaiterez peut-être également

déléguer des tâches d'administration de serveurs de la plateforme de BI à d'autres utilisateurs ou faire en sorte que certains groupes de votre organisation puissent contrôler leur propre gestion des serveurs.

> **Remarque**
>
> Vous pouvez sélectionner un serveur ou un groupe de serveurs pour une publication (pas pour un utilisateur spécifique). Cependant, vous pouvez affecter des droits en administration à des utilisateurs ou groupes d'utilisateurs pour un serveur ou groupe de serveurs donné.

11.8.5.1 Octroi de droits d'accès en administration à un serveur ou à un groupe de serveurs

Vous pouvez affecter des droits en administration à des utilisateurs ou groupes d'utilisateurs pour un serveur ou groupe de serveurs donné.

> **Remarque**
>
> Vous pouvez sélectionner un serveur ou un groupe de serveurs pour une publication (pas pour un utilisateur).

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez avec le bouton droit de la souris sur le serveur ou le groupe de serveurs auquel vous souhaitez accorder les droits d'accès en administration et sélectionnez *Sécurité de l'utilisateur*.
3. Cliquez sur *Ajouter des utilisateurs/groupes principaux* pour ajouter les utilisateurs ou les groupes pour lesquels vous voulez accorder les droits d'administration au serveur ou groupe de serveurs.
4. Dans la boîte de dialogue *Ajouter des utilisateurs/groupes principaux*, sélectionnez un utilisateur ou un groupe pour lequel donner les droits d'administration au serveur ou groupe de serveurs, puis cliquez sur >.
5. Cliquez sur *Ajouter et affecter la sécurité*.
6. Dans l'écran *Affecter la sécurité*, sélectionnez les paramètres de sécurité à affecter à l'utilisateur ou au groupe puis cliquez sur *OK*.

Informations associées

Fonctionnement des droits sur la plateforme de BI [page 128]

11.8.5.2 Droits d'accès aux objets du Report Application Server

Pour autoriser les utilisateurs à créer ou modifier des rapports sur le Web via le RAS (Report Application Server), vous devez posséder des licences RAS Report Modification disponibles sur votre système. Vous devez également accorder aux utilisateurs un minimum de droits d'accès aux objets. Lorsque vous accordez aux

utilisateurs ces droits pour un objet rapport, ils peuvent sélectionner le rapport comme source de données d'un nouveau rapport ou modifier le rapport directement.

- Visualiser les objets (ou « Afficher les instances du document », le cas échéant)
- Modifier les objets
- Actualiser les données du rapport
- Exporter les données du rapport

Les utilisateurs doivent également avoir les droits permettant d'ajouter des objets à au moins un dossier avant de pouvoir enregistrer les nouveaux rapports sur la plateforme de BI.

Pour que les utilisateurs conservent la possibilité d'effectuer des tâches supplémentaires (telles que copier, planifier, imprimer des rapports, etc.), il est recommandé de commencer par attribuer le niveau d'accès approprié et de mettre à jour vos modifications. Modifiez ensuite le niveau d'accès en sélectionnant Avancés et ajoutez tous les droits non encore accordés. Par exemple, si les utilisateurs détiennent déjà les droits Visualiser à la demande pour un rapport, vous pouvez les autoriser à modifier le rapport en sélectionnant le niveau d'accès Avancés et en leur octroyant les droits Modifier les objets.

Lorsque les utilisateurs visualisent les rapports via le visualiseur DHTML avancé et le RAS, le niveau d'accès Visualiser est suffisant pour afficher le rapport, mais Visualiser à la demande est nécessaire pour utiliser les fonctions de recherche avancée. Le droit supplémentaire Modifier les objets n'est pas obligatoire.

11.8.6 Mappage d'un groupe d'utilisateurs à un groupe de serveurs

Vous pouvez désormais mapper un groupe d'utilisateurs à un groupe de serveurs donné grâce à l'option *Paramètres par défaut*.

Pour mapper un groupe d'utilisateurs à un groupe de serveurs, réalisez les étapes suivantes :

1. Connectez-vous à la CMC
2. Sélectionnez *Utilisateurs et groupes*.
3. Dans la page *Utilisateurs et groupes*, cliquez avec le bouton droit sur le groupe d'utilisateurs à mapper au groupe de serveurs.
4. Sélectionnez *Paramètres par défaut*.
5. Dans la page *Groupe de serveurs de planification*, définissez les serveurs par défaut à utiliser pour planifier le groupe d'utilisateurs.

   Vous pouvez sélectionner l'une des options suivantes :

   - (Par défaut) Sélectionnez *Utiliser le premier serveur disponible* pour exécuter l'objet sur le serveur ayant le plus de ressources disponibles au moment de la planification.
   - Sélectionnez *Accorder la priorité aux serveurs figurant dans le groupe sélectionné* pour exécuter l'objet sur les serveurs dans un groupe de serveurs donné. Puis sélectionnez le groupe de serveurs requis dans la liste déroulante pour définir une préférence pour un groupe de serveurs donné. Si aucun serveur du groupe de serveurs sélectionné n'est disponible, l'objet est exécuté sur le prochain serveur disponible du pool courant de serveur.
   - Sélectionnez *Utiliser uniquement les serveurs dans le groupe sélectionné* pour exécuter l'objet uniquement sur les serveurs dans un groupe de serveurs donné puis sélectionnez le groupe de

serveurs requis dans la liste déroulante pour utiliser exclusivement un groupe de serveurs. Si aucun serveur du groupe sélectionné n'est disponible, l'objet n'est pas traité. Par ailleurs, si un Job Server n'est pas présent dans le groupe de serveurs affecté, le Job conserve le statut En Suspens.

Remarque

Vous pouvez choisir de mapper un groupe de serveurs exclusif ou non exclusif à un groupe d'utilisateurs en cochant une des deux cases d'option : *Accorder la priorité aux serveurs figurant dans le groupe sélectionné* ou *Utiliser uniquement les serveurs dans le groupe sélectionné*.

De la même façon, vous pouvez affecter des groupes de serveurs pour l'affichage ou le traitement des rapports Crystal Reports et des documents Web Intelligence en accédant à *Paramètres par défaut*, puis respectivement *Paramètres de traitement Crystal Reports* et *Paramètres de processus Web Intelligence*.

Si un groupe de serveurs est associé comme requis, cela signifie que **seuls** les serveurs de ce groupe de serveurs donné sont utilisés. Les serveurs du pool courant ne sont pas utilisés. Si un groupe de serveurs est associé comme privilégié, alors les serveurs du pool de serveur courant sont utilisés si les serveurs dans le groupe de serveurs sont occupés. Le pool courant de serveur comprend tous les serveurs qui ne font pas partie d'un groupe de serveurs exclusif. Pour en savoir plus sur les groupes de serveurs exclusif, voir Pour créer un groupe de serveurs exclusif [page 447].

L'affectation d'un groupe de serveurs à un groupe d'utilisateurs peut être complexe, puisqu'un seul utilisateur peut faire partie de plusieurs groupes d'utilisateurs, Et que chaque groupe d'utilisateurs peut être mappé à des groupes de serveurs différents. Chaque groupe de serveurs peut être affecté en tant que requis ou privilégié.

Exemple

Prenons l'exemple du scénario suivant :

Un utilisateur (U) fait partie de deux groupes d'utilisateurs, à savoir UG1 et UG2. Et chaque groupe d'utilisateurs est mappé à un groupe de serveurs différent, à savoir SG1 et SG2. Alors les résultats pour les différents scénarios seraient :

Scénario	Résultat
Vous planifiez un document (D). Le groupe de serveurs 1 (SG1) est défini sur UG1 et le groupe de serveurs 2 (SG2) est défini sur UG2. SG1 est défini sur Requis (R). SG2 est également défini sur Requis (R). Aucun groupe de serveurs n'est affecté au niveau du document (D).	La combinaison des deux groupes de serveurs (SG1 et SG2) agit comme un groupe de serveurs Requis (R). Étant donné que les deux groupes de serveurs (SG1 et SG2) sont définis sur Requis, les serveurs du pool courant ne sont PAS utilisés.
Vous planifiez un document (D). Le groupe de serveurs 1 (SG1) est défini sur UG1 et le groupe de serveurs 2 (SG2) est défini sur UG2. SG1 est défini sur Privilégié (P). SG2 est également défini sur Privilégié (P).	La combinaison des deux groupes de serveurs (SG1 et SG2) agit comme un groupe de serveurs Privilégié (P). Étant donné que les deux groupes de serveurs (SG1 et SG2) sont définis sur Privilégié, si aucun des serveurs des groupes sélectionnés n'est disponible, les serveurs du pool courant sont utilisés.

Scénario	Résultat
Aucun groupe de serveurs n'est affecté au niveau du document (D).	
Vous planifiez un document (D). Le groupe de serveurs 1 (SG1) est défini sur UG1 et le groupe de serveurs 2 (SG2) est défini sur UG2. SG1 est défini sur Requis (R). SG2 est défini sur Privilégié (P). Aucun groupe de serveurs n'est affecté au niveau du document (D).	La combinaison des deux groupes de serveurs (SG1 et SG2) agit comme un groupe de serveurs Requis (R). Étant donné que la combinaison (SG1 et SG2) agit comme un groupe de serveurs Requis (R), les serveurs du pool courant ne sont PAS utilisés.

6. Cliquez sur *Enregistrer et fermer*.

   Vous venez de mapper un groupe d'utilisateurs à un groupe de serveurs.

Remarque

- Un utilisateur peut appartenir à un ou plusieurs groupes d'utilisateurs et chacun de ces groupes d'utilisateurs peut appartenir à d'autres groupes d'utilisateurs. Si aucun groupe de serveurs n'est associé au groupe d'utilisateurs immédiat auquel un utilisateur appartient, alors le programme vérifie si un groupe de serveurs est associé au niveau des groupes d'utilisateurs suivant. Ce processus se poursuit jusqu'à ce que le programme trouve un groupe d'utilisateurs auquel un groupe de serveurs est affecté. Lorsque le programme trouve un groupe de serveurs associé au niveau du groupe d'utilisateurs, il s'arrête pour approfondir la vérification. Si plusieurs groupes de serveurs sont associés au niveau du groupe d'utilisateurs, le comportement de la combinaison des deux groupes de serveurs (comme expliqué dans le tableau ci-dessus) est pris en compte. Prenons l'exemple du scénario suivant pour comprendre l'affectation du groupe de serveurs :

  #### Exemple

  Scénario : Vous planifiez le document.

  L'utilisateur (U) appartient à deux groupes d'utilisateurs, à savoir UG1 et UG2. Cependant, aucun groupe de serveurs n'est affecté à UG1 et à UG2.

  UG1 appartient au groupe d'utilisateurs 3 (UG3) et UG2 appartient au groupe d'utilisateurs 4 (UG4).

  Le groupe de serveurs 3 (SG3) est défini sur UG3.

  SG3 est défini sur Requis (R).

  Résultat : Étant donné qu'aucun groupe de serveurs n'est défini au premier niveau (UG1 et UG2), le programme vérifie s'il existe des groupes de serveurs définis au niveau suivant (UG3 et UG4). Étant donné que SG3 est défini sur UG3 et que SG3 est défini sur Requis, seuls les serveurs dans SG3 sont utilisés pour traiter l'objet et les serveurs du pool courant ne peuvent pas être utilisés.

  Cela signifie que si aucun groupe de serveurs n'est défini au niveau du groupe d'utilisateurs, le programme vérifie alors le niveau suivant immédiat pour voir si les groupes de serveurs sont

définis. Si le programme identifie qu'un groupe de serveurs est défini sur n'importe quel niveau de groupe d'utilisateurs, le programme arrête de vérifier les groupes de serveurs au niveau suivant.

- Au niveau du document, il ne peut y avoir qu'un seul groupe de serveurs qui peut être affecté et il peut être Requis ou Privilégié. Toutefois, un utilisateur peut appartenir à un ou plusieurs groupes d'utilisateurs et cela peut entraîner l'affectation de plusieurs groupes de serveurs à un utilisateur. Si un groupe de serveurs est défini au niveau du document (D) et du groupe d'utilisateurs (UG), l'association du groupe de serveurs au niveau du document est alors toujours envisagée par rapport à l'association du groupe de serveurs au niveau du groupe d'utilisateurs. Prenons l'exemple du scénario suivant pour comprendre l'affectation du groupe de serveurs :

  Exemple

  Scénario : Vous planifiez le document.

  Le groupe de serveurs 1 (SG1) est défini sur D et SG1 est défini sur Requis.

  Le groupe de serveurs 2 (SG2) est défini sur UG et SG2 est défini sur Privilégié.

  Résultat : SG1 est utilisé. Lorsque SG1 est défini sur Requis, les serveurs du pool courant ne peuvent pas être utilisés.

  Étant donné que le groupe de serveurs (SG1) est déjà défini au niveau du document (D), le programme ignore l'affectation du groupe de serveurs au niveau du groupe d'utilisateurs. Cela implique que l'affectation du groupe de serveurs au niveau du document soit envisagée par rapport à l'affectation du groupe de serveurs au niveau du groupe d'utilisateurs.

- Vous devez vous assurer que tous les serveurs requis font partie du groupe de serveurs.
- Pour en savoir plus sur l'affectation des groupes de serveurs au niveau du dossier et du groupe d'utilisateurs, consultez https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

11.8.7 Mappage d'un dossier à un groupe de serveurs

Vous pouvez désormais mapper un dossier à un groupe de serveurs donné grâce à l'option *Paramètres par défaut*.

Pour mapper un dossier à un groupe de serveurs, réalisez les étapes suivantes :

1. Connectez-vous à la CMC.
2. Accédez à *Dossiers* et cliquez avec le bouton droit de la souris sur le dossier souhaité (auquel vous voulez mapper le groupe de serveurs).
3. Sélectionnez *Paramètres par défaut*.
4. Dans la page *Groupe de serveurs de planification*, définissez les serveurs par défaut à utiliser pour la planification au niveau du dossier.

   Vous pouvez sélectionner l'une des options suivantes :

   - (Par défaut) Sélectionnez *Utiliser le premier serveur disponible* pour exécuter l'objet sur le serveur ayant le plus de ressources disponibles au moment de la planification.

- Sélectionnez *Accorder la priorité aux serveurs figurant dans le groupe sélectionné* pour exécuter l'objet sur les serveurs dans un groupe de serveurs donné. Puis sélectionnez le groupe de serveurs requis dans la liste déroulante pour définir une préférence pour un groupe de serveurs donné. Si aucun serveur du groupe de serveurs sélectionné n'est disponible, l'objet est exécuté sur le prochain serveur disponible du pool courant de serveur.
- Sélectionnez *Utiliser uniquement les serveurs dans le groupe sélectionné* pour exécuter l'objet uniquement sur les serveurs dans un groupe de serveurs donné puis sélectionnez le groupe de serveurs requis dans la liste déroulante pour utiliser exclusivement un groupe de serveurs. Si aucun serveur du groupe sélectionné n'est disponible, l'objet n'est pas traité.

> **Remarque**
>
> Vous pouvez choisir de mapper un groupe de serveurs exclusif ou non exclusif à un dossier en cochant une des deux cases d'option : *Donner la préférence aux serveurs appartenant au groupe sélectionné* ou *Utiliser uniquement les serveurs appartenant au groupe sélectionné*.
>
> De la même façon, vous pouvez affecter des groupes de serveurs pour l'affichage ou le traitement des rapports Crystal Reports et des documents Web Intelligence en accédant à *Paramètres par défaut*, puis respectivement *Paramètres de traitement Crystal Reports* et *Paramètres de processus Web Intelligence*.
>
> Si un groupe de serveurs est associé comme requis, cela signifie que **seuls** les serveurs de ce groupe de serveurs donné sont utilisés. Les serveurs du pool courant ne sont pas utilisés. Si un groupe de serveurs est associé comme privilégié, alors les serveurs du pool de serveur courant sont utilisés si les serveurs dans le groupe de serveurs sont occupés. Le pool courant de serveur comprend tous les serveurs qui ne font pas partie d'un groupe de serveurs exclusif. Pour en savoir plus sur les groupes de serveurs exclusif, voir Pour créer un groupe de serveurs exclusif [page 447].

5. Cliquez sur *Enregistrer et fermer*.

   Vous venez de mapper un dossier à un groupe de serveurs.

> **Remarque**
>
> - Au niveau du dossier ou du document, il ne peut y avoir qu'un seul groupe de serveurs qui peut être affecté et il peut être Requis ou Privilégié. Si un groupe de serveurs est défini au niveau du dossier, du document et du groupe d'utilisateurs, l'association du groupe de serveurs au niveau du document est alors toujours envisagée par rapport à l'association du groupe de serveurs au niveau du dossier, suivie par l'association du groupe de serveurs au niveau du groupe d'utilisateurs. Par conséquent, l'ordre de priorité pour l'affectation des groupes de serveurs se présente comme suit : **Document > Dossier > Groupe d'utilisateurs**
> - Un document peut appartenir à un dossier qui peut, à son tour, appartenir à un autre dossier parent. Étant donné qu'aucun groupe de serveurs n'est affecté au niveau du document, si aucun groupe de serveurs n'est associé au dossier immédiat auquel un document appartient, alors le programme vérifie si un groupe de serveurs est associé au dossier parent immédiat suivant. Ce processus se poursuit jusqu'à ce que le programme trouve un dossier parent auquel un groupe de serveur est affecté. Lorsque le programme trouve un groupe de serveurs associé au niveau du dossier, il s'arrête pour approfondir la vérification. Prenons l'exemple du scénario suivant pour comprendre l'affectation du groupe de serveurs :
>
> > **Exemple**
> >
> > **Scénario :** Vous planifiez le document.
> >
> > Cependant, aucun groupe de serveurs n'est affecté au niveau du document.

Le document appartient au dossier. Cependant, aucun groupe de serveurs n'est affecté au dossier.

Le dossier fait à son tour partie d'un autre dossier : Dossier parent. Le groupe de serveurs est défini au niveau du dossier parent.

Le groupe de serveurs est défini sur Requis.

Résultat : Étant donné qu'aucun groupe de serveurs n'est défini au niveau du document, le programme vérifie s'il existe des groupes de serveurs définis au niveau du dossier. À nouveau, étant donné qu'aucun groupe de serveurs n'est défini au niveau du dossier, le programme vérifie s'il existe des groupes de serveurs définis au niveau suivant : au niveau du dossier parent. Étant donné que le groupe de serveurs est défini sur Privilégié et que le groupe de serveurs est défini sur Requis, seuls les serveurs dans le groupe de serveurs sont utilisés pour traiter l'objet et les serveurs du pool courant ne peuvent pas être utilisés.

Cela signifie que si aucun groupe de serveurs n'est défini au niveau du document, le programme vérifie alors le dossier immédiat pour voir si les groupes de serveurs sont définis. Si le programme identifie qu'un groupe de serveurs est défini sur n'importe quel niveau de dossier, le programme arrête de vérifier les groupes de serveurs au niveau suivant.

De la même façon, si aucun groupe de serveurs n'est défini au niveau du document et qu'aucun groupe de serveurs n'est défini au niveau du dossier, alors le programme prend en compte l'affectation du groupe de serveurs au niveau du groupe d'utilisateurs.

- Vous devez vous assurer que tous les serveurs requis font partie du groupe de serveurs.
- Pour en savoir plus sur l'affectation des groupes de serveurs au niveau du dossier et du groupe d'utilisateurs, consultez https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

11.8.8 Présentation de la gestion des droits sur le groupe de serveurs

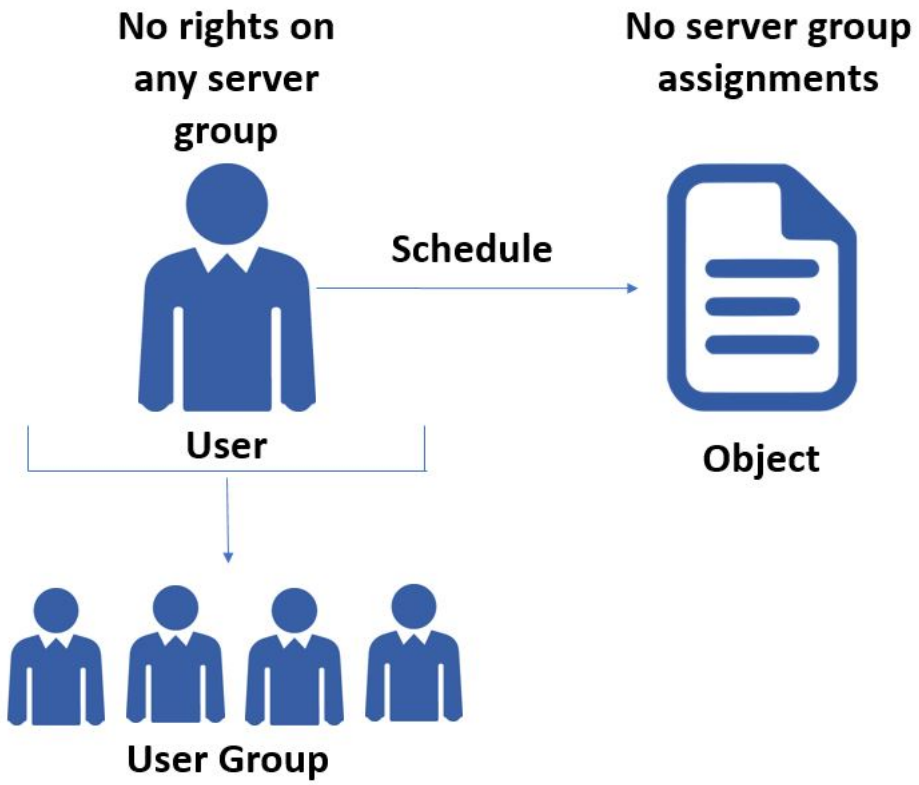
Vous pouvez activer des droits d'accès pour les groupes de serveurs au niveau de l'utilisateur ou du groupe d'utilisateurs. En d'autres termes, vous pouvez contrôler l'accès aux groupes de serveurs pour chaque utilisateur ou groupe d'utilisateurs.

ⓘ Remarque

- Les scénarios mentionnés ci-dessous utilisent un processus de planification pour illustrer la gestion des droits sur le groupe de serveurs. De même, vous pouvez comprendre la gestion des droits sur le groupe de serveurs pour l'affichage ou le masquage.
- Vous pouvez planifier un objet si les serveurs sont disponibles dans un groupe de serveurs ou dans une combinaison de groupes de serveurs. La planification échoue lorsque aucun serveur n'est disponible.

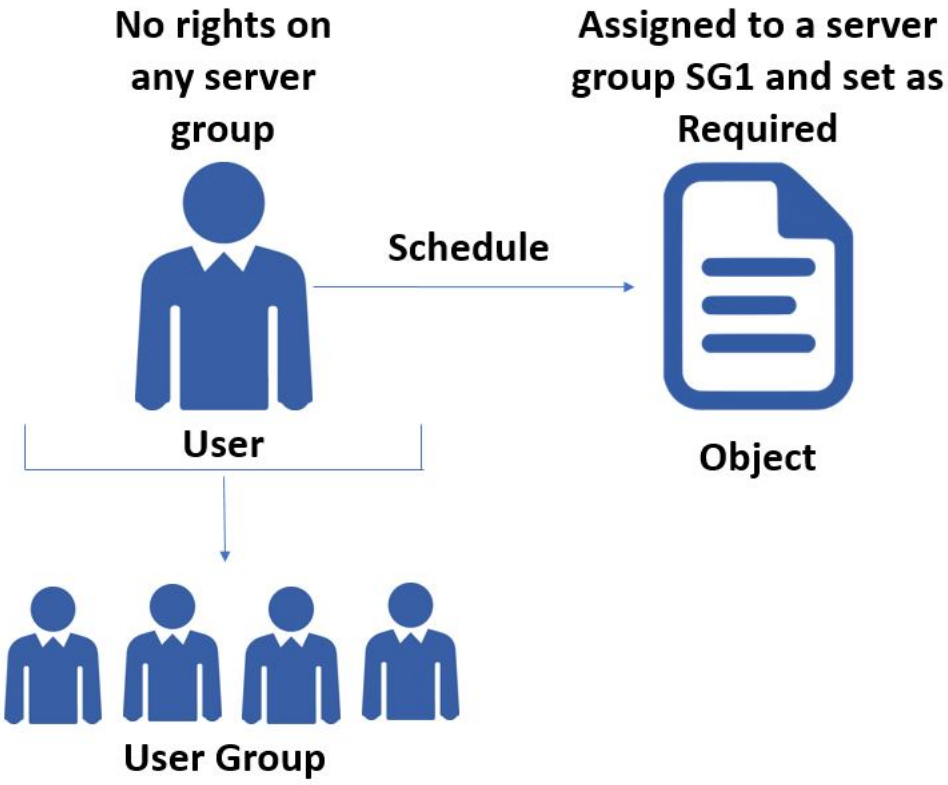
Scénario 1 :

Dans un scénario idéal, l'utilisateur fait partie d'un groupe d'utilisateurs dans la plateforme Business Intelligence. L'utilisateur et le groupe d'utilisateurs qui lui est associé ne disposent d'aucun droit sur aucun groupe de serveurs. L'utilisateur souhaite maintenant planifier un objet qui n'est affecté à aucun groupe de serveurs.



Scénario 2 :

Lorsque vous modifiez le scénario ci-dessus en affectant un groupe de serveurs à l'objet, la planification de l'objet échoue.



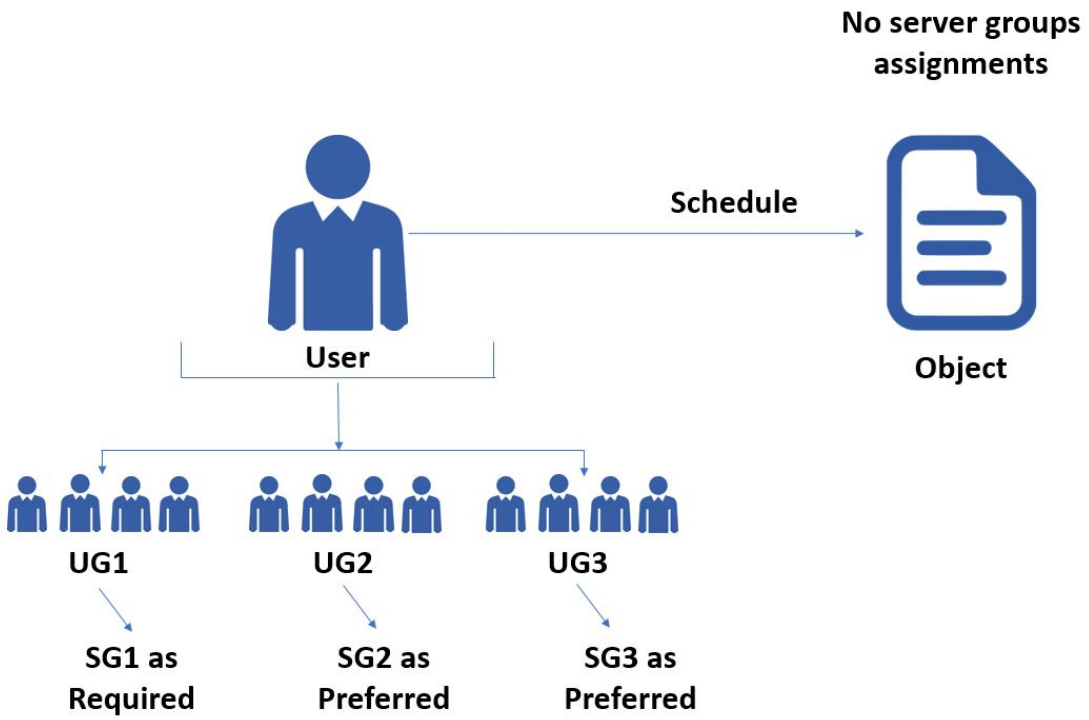
Lorsqu'un utilisateur planifie un objet, la plateforme vérifie les groupes de serveurs affectés à l'objet. Si un groupe de serveurs est affecté à l'objet, la plateforme vérifie que l'utilisateur dispose de droits d'affichage pour le groupe de serveurs.

Dans le deuxième scénario, l'utilisateur et le groupe d'utilisateurs qui lui est associé ne disposent d'aucuns droits sur le groupe de serveurs SG1. Cela entraîne l'échec du travail de planification. Pour qu'un utilisateur planifie un objet avec succès dans ce scénario, assurez-vous que cet utilisateur ou l'un des groupes d'utilisateurs associés dispose de droits d'affichage pour le groupe de serveurs SG1.

Scénario 3 :

> ⓘ Remarque
>
> Pour les scénarios 3 et 4, nous partons du principe que l'utilisateur hérite des droits des groupes d'utilisateurs qui lui sont associés.

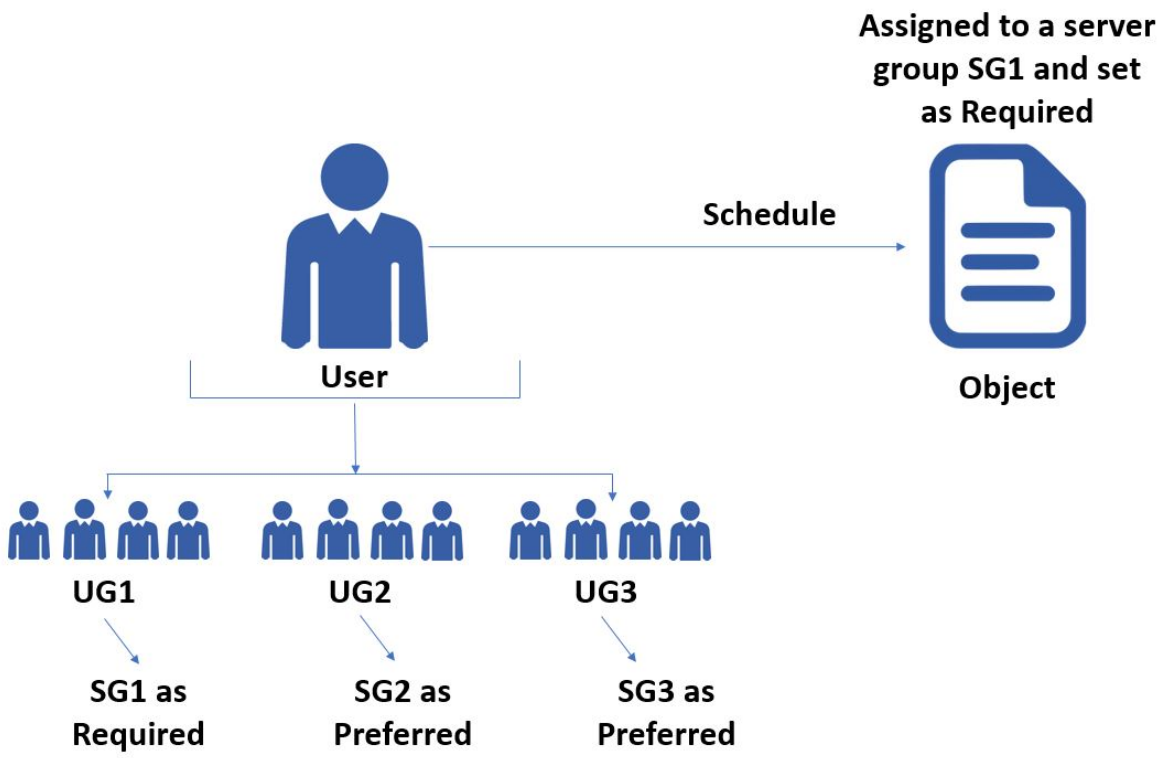
Un utilisateur appartient à trois groupes d'utilisateurs (UG1, UG2 et UG3) et vous avez mappé chaque groupe d'utilisateurs vers le groupe de serveurs SG1, SG2 et SG3 respectivement. Le groupe de serveurs SG1 est défini comme obligatoire et les groupes de serveurs SG2 et SG3 sont définis comme des groupes préférés. Pour plus d'informations sur la définition d'un groupe de serveurs comme obligatoire ou préféré, consultez la section *Mappage d'un groupe d'utilisateurs à un groupe de serveurs* dans le *Guide d'administration de la plateforme Business Intelligence*.



Lorsqu'un utilisateur est associé à plusieurs groupes d'utilisateurs et que chacun d'entre eux est mappé vers un groupe de serveurs différent, la plateforme calcule le groupe de serveurs disponible. Dans le scénario ci-dessus, le travail de planification a lieu avec succès, car aucun groupe de serveurs n'est affecté à l'objet et parce que le groupe de serveurs disponible pour la planification de l'objet est une combinaison des groupes de serveurs SG1, SG2 et SG3.

Scénario 4 :

Outre le scénario 3, vous avez affecté l'objet au groupe SG1 et vous avez défini le groupe SG1 comme étant obligatoire. Pour plus d'informations sur la définition d'un groupe de serveurs comme obligatoire ou préféré, consultez la section *Mappage d'un groupe d'utilisateurs à un groupe de serveurs* dans le *Guide d'administration de la plateforme Business Intelligence*.



Si un groupe de serveurs est affecté à un objet, la plateforme vérifie que vous avez spécifié l'utilisateur disposant de droits d'affichage pour le groupe de serveurs. Dans ce scénario, la plateforme ne calcule pas le groupe de serveurs disponible, car un groupe de serveurs affecté au niveau de l'objet possède la priorité la plus élevée. Dans le scénario 4, l'objet est planifié avec succès, car le groupe d'utilisateurs UG1 dispose de droits sur le groupe de serveurs SG1 et l'utilisateur se voit attribuer ces droits par le groupe d'utilisateurs UG1.

→ N'oubliez pas

- Avant de planifier un objet, vérifiez que les affectations de groupe de serveurs à tous les groupes d'utilisateurs associés à l'utilisateur sont correctes et calculez le groupe de serveurs disponible.
- Un travail de planification s'effectue avec succès lorsque le groupe de serveurs disponible pour un utilisateur inclut le groupe de serveurs affecté à l'objet.

Reportez-vous au tableau ci-dessous :

ⓘ Remarque

Considérons que SG1 et SG2 sont affectés aux groupes d'utilisateurs UG1 et UG2 respectivement.

Niveau d'accès	Combinaison des groupes de serveurs (SG1 + SG2)	Recherche de serveurs dans le pool courant
L'utilisateur dispose de droits sur tous les groupes de serveurs	Requis + Requis	Faux

Niveau d'accès	Combinaison des groupes de serveurs (SG1 + SG2)	Recherche de serveurs dans le pool courant
L'utilisateur dispose de droits sur tous les groupes de serveurs	Requis + Privilégié	Faux
L'utilisateur dispose de droits sur tous les groupes de serveurs	Privilégié + Privilégié	Vrai
L'utilisateur ne dispose d'aucuns droits sur les groupes de serveurs	Requis + Requis	Faux
L'utilisateur ne dispose d'aucuns droits sur les groupes de serveurs	Requis + Privilégié	Faux
L'utilisateur ne dispose d'aucuns droits sur les groupes de serveurs	Privilégié + Privilégié	Vrai
L'utilisateur dispose de droits sur quelques groupes de serveurs	Requis (Non) + Requis (Oui)	Faux
L'utilisateur dispose de droits sur quelques groupes de serveurs	Requis (Non) + Privilégié (Oui)	Faux
L'utilisateur dispose de droits sur quelques groupes de serveurs	Requis (Oui) + Privilégié (Non)	Faux
L'utilisateur dispose de droits sur quelques groupes de serveurs	Privilégié (Non) + Privilégié (Oui)	Vrai

11.9 Configuration des serveurs de traitement adaptif (APS, Adaptive Processing Servers) pour les systèmes de production

Le programme d'installation installe un serveur de traitement adaptatif (APS) par système hôte. Selon les fonctionnalités que vous avez installées, cet APS peut héberger un grand nombre de services, tels que le service de surveillance, le service de gestion des promotions, le service d'analyse multidimensionnelle (MDAS), le service de publication et d'autres.

Pour les systèmes de production ou de test, la meilleure méthode consiste à créer des APS supplémentaires, puis de les configurer pour répondre à vos exigences de gestion.

Il est possible de créer des APS supplémentaires de deux manières :

- Activez l'Assistant de configuration du système.
  L'assistant apporte son aide pour les configurations de base de votre système de la plateforme de BI, y compris pour la configuration des APS selon les modèles de déploiement prédéfinis. La configuration des

APS fournie par l'assistant est un bon point de départ ; cependant, le dimensionnement du système doit toujours être effectué.

- Utilisez la CMC pour créer et configurer manuellement les APS supplémentaires.

Pour en savoir plus sur la configuration des serveurs de traitement adaptatif pour les systèmes de production, consultez l'article suivant de la base de connaissances à l'adresse : 1694041.

> → N'oubliez pas
>
> La sélection d'un modèle de déploiement dans l'assistant ou la création manuelle d'APS supplémentaires ne remplace pas le dimensionnement du système. Assurez-vous que le dimensionnement est effectué : http://www.sap.com/bisizing.

11.10 Évaluation des performances du système

11.10.1 Surveillance des serveurs de la plateforme de BI

L'application de surveillance offre la possibilité de capturer les métriques historiques et d'exécution des serveurs de la plateforme de BI pour le reporting et la notification. L'application aide les administrateurs système à identifier si les serveurs fonctionnent normalement et si les temps de réponse sont ceux escomptés.

Informations associées

Surveillance [page 821]

11.10.2 Analyse des performances du serveur

La CMC (Central Management Console) permet de visualiser les métriques des serveurs de votre système. Ces performances fournissent des informations générales sur chaque machine ainsi que des détails propres au type de serveur. La CMC vous permet aussi d'afficher les performances d'un système et d'obtenir des informations sur la version du produit, le CMS et les activités en cours du système.

> ⓘ Remarque
>
> Vous pouvez visualiser uniquement les métriques des serveurs en cours d'exécution.

11.10.2.1 Pour visualiser les métriques de serveur

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez avec le bouton droit de la souris sur le serveur dont vous voulez afficher les métriques et sélectionnez *Métriques*.

L'onglet *Métriques* affiche la liste des métriques du serveur.

Informations associées

Pour modifier les propriétés d'un serveur [page 468]
A propos de l'annexe Métriques du serveur [page 1212]

11.10.3 Affichage des performances du système

La zone de gestion *Paramètres* de la CMC affiche les métriques système vous fournissant des informations générales sur votre installation de la plateforme de BI. La section *Propriétés* communique la version du produit et le numéro d'édition. Elle contient également la source de données, le nom de la base de données et le nom d'utilisateur de la base de données du CMS. Dans la section *Afficher les métriques système globales*, vous trouverez des informations sur l'activité du compte actuel ainsi que des statistiques sur les travaux en cours et déjà traités. La section *Cluster* affiche le nom du CMS auquel vous êtes connecté, le nom du cluster de CMS et les noms des autres membres du cluster.

11.10.3.1 Pour visualiser les métriques système

1. Accédez à la zone de gestion *Paramètres* de la CMC.
2. Cliquez sur une flèche pour développer et afficher les paramètres dans la zone *Propriétés*, *Afficher les métriques système globales*, *Cluster* ou *Sauvegarde à chaud*.

11.10.4 Journalisation des activités du serveur

La plateforme de BI permet de journaliser des informations spécifiques sur l'activité Web de la plateforme de BI.

- En outre, chacun des serveurs de la plateforme de BI est conçu de manière à consigner les messages dans le journal système standard de votre système d'exploitation.
  - Sous Windows, la plateforme de BI journalise dans le service Journal des événements. Vous pouvez consulter les résultats à l'aide de l'observateur d'événements (dans le journal des applications).
  - Sous UNIX, la plateforme de BI journalise les informations dans le démon syslog en tant qu'application utilisateur. Chaque serveur ajoute son nom et son PID au début des messages qu'il journalise.

Chaque serveur enregistre aussi des messages d'assertion dans le répertoire des journaux de l'installation du produit. Les informations programmatiques consignées dans ces fichiers ne s'adressent généralement qu'au personnel du support technique de SAP Business Objects à des fins de débogage avancé. L'emplacement de ces fichiers journaux dépend de votre système d'exploitation :

- Sous Windows, le répertoire de journalisation par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\logging`
- Sous UNIX, le répertoire de journalisation par défaut est le répertoire `<REPINSTALL>/sap_bobj/logging` de votre installation.

N'oubliez pas que ces fichiers journaux sont nettoyés automatiquement et que le volume de données journalisées par serveur ne dépasse jamais 1 Mo.

> **Remarque**
>
> Pour que la journalisation fonctionne sur les ordinateurs UNIX hébergeant les serveurs de la plateforme de BI, vous devez définir et configurer la journalisation système de sorte que tous les messages journalisés dans la structure « utilisateur » du niveau « info » ou supérieur soient enregistrés. Vous devez également configurer `SYSLOGD` pour accepter la connexion à distance.
>
> Les procédures de configuration varient d'un système à l'autre. Consultez la documentation de votre système d'exploitation pour obtenir des instructions spécifiques.

11.11 Configuration des paramètres des serveurs

Cette section comprend des informations techniques et des procédures expliquant comment modifier les paramètres des serveurs de la plateforme de BI.

La plupart des paramètres étudiés dans cette section vous permettent d'intégrer plus aisément la plateforme de BI à vos configurations matérielles, logicielles et réseau actuelles. Le choix des paramètres dépend donc essentiellement de vos propres besoins.

Vous pouvez modifier de deux manières les paramètres du serveur via la Central Management Console (CMC).

- Dans l'écran *Propriétés* du serveur.
- Dans l'écran *Modifier les services communs* du serveur.

Il est important de noter que toutes les modifications ne sont pas immédiatement prises en compte. Si un paramètre ne peut pas être modifié immédiatement, les écrans *Propriétés* et *Modifier les services communs* affichent à la fois le paramètre actuel (en rouge) et le paramètre souhaité. Lorsque vous revenez à la zone de gestion Serveurs, le serveur sera marqué Périmé. Lorsque vous redémarrerez le serveur, ce dernier utilisera les paramètres souhaités et l'indicateur Périmé sera supprimé du serveur.

> **Remarque**
>
> Cette section n'indique pas comment configurer votre serveur d'applications Web pour déployer des applications de la plateforme de BI. Cette tâche est généralement effectuée lors de l'installation du produit. Pour en savoir plus, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*.

Informations associées

Configuration des numéros de port [page 477]
Pour modifier les propriétés d'un serveur [page 468]
Recréation de la base de données système du CMS [page 518]
Sélection d'une base de données CMS (nouvelle ou existante) [page 515]

11.11.1 Pour modifier les propriétés d'un serveur

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur dont vous souhaitez modifier les paramètres.
   L'écran *Propriétés* s'affiche.
3. Apportez les modifications requises, puis cliquez sur *Enregistrer* ou *Enregistrer et fermer*.

> ⓘ Remarque
>
> Toutes les modifications ne sont pas immédiatement prises en compte. Si un paramètre ne peut pas être modifié immédiatement, la boîte de dialogue Propriétés affiche à la fois le paramètre actuel (en rouge) et le paramètre souhaité. Lorsque vous revenez à la zone de gestion Serveurs, le serveur sera marqué Périmé. Lorsque vous redémarrerez le serveur, ce dernier utilisera les paramètres souhaités de la boîte de dialogue Propriétés et l'indicateur Périmé sera supprimé du serveur.

11.11.2 Pour appliquer les paramètres de service à plusieurs serveurs

Vous pouvez appliquer la même configuration à des services hébergés sur plusieurs serveurs.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Tout en maintenant la touche `Ctrl` enfoncée, cliquez sur chaque serveur dont vous voulez changer les paramètres, puis cliquez avec le bouton droit de la souris et sélectionnez *Modifier les services communs*.
   La boîte de dialogue *Modifier les services communs* apparaît, affichant une liste des services hébergés sur les serveurs sélectionnés et disposant de paramètres que vous pouvez modifier.
3. Si la boîte de dialogue *Modifier les services communs* répertorie plusieurs services, sélectionnez le service à modifier et cliquez sur *Continuer*.
4. Apportez les modifications souhaitées, puis cliquez sur *OK*.

> ⓘ Remarque
>
> Vous être redirigé vers la zone de gestion *Serveurs* de la CMC. Si un serveur requiert un redémarrage, il porte la mention Périmé. Lorsque vous redémarrerez le serveur, ce dernier utilise les nouveaux paramètres et l'indicateur Périmé est supprimé.

11.11.3 Utilisation des modèles de configuration

Les modèles de configuration vous permettent de configurer facilement plusieurs instances des serveurs. Les modèles de configuration stockent une liste de paramètres pour chaque type de service que vous pouvez utiliser pour configurer des instances de serveur supplémentaires. Par exemple, si vous avez une douzaine de serveurs de traitement Web Intelligence que vous souhaitez configurer de manière identique, vous n'avez besoin de configurer les paramètres que pour un seul serveur. Vous pouvez ensuite utiliser le service configuré pour définir le modèle de configuration pour les serveurs de traitement Web Intelligence et appliquer ensuite le modèle aux 11 autres instances du service.

Chaque type de service de la plateforme de BI possède son propre modèle de configuration. Par exemple, il existe un modèle de configuration pour le type de service de traitement Web Intelligence, un pour le type de service de publication, etc. Le modèle de configuration est défini dans les propriétés du serveur de la CMC (Central Management Console).

Lorsqu'un serveur utilise un modèle de configuration, les paramètres existants de ce serveur sont remplacés par les valeurs du modèle. Si, par la suite, vous ne souhaitez plus utiliser le modèle, les paramètres d'origine ne sont pas restaurés. Les modifications ultérieures apportées au modèle de configuration n'affectent plus le serveur.

Il est conseillé d'utiliser les modèles de configuration comme suit :

1. Définissez le modèle de configuration sur un serveur.
2. Si l'on suppose que vous souhaitez la même configuration sur tous les serveurs de même type, cochez l'option *Utiliser le modèle de configuration* pour tous les serveurs de même type, y compris celui sur lequel vous avez défini le modèle de configuration.
3. Ultérieurement, si vous souhaitez modifier la configuration de tous les services de ce type, affichez les propriétés de l'un de ces services et désélectionnez la case à cocher *Utiliser le modèle de configuration*. Modifiez les paramètres souhaités, puis sélectionnez *Définir le modèle de configuration* pour ce serveur et cliquez sur *Enregistrer*. Tous les services de ce type sont mis à jour. En ne définissant pas de serveur comme modèle de configuration, vous protégez tous les serveurs de même type contre une modification accidentelle des paramètres de configuration .

Informations associées

Pour définir un modèle de configuration [page 469]
Pour appliquer un modèle de configuration à un serveur [page 470]

11.11.3.1 Pour définir un modèle de configuration

Vous pouvez définir un modèle de configuration pour chaque type de service. Vous ne pouvez pas définir des modèles de configuration multiples pour un service. Vous pouvez utiliser la page *Propriétés* de n'importe quel serveur pour configurer les paramètres qui seront utilisés par le modèle de configuration pour un type de service hébergé sur le serveur.

1. Accédez à la zone de gestion *Serveurs* de la CMC.

2. Cliquez deux fois sur le serveur hébergeant les services dont vous souhaitez définir le modèle de configuration.
   L'écran *Propriétés* s'affiche.
3. Configurez les paramètres du service que vous souhaitez utiliser pour le modèle, activez la case à cocher *Définir le modèle de configuration*, puis cliquez sur *Enregistrer* ou sur *Enregistrer et fermer*.

Le modèle de configuration pour le type de service que vous avez sélectionné est défini en fonction des paramètres du serveur actuel. Les autres serveurs de même type hébergeant les mêmes services seront automatiquement et immédiatement reconfigurés afin de correspondre au modèle de configuration si l'option *Utiliser le modèle de configuration* est activée dans leurs propriétés.

> **Remarque**
>
> Si vous ne définissez pas explicitement les paramètres du modèle de configuration, les paramètres par défaut du service sont utilisés.

Informations associées

Pour appliquer un modèle de configuration à un serveur [page 470]

11.11.3.2 Pour appliquer un modèle de configuration à un serveur

Avant d'appliquer un modèle de configuration, assurez-vous d'avoir défini les paramètres du modèle de configuration pour le type de serveur auquel vous souhaitez appliquer le modèle. Si vous n'avez pas défini de façon explicite les paramètres du modèle de configuration, les paramètres par défaut de ce service sont utilisés.

> **Remarque**
>
> Les serveurs pour lesquels le paramètre Utiliser le modèle de configuration n'est pas activé ne seront pas mis à jour lors d'une modification des paramètres du modèle de configuration.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur hébergeant un service auquel vous souhaitez appliquer le modèle de configuration.
   L'écran *Propriétés* s'affiche.
3. Sélectionnez la case à cocher *Utiliser le modèle de configuration* et cliquez sur *Enregistrer* ou *Enregistrer et fermer*.

   > **Remarque**
   >
   > Si le serveur nécessite un redémarrage afin de prendre en compte les nouveaux paramètres, il affichera l'indicateur "Périmé" dans la liste des serveurs.

Le modèle de configuration approprié est appliqué au serveur actuel. Tout changement ultérieur apporté au modèle de configuration modifie la configuration de tous les serveurs qui utilisent ce modèle.

Le fait de désactiver *Utiliser le modèle de configuration* ne rétablit pas les valeurs initiales du serveur telles qu'elles étaient lorsque le modèle de configuration a été appliqué. Les changements ultérieurs apportés au modèle de configuration n'affectent pas la configuration des serveurs qui utilisent ce modèle.

Informations associées

Pour définir un modèle de configuration [page 469]

11.11.3.3 Pour restaurer les valeurs par défaut du système

Vous souhaiterez peut-être restaurer la configuration d'un service pour revenir aux paramètres initialement installés (par exemple, si vous avez incorrectement configuré les serveurs ou si vous rencontrez des problèmes de performances).

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur hébergeant un service pour lequel vous souhaitez restaurer les valeurs système par défaut.
   L'écran *Propriétés* s'affiche.
3. Sélectionnez la case à cocher *Restaurer les valeurs par défaut du système* et cliquez sur *Enregistrer* ou *Enregistrer et fermer*.
   Les paramètres par défaut pour le type de service spécifique sont restaurés.

11.12 Configuration des paramètres réseau du serveur

Les paramètres réseau des serveurs de la plateforme de BI sont gérés via la CMC. Ces paramètres sont divisés en deux catégories : les paramètres de port et l'identification de l'hôte.

Paramètres par défaut

Lors de l'installation, les identificateurs de l'hôte du serveur sont définis sur *Affecter automatiquement*. Il est toutefois possible d'affecter à chaque serveur une adresse IP ou un nom d'hôte spécifique. Le numéro de port par défaut du CMS est 6400. Les autres serveurs de la Plateforme de BI sont liés dynamiquement aux ports disponibles. Les numéros de port sont automatiquement gérés par la plateforme de BI mais vous pouvez utiliser la CMC pour spécifier des numéros de port.

11.12.1 Options d'environnement réseau

La plateforme de BI prend en charge Internet Protocol version 4 (IPv4) et un trafic de réseau mixte combiné IPv4/IPv6. Vous pouvez utiliser les composants client et serveur dans les environnements suivants :

- Réseau IPv4 : tous les composants client et serveur s'exécutent uniquement avec le protocole IPv4.
- Réseau mixte IPv6/IPv4 : les composants client et serveur peuvent s'exécuter avec les protocoles IPv6 et IPv4.
  c'est-à dire :
  - IPv6 uniquement (pile IPv6 activée, pile IPv4 installée et pile IPv4 désactivée)
  - Mixte IPv6/IPv4 (les deux piles IPv6 et IPv4 activées)
  - IPv4 uniquement (pile IPv4 activée, pile IPv6 désactivée ou désinstallée

> **Remarque**
>
> - La configuration du réseau doit être effectuée par l'administrateur réseau et système. La plateforme de BI ne propose pas de mécanisme permettant d'indiquer un environnement réseau. Vous pouvez utiliser la CMC pour lier n'importe quel serveur de la plateforme de BI à une adresse IPv6 ou IPv4 spécifique.
> - La pile IPv6 pure (IPv6 seul installé et activé) n'est pas prise en charge. En revanche, un réseau mixte IPv6 est pris en charge.

11.12.1.1 Environnement mixte IPv6/IPv4

L'environnement réseau IPv6/IPv4 offre les avantages suivants :

- Les serveurs de la plateforme de BI peuvent traiter à la fois des requêtes IPv6 et IPv4 quand ils s'exécutent en mode mixte.
- Les composants client peuvent interagir avec les serveurs en tant que nœuds uniquement IPv4 ou nœuds IPv6/IPv4.

Le mode mixte est particulièrement utile dans les cas suivants :

- Lorsque vous passez d'un environnement de nœud uniquement IPv4 à un environnement IPv6 mixte. Tous les composants client et serveur continuent à interagir de façon transparente jusqu'à la fin de la transition. Vous pouvez ensuite désactiver les paramètres IPv4 pour tous les serveurs.
- Les logiciels tiers non compatibles IPv6 continuent à fonctionner dans l'environnement de nœud IPv6/IPv4.

11.12.2 Options d'identification de l'hôte du serveur

Les options d'identification de l'hôte peuvent être spécifiées dans la CMC pour chaque serveur de la plateforme de BI. Le tableau suivant résume les options disponibles dans la zone *Paramètres courants* :

Option	Description
Affecter automatiquement	Il s'agit du paramètre par défaut pour tous les serveurs. Quand cette case est cochée, le serveur lie automatiquement le port de requêtes du serveur à la première interface réseau de l'ordinateur. **Remarque** Il est recommandé de cocher la case *Affecter automatiquement* pour le nom d'hôte. Toutefois, dans certains cas comme lorsque le serveur est exécuté sur un ordinateur multirésident ou lorsque le serveur doit interagir avec une certaine configuration de pare-feu, il est recommandé d'utiliser un nom d'hôte ou une adresse IP spécifique. Pour en savoir plus sur la configuration d'un ordinateur multi-résident et l'utilisation des pare-feu, voir le *Guide d'administration de la plateforme de Business Intelligence*.
Nom d'hôte	Spécifie le nom d'hôte de l'interface réseau sur laquelle le serveur écoute les requêtes. Pour le CMS, ce paramètre spécifie le nom d'hôte de l'interface réseau à laquelle le CMS lie le port du serveur de noms et le port de requêtes.
Adresse IP	Spécifie l'adresse IP de l'interface réseau sur laquelle le serveur écoute les requêtes. Pour le CMS, ce paramètre spécifie l'adresse de l'interface réseau utilisée par le CMS pour lier le port du serveur de noms et le port de requêtes. Pour tous les serveurs, des champs distincts sont fournis pour spécifier des adresses IP IPv4 et/ou IPv6.

Attention

Si vous cochez la case *Affecter automatiquement* sur un ordinateur multirésident, le CMS risque d'être lié automatiquement à une interface réseau inappropriée. Pour l'éviter, veillez à ce que les interfaces réseau de l'ordinateur hôte soient répertoriées dans le bon ordre (à l'aide des outils du système d'exploitation de l'ordinateur). Vous devez spécifier le nom d'hôte du CMS dans la CMC.

Remarque

Si vous utilisez des ordinateurs multirésidents ou certaines configurations de pare-feu NAT, vous devez spécifier le nom de l'hôte à l'aide de noms de domaine complets à la place de noms d'hôte.

Informations associées

Pour configurer le système pour des pare-feu [page 211]

Configuration d'un ordinateur multi-résident [page 474]
Pour dépanner plusieurs interfaces réseau [page 476]

11.12.2.1 Pour modifier l'identification de l'hôte d'un serveur

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Sélectionnez le serveur, puis cliquez sur *Arrêter le serveur* dans le menu *Actions*.
3. Sélectionnez *Propriétés* dans le menu *Gérer*.
4. Sous *Paramètres courants*, sélectionnez l'une des options suivantes :

Option	Description
Affecter automatiquement	Le serveur sera lié à l'une des interfaces réseau disponibles.
Nom d'hôte	Saisissez le nom d'hôte de l'interface réseau sur laquelle le serveur écoute les requêtes.
Adresse IP	Dans les champs prévus à cet effet, saisissez l'adresse IPv4 ou l'adresse IPv6 de l'interface réseau sur laquelle le serveur écoute les requêtes. **Remarque** Pour permettre au serveur de fonctionner en tant que nœud double IPv4/IPv6, saisissez une adresse IP valide dans les deux champs.

5. Cliquez sur *Enregistrer* ou sur *Enregistrer & Fermer*.
   Les modifications sont visibles dans la ligne de commande affichée dans l'onglet *Propriétés*.
6. Démarrez et activez le serveur.

11.12.3 Configuration d'un ordinateur multi-résident

Un ordinateur multi-résident désigne un ordinateur qui possède plusieurs adresses réseau. Pour cela, il suffit d'avoir plusieurs interfaces réseau, chacune dotée d'une ou plusieurs adresses IP, ou une seule interface réseau affectée à plusieurs adresses IP.

Si vous avez plusieurs interfaces réseau, toutes dotées d'une adresse IP unique, modifiez l'ordre de liaison pour placer en première position l'interface réseau à laquelle vous souhaitez lier les serveurs de la plateforme de BI. Si votre interface dispose de plusieurs adresses IP, utilisez l'option Identifiants de l'hôte dans la CMC pour spécifier une carte d'interface réseau pour le serveur de la plateforme de BI. Vous pouvez indiquer un nom d'hôte ou une adresse IP. Pour en savoir plus sur la configuration du paramètre *Identifiants de l'hôte*, voir « Pour dépanner plusieurs interfaces réseau ».

> **→ Conseil**
>
> Cette section vous explique comment obliger tous les serveurs à utiliser la même adresse réseau en sachant toutefois qu'il est possible de lier des serveurs individuels à différentes adresses. Vous pourriez, par exemple, lier les File Repository Servers à une adresse privée non accessible à partir des machines des utilisateurs. Pour parvenir à des configurations avancées de ce type, votre configuration DNS doit parfaitement acheminer les communications entre tous les composants serveur de la plateforme de BI.

> Dans cet exemple, le DNS doit acheminer les communications des autres serveurs de la plateforme de BI vers l'adresse privée des File Repository Servers.

Informations associées

Pour dépanner plusieurs interfaces réseau [page 476]

11.12.3.1 Pour configurer le CMS de manière à le lier à une adresse réseau

> **Remarque**
>
> Sur un ordinateur multi-résident, l'identificateur de l'hôte peut être le nom de domaine complet ou l'adresse IP de l'interface à laquelle vous voulez lier le serveur.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le CMS.
3. Sous *Paramètres courants*, sélectionnez l'une des options suivantes :
   - *Nom d'hôte*
   - Saisissez le nom d'hôte de l'interface réseau à laquelle le serveur sera lié.
   - *Adresse IP*
   - Saisissez dans les champs prévus à cet effet l'adresse IPv4 ou IPv6 de l'interface réseau à laquelle le serveur sera lié.

     > **Remarque**
     >
     > Pour permettre au serveur de fonctionner en tant que nœud double IPv4/IPv6, saisissez une adresse IP valide dans les deux champs.

   > **Attention**
   >
   > Ne sélectionnez pas l'option Affecter automatiquement.
4. Pour *Port de requêtes*, vous pouvez effectuer l'une des opérations suivantes :
   - Sélectionnez l'option *Affecter automatiquement*.
   - Saisissez un numéro de port valide dans le champ *Port de requêtes*.
5. Assurez-vous qu'un numéro de port est indiqué dans la boîte de dialogue Port du serveur de noms.

   > **Remarque**
   >
   > Le numéro de port par défaut est 6400.

11.12.3.2 Configuration des serveurs restants pour les lier à une adresse réseau

Les autres serveurs de la plateforme de BI sélectionnent leurs ports de manière dynamique par défaut. Pour en savoir plus sur la désactivation du paramètre Affecter automatiquement qui propage dynamiquement ces informations, voir « Changement du port utilisé par un serveur pour accepter les requêtes ».

Informations associées

Pour changer le port utilisé par un serveur pour accepter les requêtes [page 480]

11.12.3.3 Pour dépanner plusieurs interfaces réseau

Sur un ordinateur multirésidents, le CMS risque d'être lié automatiquement à une interface réseau inappropriée. Pour éviter que cela ne se produise, vous pouvez veiller à ce que les interfaces réseau de l'ordinateur hôte soient répertoriées dans l'ordre correct (à l'aide des outils du système d'exploitation de l'ordinateur) ou veiller à spécifier le paramètre du nom d'hôte du CMS dans la CMC. Si l'interface réseau primaire n'est pas accessible, vous pouvez utiliser la procédure suivante pour configurer la plateforme de BI afin d'effectuer une liaison à une interface réseau accessible non primaire. Exécutez ces étapes immédiatement après l'installation de la plateforme de BI sur l'ordinateur local, avant d'installer la plateforme de BI sur d'autres ordinateurs.

1. Ouvrez le CCM et arrêtez le SIA correspondant au nœud de l'ordinateur possédant plusieurs interfaces réseau.
2. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*.
3. Dans la boîte de dialogue *Propriétés*, cliquez sur l'onglet *Configuration*.
4. Pour lier le SIA à une interface réseau particulière, entrez le numéro de port de l'interface réseau cible dans le champ *Port*.
5. Cliquez sur *OK*, puis sélectionnez l'onglet *Démarrage*.
6. Dans la liste *Serveurs CMS locaux*, sélectionnez le CMS puis cliquez sur *Propriétés*.
7. Pour lier le CMS à une interface réseau particulière, saisissez le numéro de port de l'interface réseau cible dans le champ *Port*.
8. Cliquez sur *OK* pour appliquer les nouveaux paramètres.
9. Démarrez le SIA et attendez le démarrage des serveurs.
10. Lancez la CMC (Central Management Console), puis accédez à la zone de gestion *Serveurs*. Répétez les étapes 11 à 14 pour chaque serveur.
11. Sélectionnez le serveur, puis cliquez sur *Arrêter le serveur* dans le menu *Actions*.
12. Sélectionnez *Propriétés* dans le menu *Gérer*.
13. Sous *Paramètres courants*, sélectionnez l'une des options suivantes :
    - Nom d'hôte : saisissez le nom d'hôte de l'interface réseau à laquelle le serveur sera lié.
    - Adresse IP : dans les champs prévus à cet effet, saisissez l'adresse IPv4 ou IPv6 de l'interface réseau à laquelle le serveur sera lié.

> **Remarque**
>
> Pour permettre au serveur de fonctionner en tant que nœud double IPv4/IPv6, saisissez une adresse IP valide dans les deux champs.

> **Attention**
>
> Ne sélectionnez pas l'option Affecter automatiquement.

14. Cliquez sur *Enregistrer* ou sur *Enregistrer & Fermer*.
15. Revenez au CCM et redémarrez le SIA.

    Le SIA redémarre tous les serveurs du nœud. Tous les serveurs de l'ordinateur sont à présent liés à l'interface réseau appropriée.

11.12.4 Configuration des numéros de port

Lors de l'installation, le CMS est configuré de manière à utiliser les numéros de port par défaut. Le numéro de port par défaut du CMS est 6400. Ce port fait partie de la plage de ports réservée par SAP BusinessObjects (6400 à 6410). La communication sur ces ports ne doit pas entrer en conflit avec des applications tierces.

Lors du démarrage et de l'activation, tous les autres serveurs de la plateforme de BI se lient dynamiquement à un port disponible (supérieur à 1024), s'enregistrent auprès du CMS avec ce port, puis restent à l'écoute des requêtes de la plateforme de BI. Si nécessaire, vous pouvez demander à chaque composant serveur d'être à l'écoute sur un port spécifique (plutôt que d'opter pour la sélection dynamique d'un port disponible). Par exemple, vous devrez configurer manuellement un port de requêtes pour chaque serveur de la plateforme de BI devant communiquer à travers un pare-feu.

Vous pouvez les spécifier dans l'onglet Propriétés de chaque serveur dans la CMC. Ce tableau résume les options figurant sous la zone *Paramètres courants*. Il s'agit d'options relatives à l'utilisation des ports pour des types de serveur spécifiques.

Paramètre	CMS	Autres serveurs
Port de requêtes	Indique le port que le CMS utilise pour accepter toutes les requêtes en provenance d'autres serveurs (à l'exception des requêtes du serveur de noms). Utilise la même interface réseau que le port du serveur de noms. Lorsque l'option *Affecter automatiquement* est sélectionnée, le serveur utilise automatiquement un numéro de port affecté par le système d'exploitation.	Spécifie le port sur lequel le serveur écoute toutes les requêtes. Lorsque l'option *Affecter automatiquement* est sélectionnée, le serveur utilise automatiquement un numéro de port affecté par le système d'exploitation.
Port du serveur de noms	Spécifie le port de la plateforme de BI sur lequel le CMS écoute les requêtes de service de noms. Le port par défaut est 6400.	Non applicable

11.12.4.1 Pour changer le port par défaut du CMS dans la CMC

Si un CMS s'exécute déjà sur le cluster, vous pouvez utiliser la CMC pour changer le numéro de port par défaut du CMS. Si aucun CMS n'est en cours d'exécution sur le cluster, vous devez utiliser le CCM sous Windows, ou le script `serverconfig.sh` sous UNIX, pour changer le numéro de port.

> **Remarque**
>
> Le CMS utilise la même carte d'interface réseau pour le port de requêtes et le port du serveur des noms.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le CMS dans la liste de serveurs.
3. Remplacer le numéro du *Port de serveur de noms* par celui du port sur lequel le CMS sera à l'écoute. (Le port par défaut est 6400.)
4. Cliquez sur *Enregistrer & Fermer*.
5. Redémarrez le CMS.

   Le CMS démarre l'écoute sur le numéro de port spécifié. Le Server Intelligence Agent propage dynamiquement les nouveaux paramètres aux autres serveurs du nœud, si l'option *Affecter automatiquement* de ces serveurs est sélectionnée pour le port de requêtes. (La prise en compte des modifications apportées aux paramètres Propriétés sur tous les membres du nœud peut prendre quelques minutes.)

   Les paramètres que vous sélectionnez sur la page *Propriétés* sont répercutés sur la ligne de commande du serveur qui s'affiche également sur la page *Propriétés*.

11.12.4.2 Changement du port par défaut du CMS dans le CCM (Central Configuration Manager) sous Windows

Si aucun CMS n'est accessible sur le cluster et que vous souhaitez modifier le port par défaut d'un ou plusieurs CMS de votre déploiement, vous devez utiliser le CCM pour changer le numéro de port de CMS.

1. Ouvrez le CCM et arrêtez le SIA correspondant au nœud.
2. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*.
3. Dans al boîte de dialogue *Propriétés*, cliquez sur l'onglet *Démarrage*.
4. Dans la liste *Serveurs CMS locaux*, sélectionnez le CMS dont vous voulez changer le numéro de port, puis cliquez sur *Propriétés*.
5. Pour lier le CMS à un port particulier, saisissez le numéro de port dans le champ *Port*.
6. Cliquez sur *OK* pour appliquer les nouveaux paramètres.
7. Démarrez le SIA et attendez le démarrage des serveurs.

11.12.4.3 Changement du port par défaut du CMS dans le CCM sous UNIX

Si aucun CMS n'est accessible sur le cluster et que vous désirez modifier le port par défaut d'un ou plusieurs CMS de votre déploiement, utilisez le script `serverconfig.sh` pour changer le numéro de port de CMS.

1. Utilisez le script `ccm.sh` pour arrêter le SIA (Serveur Intelligence Agent) qui héberge le CMS dont vous souhaitez modifier le numéro de port.
2. Exécutez le script `serverconfig.sh`.

   Par défaut, ce script se trouve dans le répertoire `<RepInstall>/sap_bobj`.
3. Sélectionnez *3 - Modifier le nœud*, puis appuyez sur `Entrée`.
4. Sélectionnez le nœud qui héberge le CMS que vous souhaitez modifier, puis appuyez sur la touche `Entrée`.
5. Sélectionnez *3 - Modifier un CMS local*, puis appuyez sur `Entrée`.
   Une liste des CMS hébergés sur le nœud s'affiche.
6. Sélectionnez le CMS à modifier, puis appuyez sur `Entrée`.
7. Saisissez le nouveau numéro de port du CMS et appuyez sur `Entrée`.
8. Spécifiez si vous voulez que le CMS démarre automatiquement en même temps que le SIA, puis appuyez sur la touche `Entrée`.
9. Saisissez les arguments de la ligne de commande pour le CMS ou acceptez les arguments actuels, puis appuyez sur la touche `Entrée`.
10. Saisissez **`quit`** pour fermer le script.
11. Démarrez le SIA avec le script `ccm.sh` et attendez le démarrage des serveurs.

11.12.4.4 Pour changer le port utilisé par un CMS pour accepter les requêtes

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Sélectionnez le CMS, puis cliquez sur *Propriétés* dans le menu *Gérer*.
3. Sous *Paramètres courants*, décochez la case *Affecter automatiquement* du *Port de requêtes*, puis saisissez le numéro de port sur lequel le serveur sera à l'écoute.
4. Cliquez sur *Enregistrer* ou sur *Enregistrer & Fermer*.
5. Redémarrez le CMS.

Le CMS se lie au nouveau port et démarre l'écoute des requêtes des autres serveurs.

11.12.4.5 Pour changer le port utilisé par un serveur pour accepter les requêtes

> **Remarque**
>
> Cette procédure ne peut pas être utilisée pour modifier le port de requête du CMS (Central Management Server). Voir plutôt « Modification du port utilisé par le CMS pour l'acceptation des requêtes ».

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Sélectionnez le serveur, puis cliquez sur *Arrêter le serveur* dans le menu *Actions*.
3. Cliquez deux fois sur le serveur.
   L'écran *Propriétés* s'affiche.
4. Sous *Paramètres courants*, désélectionnez la case à cocher *Affecter automatiquement* du *Port de requêtes*, puis saisissez le numéro de port sur lequel le serveur sera à l'écoute.
5. Cliquez sur *Enregistrer* ou sur *Enregistrer & Fermer*.
6. Démarrez et activez le serveur.

Le serveur se lie au nouveau port, s'enregistre auprès du CMS et démarre l'écoute des requêtes de la plateforme de BI sur le nouveau port.

11.13 Gestion des nœuds

11.13.1 Utilisation des nœuds

Un nœud est un groupe de serveurs de la plateforme de BI qui s'exécutent sur le même hôte et sont gérés par le même SIA (Server Intelligence Agent). Tous les serveurs d'un nœud s'exécutent sous le même compte utilisateur. Un ordinateur peut comporter plusieurs nœuds ;vous pouvez donc exécuter des processus sous différents comptes utilisateur. Un SIA gère et surveille l'ensemble des serveurs d'un nœud en vérifiant qu'ils fonctionnent correctement.

> **Remarque**
>
> Vous devez utiliser un compte administrateur avec l'authentification Enterprise pour effectuer en sécurité toutes les procédures de gestion des nœuds. Toutefois, si la communication SSL entre les serveurs est activée, vous devez désactiver SSL pour effectuer des procédures de gestion de nœuds.

> **Remarque**
>
> Assurez-vous que tous les pilotes de base de données nécessaires pour que les serveurs de la plateforme de BI se connectent à leur source de données (par exemple, pour que le CMS se connecte à la base de données du CMS) sont présents et que l'environnement adapté a déjà été configuré (par exemple, les variables d'environnement appropriées ont été définies).

11.13.1.1 Variables

Variable	Description
`<REPINSTALL>`	Répertoire où est installée la plateforme SAP BusinessObjects Business Intelligence. Sous Windows : `C:\Program Files (x86)\SAP BusinessObjects`
`<REPSCRIPT>`	Répertoire où se trouvent les scripts de gestion des nœuds. • Sous Windows : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` • Sous Unix : `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME64>/scripts`
`<PLATEFORME32>`	Nom de votre système d'exploitation Unix. Les valeurs acceptées sont les suivantes : • `aix_rs6000` • `linux_x86` • `solaris_sparc` • `win32_x86`
`<PLATEFORME64>`	Nom de votre système d'exploitation Unix. Les valeurs acceptées sont les suivantes : • `aix_rs6000_64` • `linux_x64` • `solaris_sparcv9` • `win64_x64`

11.13.1.2 Pour préparer un ordinateur sous Unix pour SQL Anywhere

Vous devez créer un fichier `odbc.ini` et le localiser avant de pouvoir utiliser SQL Anywhere comme source de données ODBC sur un ordinateur sous Unix.

> **Remarque**
>
> Cette procédure n'est pas nécessaire si vous utilisez SQL Anywhere fourni et installé avec la plateforme de BI.

1. Créez `odbc.ini` à l'emplacement `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME64>`.

2. Saisissez le nom de source de base de données (DSN), le nom de base de données et le nom de serveur pour SQL Anywhere ainsi que l'adresse IP et le numéro de port de l'ordinateur hébergeant le serveur de base de données SQL Anywhere.
3. Enregistrez `odbc.ini`
4. Ajoutez l'environnement SQL Anywhere dans votre environnement actuel.

   Par exemple, si vous utilisez Bash comme shell de ligne de commande, donnez comme source la version 64 bits de `sa_config.sh`.
5. Définissez une variable d'environnement nommée `ODBCINI` qui indique l'emplacement où a été créé le fichier `odbc.ini`.

   Configurez la variable d'environnement `ODBCINI` afin que les processus enfant puissent la voir .

Exemple

Exemple de fichier `odbc.ini` :

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0
[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Exemple de commande `source` :

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Informations associées

Variables [page 481]

11.13.2 Ajout d'un nœud

Le programme d'installation crée un seul nœud lors de la première installation de la plateforme de BI.

Il est possible que vous ayez besoin d'autres nœuds pour exécuter des serveurs sous différents comptes utilisateur.

Vous pouvez ajouter un nœud à l'aide du CCM (Central Configuration Manager) ou d'un script de gestion de nœuds. Si vous utilisez un pare-feu, vérifiez que les ports du SIA (Server Intelligence Agent) et du CMS (Central Management Server) sont ouverts.

> **Remarque**
>
> Utilisez le CCM ou le script de gestion des nœuds sur l'ordinateur où vous désirez ajouter un nœud. Il n'est pas possible d'ajouter un nœud sur un ordinateur distant.

Une installation de la plateforme de BI est une instance unique des fichiers de la plateforme de BI créée par le programme d'installation sur un ordinateur. Une instance d'installation de la plateforme de BI ne peut être utilisée qu'au sein d'un seul cluster. Les nœuds appartenant à différents clusters qui partagent la même installation de la plateforme de BI ne sont pas pris en charge parce que ce type de déploiement ne peut pas se voir appliquer des correctifs ou des mises à jour. Seules les plateformes Unix prennent en charge plusieurs installations du logiciel sur le même ordinateur et ce, uniquement si chaque installation est effectuée sous un compte utilisateur unique et est placée dans un dossier distinct afin que les installations ne partagent aucun fichier.

Rappelez-vous que tous les ordinateurs du cluster doivent avoir le même niveau de version et de correctif.

> **→ Recommandation**
>
> Pour ajouter des nœuds à un déploiement de la plateforme de BI dans lequel FIPS est activé et CORBA SSL est configuré, il est recommandé d'utiliser l'option "Démarrer un nouveau CMS temporaire".
>
> Pour ajouter des nœuds à un déploiement de la plateforme de BI dans lequel FIPS n'est pas activé et CORBA SSL est configuré, il est recommandé d'utiliser l'option "Démarrer un nouveau CMS temporaire".
>
> Pour ajouter des nœuds à un déploiement de la plateforme de BI dans lequel FIPS est activé et CORBA SSL n'est pas configuré, il est recommandé d'utiliser le CMS existant.

11.13.2.1 Ajout d'un nœud à un nouvel ordinateur sur un déploiement existant

Vous pouvez créer automatiquement le premier nœud sur un ordinateur lorsque vous utilisez le programme d'installation pour ajouter un nouvel ordinateur à un déploiement existant.

> **→ Conseil**
>
> Pendant l'installation, cliquez sur *Développer* et spécifiez le Central Management Server existant.

Pour créer d'autres nœuds, utilisez le CCM (Central Configuration Manager) ou le script `serverconfig.sh`.

Pour en savoir plus sur l'installation, voir le *Guide d'installation de la plateforme SAP BI*.

11.13.2.2 Ajout d'un nœud sous Windows

> **⚠ Attention**
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après l'ajout du nœud.

1. Sur la barre d'outils du CCM (Central Configuration Manager), cliquez sur *Ajouter un nœud*.
2. Dans l'*Assistant d'ajout de nœud*, saisissez le nom du nœud et le numéro de port du nouveau SIA (Server Intelligence Agent).
3. Choisissez si vous voulez ou non créer des serveurs sur le nouveau nœud.
   - *Ajouter un nœud sans serveur*
   - *Ajouter un nœud avec le CMS*
   - *Ajouter un nœud avec des serveurs par défaut*
     Cette option crée uniquement les serveurs installés sur cet ordinateur. Elle n'inclut pas tous les serveurs possibles.
4. Sélectionnez un CMS.
   - Si votre déploiement est en cours d'exécution, sélectionnez *Utiliser le CMS existant en cours d'exécution* puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro de port du CMS existant, les références de connexion Administrateur, le nom de la source de données, les références de connexion à la base de données système ainsi que la clé du cluster.
   - Si votre déploiement est arrêté, sélectionnez *Démarrer un nouveau CMS temporaire* puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro de port du CMS temporaire, les références de connexion Administrateur, le nom de la source de données, les références de connexion à la base de données système ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

     > ⚠ Attention
     >
     > Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existants et nouveaux utilisent des ports différents.
5. Révisez la page de confirmation et cliquez sur *Terminer*.
   Le CCM crée un nœud. En cas d'erreurs, vérifiez le fichier journal.

Vous pouvez à présent utiliser le CCM pour démarrer le nouveau nœud.

11.13.2.2.1 Ajout d'un nœud à l'aide d'un script sous Windows

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après l'ajout du nœud.

Vous pouvez utiliser `AddNode.bat` pour ajouter un nœud à un ordinateur Windows. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

En raison des limitations de l'invite de commande, vous devez utiliser le caret (^) pour échapper les espaces, le signe égal (=) et le point-virgule (;) dans ces paramètres, sauf si vous mettez le texte entre guillemets.

```
<REPSCRIPT>\AddNode.bat -name mynode2
  -siaport 6415
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
      -createcms
```

> **Remarque**
>
> Pour éviter d'utiliser le caret dans les chaînes longues, vous pouvez écrire le nom du script et tous ses paramètres dans un fichier `response.bat` temporaire, puis exécuter le fichier `response.bat` sans paramètres.

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.2.3 Ajout d'un nœud sous Unix

> **Attention**
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après l'ajout du nœud.

1. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`
2. Sélectionnez *Ajouter un nœud*, puis appuyez sur `Entrée`.
3. Tapez le nom du nouveau nœud et appuyez sur `Entrée`.
4. Tapez le numéro de port du nouveau SIA et appuyez sur `Entrée`.
5. Choisissez si vous voulez ou non créer des serveurs sur le nouveau nœud.
   - *no servers*
     Crée un nœud qui ne contient aucun serveur.
   - *cms*
     Crée un CMS sur le nœud, mais aucun autre serveur.
   - *default servers*

Crée uniquement les serveurs installés sur cet ordinateur. Tous les serveurs possibles ne sont pas inclus.

6. Sélectionnez un CMS.
   - Si votre déploiement est en cours d'exécution, sélectionnez *existing* puis appuyez sur `Entrée`.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro port du CMS existant, les références de connexion Administrateur, les informations de connexion à la base de données et les références de connexion à la base de données système ainsi que la clé du cluster.
   - Si votre déploiement est arrêté, sélectionnez *temporary*, puis appuyez sur `Entrée`.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro port du CMS temporaire, les références de connexion Administrateur, les informations de connexion à la base de données et les références de connexion à la base de données système ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

     > ⚠ Attention
     >
     > Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existants et nouveaux utilisent des ports différents.

7. Révisez la page de confirmation et appuyez sur `Entrée`.
   Le CCM crée un nœud. En cas d'erreurs, vérifiez le fichier journal.

Vous pouvez maintenant exécuter `<REPINSTALL>/sap_bobj/ccm.sh -start <nomNœud>` pour démarrer le nouveau nœud.

11.13.2.3.1 Ajout d'un nœud à l'aide d'un script sous Unix

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après l'ajout du nœud.

Vous pouvez utiliser `addnode.sh` pour ajouter un nœud à un ordinateur Unix. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

```
<REPSCRIPT>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.3 Recréation d'un nœud

Vous pouvez recréer un nœud à l'aide du CCM (Central Configuration Manager) ou d'un script de gestion de nœuds, après restauration de la configuration serveur pour l'ensemble du cluster ou si l'ordinateur hébergeant votre déploiement tombe en panne, est endommagé ou bien a un système de fichiers corrompu. Utilisez les règles suivantes :

- Il n'est pas nécessaire de recréer un nœud si vous réinstallez le déploiement sur un ordinateur de remplacement ayant des options d'installation et un nom de nœud identiques. Le programme d'installation recrée automatiquement le nœud.
- Un nœud ne doit être recréé que sur un ordinateur dont le déploiement existant a des options d'installation et un niveau de correctif identiques.
- Vous ne devez recréer que des nœuds qui n'existent sur aucun ordinateur de votre déploiement. Assurez-vous qu'aucun autre ordinateur n'héberge le même nœud.
- Bien que le déploiement permette aux nœuds de s'exécuter sur différents systèmes d'exploitation, recréez des nœuds uniquement sur des ordinateurs qui utilisent le même système d'exploitation.
- Si vous utilisez un pare-feu, vérifiez que les ports du SIA (Server Intelligence Agent) et du CMS (Central Management Server) sont ouverts.

> ⓘ Remarque
>
> Tous les serveurs à l'exception du CMS doivent être arrêtés avant de pouvoir recréer un nœud.

> → N'oubliez pas
>
> Vous pouvez recréer un nœud uniquement sur l'ordinateur sur lequel se trouve le nœud.

11.13.3.1 Recréation d'un nœud sous Windows

1. Sur la barre d'outils du CCM (Central Configuration Manager), cliquez sur *Ajouter un nœud*.
2. Dans l'*Assistant d'ajout de nœud*, saisissez le nom du nœud et le numéro de port du SIA (Server Intelligence Agent) recréé.

   > ⓘ Remarque
   >
   > Le nœud recréé doit avoir le même nom que le nœud d'origine.

3. Sélectionnez *Recréer le nœud*, puis cliquez sur *Suivant*.
   - Si le nœud existe dans la base de données système du CMS (Central Management Server), il est recréé sur l'hôte local.

> ⚠ Attention
>
> Utilisez cette option uniquement si le nœud n'existe sur aucun hôte du cluster.

- Si le nœud n'existe pas dans la base de données système du CMS, un nouveau nœud comportant les serveurs par défaut est ajouté. Les serveurs par défaut constituent l'ensemble des serveurs installés sur l'hôte.

4. Sélectionnez un CMS.
   - Si votre CMS est en cours d'exécution, sélectionnez *Utiliser le CMS existant en cours d'exécution* puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro de port du CMS existant, les références de connexion Administrateur, le nom de la source de données, les références de connexion à la base de données système ainsi que la clé du cluster.
   - Si votre CMS est arrêté, sélectionnez *Démarrer un nouveau CMS temporaire* puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom de l'hôte du CMS temporaire, les références de connexion Administrateur, le nom de la source de données, les références de connexion à la base de données système ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

     > ⚠ Attention
     >
     > Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.

5. Révisez la page de confirmation et cliquez sur *Terminer*.
   Le CCM recrée le nœud et ajoute à l'ordinateur local des informations sur le nœud. En cas d'erreurs, vérifiez le fichier journal.

Vous pouvez à présent utiliser le CCM pour démarrer le nœud recréé.

11.13.3.1.1 Recréation d'un nœud à l'aide d'un script sous Windows

Vous pouvez utiliser `AddNode.bat` pour recréer un nœud sur un ordinateur Windows. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

En raison des limitations de l'invite de commande, vous devez utiliser le caret (^) pour échapper les espaces, le signe égal (=) et le point-virgule (;) dans ces paramètres, sauf si vous mettez le texte entre guillemets.

```
<REPSCRIPT>\AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
```

```
        -dbkey abc1234
  -adopt
```

> **Remarque**
>
> Pour éviter d'utiliser le caret dans les chaînes longues, vous pouvez écrire le nom du script et tous ses paramètres dans un fichier `response.bat` temporaire, puis exécuter le fichier `response.bat` sans paramètres.

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.3.2 Recréation d'un nœud sous Unix

1. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`
2. Sélectionnez *Ajouter un nœud*, puis appuyez sur `Entrée`.
3. Tapez le nom du nouveau nœud et appuyez sur `Entrée`.

   > **Remarque**
   >
   > Le nœud recréé doit avoir le même nom que le nœud d'origine.

4. Tapez le numéro de port du nouveau SIA et appuyez sur `Entrée`.
5. Sélectionnez *Recréer un nœud*, puis appuyez sur `Entrée`.
   - Si le nœud existe dans la base de données système du CMS (Central Management Server), il est recréé sur l'hôte local.

     > **Attention**
     >
     > Utilisez cette option uniquement si le nœud n'existe sur aucun hôte du cluster.

   - Si le nœud n'existe pas dans la base de données système du CMS, un nouveau nœud comportant les serveurs par défaut est ajouté. Les serveurs par défaut constituent l'ensemble des serveurs installés sur l'hôte.
6. Sélectionnez un CMS.
   - Si votre déploiement est en cours d'exécution, sélectionnez *existing* puis appuyez sur `Entrée`.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro port du CMS existant, les références de connexion Administrateur, les informations de connexion à la base de données et les références de connexion à la base de données système ainsi que la clé du cluster.
   - Si votre déploiement est arrêté, sélectionnez *temporary*, puis appuyez sur `Entrée`.
     Si vous y êtes invité, saisissez le nom de l'hôte du CMS temporaire, les références de connexion Administrateur, les informations de connexion à la base de données et les références de connexion à la base de données système ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

> ⚠ Attention
>
> Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.

7. Révisez la page de confirmation et appuyez sur `Entrée`.
   Le CCM recrée le nœud et ajoute à l'ordinateur local des informations sur le nœud. En cas d'erreurs, vérifiez le fichier journal.

Vous pouvez maintenant exécuter `<REPINSTALL>/sap_bobj/ccm.sh -start <nomNœud>` pour démarrer le nœud recréé.

11.13.3.2.1 Recréation d'un nœud à l'aide d'un script sous Unix

Vous pouvez utiliser `addnode.sh` pour recréer un nœud sur un ordinateur Unix. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.4 Suppression d'un nœud

Vous pouvez supprimer un nœud arrêté à l'aide d'un CCM (Central Configuration Manager) en cours d'exécution ou d'un script de gestion de nœuds. Utilisez les règles suivantes :

- La suppression d'un nœud supprime également de manière définitive les serveurs de ce nœud.

- Si votre cluster comporte plusieurs machines, supprimez les nœuds avant de retirer une machine du cluster et d'en désinstaller le logiciel. Si vous retirez une machine d'un cluster avant de supprimer un nœud ou si le système de fichiers d'un ordinateur fonctionne mal, vous devez recréer le nœud sur un autre ordinateur avec les mêmes serveurs et dans le même cluster, puis supprimer le nœud.

> → N'oubliez pas
>
> Vous pouvez supprimer un nœud uniquement sur l'ordinateur sur lequel se trouve le nœud.

Informations associées

Recréation d'un nœud [page 487]

11.13.4.1 Suppression d'un nœud sous Windows

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après la suppression d'un nœud.

1. Exécutez le CCM (Central Configuration Manager).
2. Dans le CCM, arrêtez le nœud que vous voulez supprimer.
3. Sélectionnez le nœud et cliquez sur *Supprimer le nœud* dans la barre d'outils.
4. A l'invite, saisissez le nom de l'hôte, le port et les références de connexion administrateur du CMS.

Le CMS supprime le nœud et tous les serveurs du nœud.

> ⓘ Remarque
>
> Vous pouvez supprimer un nœud nouvellement ajouté après avoir configuré le SSL à l'aide des deux manières suivantes :
>
> - Supprimez les paramètres SSL du nœud nouvellement créé et du nœud SIA dont vous essayez de connecter les CMS.
> - Ajoutez les paramètres SSL suivants au RemoveNode.bat avant la déclaration de classe principale et exécutez-le : -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.1.1 Suppression d'un nœud à l'aide d'un script sous Windows

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après la suppression d'un nœud.

Vous pouvez utiliser `RemoveNode.bat` pour supprimer un nœud sur un ordinateur Windows. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.4.2 Suppression d'un nœud sous Unix

Avant et après suppression d'un nœud, sauvegardez la configuration des serveurs de l'ensemble du cluster.

1. Exécutez `<REPINSTALL>/sap_bobj/ccm.sh -stop <nomNœud>` pour arrêter le nœud que vous voulez supprimer.
2. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`
3. Sélectionnez *2 - Supprimer un nœud*, puis appuyez sur `Entrée`.
4. Sélectionnez le nœud que vous souhaitez supprimer, puis appuyez sur `Entrée`.
5. A l'invite, saisissez le nom de l'hôte, le numéro de port et les références de connexion administrateur du CMS.

Le nœud et tous les serveurs de ce nœud sont supprimés.

> ⓘ Remarque
>
> Vous pouvez supprimer un nœud nouvellement ajouté après avoir configuré le SSL à l'aide des deux manières suivantes :
>
> - Supprimez les paramètres SSL du nœud nouvellement créé et du nœud SIA dont vous essayez de connecter les CMS.

- Ajoutez les paramètres SSL suivants au RemoveNode.bat avant la déclaration de classe principale et exécutez-le : -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.2.1 Suppression d'un nœud à l'aide d'un script sous Unix

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après la suppression d'un nœud.

Vous pouvez utiliser `removenode.sh` pour supprimer un nœud sur un ordinateur UNIX. Pour en savoir plus, voir la section « Paramètres de script pour ajouter, recréer et supprimer des nœuds ».

Exemple

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Informations associées

Variables [page 481]
Paramètres de script pour ajouter, recréer et supprimer des nœuds [page 499]

11.13.5 Renommer un nœud

Vous pouvez renommer un nœud à l'aide du CCM (Central Configuration Manager). Pour renommer un nœud, vous devez créer un nœud ayant un nouveau nom, cloner les serveurs du nœud d'origine vers le nouveau nœud, puis supprimer le nœud d'origine. Utilisez les règles suivantes :

- Si vous renommez l'ordinateur où se trouve le nœud, il est inutile de renommer le nœud. Vous pouvez continuer à utiliser le nom de nœud existant.
- Si vous utilisez un pare-feu, vérifiez que les ports du SIA (Server Intelligence Agent) et du CMS (Central Management Server) sont ouverts.

→ N'oubliez pas

Vous pouvez renommer un nœud uniquement sur l'ordinateur sur lequel se trouve le nœud.

Informations associées

Ajout d'un nœud [page 482]
Suppression d'un nœud [page 490]

11.13.5.1 Pour renommer un nœud sous Windows

⚠ Attention

Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après avoir renommé un nœud.

1. Démarrez le Central Configuration Manager (CCM).
2. Sur la barre d'outils du CCM (Central Configuration Manager), cliquez sur *Ajouter un nœud*.
3. Dans l'*Assistant d'ajout de nœud*, saisissez le nom du nœud et le numéro de port du nouveau SIA (Server Intelligence Agent), les références de connexion Administrateur, les informations de connexion à la base de données, les références de connexion à la base de données système ainsi que la clé du cluster.
4. Sélectionnez *Ajouter un nœud sans serveur*.
5. Après la création du nœud, utilisez la page *Gestion des serveurs* de la Central Management Console pour cloner l'ensemble des serveurs du nœud d'origine vers le nouveau nœud.

   ⓘ Remarque

   Vérifiez que les serveurs clonés n'ont pas de conflit de port avec les serveurs de l'ancien nœud.
6. Dans le CCM, démarrez le nouveau nœud.
7. Après exécution du nouveau nœud pendant cinq minutes, utilisez le CCM pour supprimer le nœud d'origine.

Informations associées

Ajout d'un nœud [page 482]
Suppression d'un nœud [page 490]

11.13.5.2 Renommer un nœud sous Unix

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après avoir renommé un nœud.

1. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`.
2. Sélectionnez *Ajouter un nœud*, puis appuyez sur `Entrée`.
3. Tapez le nom du nouveau nœud et appuyez sur `Entrée`.
4. Tapez le numéro de port du nouveau SIA et appuyez sur `Entrée`.
5. Si vous y êtes invité, saisissez les références de connexion Administrateur, les informations de connexion à la base de données, les références de connexion à la base de données système ainsi que la clé du cluster.
6. Sélectionnez *aucun serveur*, puis appuyez sur `Entrée`.
7. Après la création du nœud, utilisez la page *Gestion des serveurs* de la Central Management Console pour cloner l'ensemble des serveurs du nœud d'origine vers le nouveau nœud.

   > ⓘ Remarque
   >
   > Vérifiez que les serveurs clonés n'ont pas de conflit de port avec les serveurs de l'ancien nœud.

8. Exécutez `<REPINSTALL>/sap_bobj/ccm.sh -start <nomNœud>` pour démarrer le nouveau nœud.
9. Après exécution du nouveau nœud pendant cinq minutes, utilisez `serverconfig.sh`pour supprimer le nœud d'origine.

Informations associées

Ajout d'un nœud [page 482]
Clonage des serveurs [page 438]
Suppression d'un nœud [page 490]

11.13.6 Déplacement d'un nœud

Vous pouvez déplacer un nœud arrêté d'un cluster à un autre à l'aide du CCM (Central Configuration Manager) ou d'un script de gestion de nœuds. Utilisez les règles suivantes :

- Vérifiez que le cluster de destination ne possède pas de nœud du même nom.
- Vérifiez que tous les types de serveur installés sur l'ordinateur où est situé le nœud source sont également installés sur le cluster de destination.
- Si vous voulez ajouter un ordinateur à un cluster de production sans que l'ordinateur ne soit utilisable tant que vous n'avez pas fini de le tester, installez la plateforme de BI sur un ordinateur autonome, testez-le puis déplacez le nœud vers un cluster de production.
- Le niveau de version et de Service Pack de la plateforme de BI de cet ordinateur doit être cohérent avec le reste du cluster.

→ N'oubliez pas

Vous pouvez déplacer un nœud uniquement sur l'ordinateur sur lequel se trouve le nœud.

11.13.6.1 Déplacement d'un nœud existant sous Windows

Dans cet exemple, le nœud à déplacer est installé sur le système source. L'ordinateur du système source faisait initialement partie d'une installation autonome, mais il va désormais être ajouté au cluster de destination.

⚠ Attention

Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après le déplacement d'un nœud.

1. Arrêtez le nœud dans le CCM (Central Configuration Manager)
2. Cliquez avec le bouton droit sur le nœud et sélectionnez *Déplacer*.
3. Si vous y êtes invité, sélectionnez le nom de la source de données et saisissez le nom d'hôte, le port, les informations de connexion à la base de données, les références de connexion Administrateur du CMS de destination ainsi que la clé du cluster.
4. Sélectionnez un CMS.
   - Si votre déploiement source est en cours d'exécution, sélectionnez *Utiliser le CMS existant en cours d'exécution*, puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro de port du CMS existant du système source ainsi que les références de connexion Administrateur.
   - Si votre déploiement source est arrêté, sélectionnez *Démarrer un nouveau CMS temporaire* puis cliquez sur *Suivant*.
     Si vous y êtes invité, saisissez le nom d'hôte et le numéro port du CMS temporaire du système source, les références de connexion Administrateur, le nom de la source de données, les références de connexion à la base de données pour la base de données système source ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

     ⚠ Attention

     Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.
5. Révisez la page de confirmation et cliquez sur *Terminer*.
   Le CCM crée un nœud sur le cluster de destination comportant le même nom et les mêmes serveurs que le nœud du cluster source. Une copie du nœud reste sur le cluster source. Les modèles de configuration des serveurs dans le nœud ne sont pas déplacés. En cas d'erreurs, vérifiez le fichier journal.

   ⚠ Attention

   N'utilisez pas le cluster source après le déplacement du nœud.
6. Dans le CCM, démarrez le nœud déplacé.

11.13.6.1.1 Déplacement d'un nœud à l'aide d'un script sous Windows

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après le déplacement d'un nœud.

Vous pouvez utiliser `MoveNode.bat` pour déplacer un nœud sur un ordinateur Windows. Pour en savoir plus, voir la section « Paramètres de script pour déplacer des nœuds ».

Exemple

En raison des limitations de l'invite de commande, vous devez utilisez le caret (^) pour échapper les espaces, le signe égale (=) et le point-virgule (;) dans ces paramètres, sauf si vous mettez le texte entre guillemets.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> ⓘ Remarque
>
> Pour éviter d'utiliser le caret dans les chaînes longues, vous pouvez écrire le nom du script et tous ses paramètres dans un fichier `response.bat` temporaire, puis exécuter le fichier `response.bat` sans paramètres.

Informations associées

Variables [page 481]
Paramètres de script pour le déplacement de nœuds [page 501]

11.13.6.2 Déplacement d'un nœud existant sous Unix

Dans cet exemple, le nœud à déplacer est installé sur le système source. L'ordinateur du système source faisait initialement partie d'une installation autonome, mais il va désormais être ajouté au cluster de destination.

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après le déplacement d'un nœud.

1. Exécutez `<REPINSTALL>/sap_bobj/ccm.sh -stop <nomNœud>` pour arrêter le nœud.
2. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`
3. Sélectionnez *4 - Déplacer un nœud*, puis appuyez sur `Entrée`.
4. Sélectionnez le nœud que vous souhaitez déplacer, puis appuyez sur `Entrée`.
5. Quand vous y êtes invité, sélectionnez les informations de connexion à la base de données système et saisissez le nom d'hôte, le port, les références de connexion Administrateur pour le CMS de destination ainsi que la clé du cluster.
6. Sélectionnez un CMS.
   - Si votre déploiement source est en cours d'exécution, sélectionnez *existant* puis appuyez sur `Entrée`. Si vous y êtes invité, saisissez le nom d'hôte et le numéro de port du CMS existant du système source ainsi que les références de connexion Administrateur.
   - Si votre déploiement source est arrêté, sélectionnez *temporaire* puis appuyez sur `Entrée`. Si vous y êtes invité, saisissez le nom d'hôte et le port du CMS temporaire du système source, les références de connexion Administrateur, les informations de connexion à la base de données, les références de connexion à la base de données système source ainsi que la clé du cluster. Un CMS temporaire va démarrer. (Il s'arrêtera à la fin de ce processus.)

     > ⚠ Attention
     >
     > Evitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existant et temporaire utilisent des ports différents.
7. Révisez la page de confirmation et appuyez sur `Entrée`.
   Le CCM crée un nœud sur le cluster de destination comportant le même nom et les mêmes serveurs que le nœud du cluster source. Une copie du nœud reste sur le cluster source. Les modèles de configuration des serveurs dans le nœud ne sont pas déplacés. En cas d'erreurs, vérifiez le fichier journal.

   > ⚠ Attention
   >
   > N'utilisez pas le cluster source après le déplacement du nœud.
8. Exécutez `<REPINSTALL>/sap_bobj/ccm.sh -start <nomNœud>` pour démarrer le nœud déplacé.

11.13.6.2.1 Déplacement d'un nœud à l'aide d'un script sous Unix

> ⚠ Attention
>
> Sauvegardez la configuration de serveur pour l'ensemble du cluster avant et après le déplacement d'un nœud.

Vous pouvez utiliser `movenode.sh` pour déplacer un nœud sur un ordinateur Unix. Pour en savoir plus, voir la section « Paramètres de script pour déplacer des nœuds ».

Exemple

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

Informations associées

Variables [page 481]
Paramètres de script pour le déplacement de nœuds [page 501]

11.13.7 Paramètres de script

11.13.7.1 Paramètres de script pour ajouter, recréer et supprimer des nœuds

Paramètre	Description	Exemple
`-adopt`	Recrée le nœud s'il existe déjà dans le CMS.	**`-adopt`**
`-cms`	Nom et numéro de port du CMS (Central Management Server). **⚠ Attention** N'utilisez pas ce paramètre si vous utilisez `-usetempcms` **ⓘ Remarque** Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.	**`-cms mycms:6409`**

Paramètre	Description	Exemple
`-cmsport`	• Numéro de port du CMS lors du démarrage d'un CMS temporaire. **⚠ Restriction** Vous devez également utiliser les paramètres `-usetempcms`, `-dbdriver`, `-connect` et `-dbkey`. • Numéro de port du CMS lors de la création d'un CMS. **⚠ Restriction** Vous devez également utiliser les paramètres `-dbdriver`, `-connect` et `-dbkey`.	**`-cmsport 6401`**
`-connect`	Chaîne de connexion de la base de données système du CMS (ou du CMS temporaire). **ⓘ Remarque** Ignorez les attributs HOSTNAME et PORT lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.	**`-connect "DSN=BusinessObjects CMS 140;UID=nom_utilisateur;PWD=mot_de_passe;HOSTNAME=base_de_données;PORT=3306"`**
`-dbdriver`	Pilote de la base de données du CMS. Valeurs acceptées : • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	Clé du cluster.	**`-dbkey abc1234`**
`-name`	Nom d'un nœud.	**`-name mynode2`**
`-noservers`	Crée un nœud sans serveurs. **ⓘ Remarque** Le paramètre supplémentaire `-createcms` crée un nœud avec un CMS, mais avec aucun autre serveur. Ignorez ces paramètres pour créer un nœud avec tous les serveurs par défaut.	**`-noservers`**

Paramètre	Description	Exemple
`-password`	Mot de passe du compte Administrateur.	`-password MotDePasse1`
`-siaport`	Numéro de port du Server Intelligence Agent pour le nœud.	`-siaport 6409`
`-username`	Nom d'utilisateur du compte Administrateur.	`-username Administrator`
`-usetempcms`	⚠ Attention N'utilisez pas ce paramètre si vous utilisez `-cms` Démarre et utilise le CMS temporaire. ⓘ Remarque Utilisez un CMS temporaire lorsque votre déploiement n'est pas en cours d'exécution.	`-usetempcms`

Informations associées

Ajout d'un nœud à l'aide d'un script sous Windows [page 484]
Ajout d'un nœud à l'aide d'un script sous Unix [page 486]
Recréation d'un nœud à l'aide d'un script sous Windows [page 488]
Recréation d'un nœud à l'aide d'un script sous Unix [page 490]
Suppression d'un nœud à l'aide d'un script sous Windows [page 492]
Suppression d'un nœud à l'aide d'un script sous Unix [page 493]

11.13.7.2 Paramètres de script pour le déplacement de nœuds

Paramètre	Description	Exemple
`-cms`	Nom du CMS (Central Management Server) source. ⚠ Attention N'utilisez pas ce paramètre si vous utilisez `-usetempcms` ⓘ Remarque Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.	`-cms sourceMachine:6409`

Paramètre	Description	Exemple
`-cmsport`	• Numéro de port du CMS lors du démarrage d'un CMS temporaire. **⚠ Restriction** Vous devez également utiliser les paramètres `-usetempcms`, `-dbdriver`, `-connect` et `-dbkey`. • Numéro de port du CMS lors de la création d'un CMS. **⚠ Restriction** Vous devez également utiliser les paramètres `-dbdriver`, `-connect` et `-dbkey`.	**`-cmsport 6401`**
`-connect`	Chaîne de connexion de la base de données système du CMS source (ou du CMS temporaire). **ⓘ Remarque** Ignorez les attributs HOSTNAME et PORT lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.	**`-connect "DSN=Source BOEXI40;UID=nom_utilisateur;PWD=mot_de_passe;HOSTNAME=base_de_données;PORT=3306"`**
`-dbdriver`	Pilote de la base de données du CMS source. Valeurs acceptées : • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	Clé du cluster source.	**`-dbkey abc1234`**
`-destcms`	Nom du CMS de destination. **ⓘ Remarque** Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.	**`-destcms destinationMachine:6401`**

Paramètre	Description	Exemple
`-destconnect`	Chaîne de connexion de la base de données système du CMS de destination. **Remarque** Ignorez les attributs `HOSTNAME` et `PORT` lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.	**`-destconnect "DSN=Destin BOEXI40;UID=nom_utilisateur;PWD= mot_de_passe;HOSTNAME=base_de_do nnées;PORT=3306"`**
`-destdbdriver`	Pilote de la base de données du CMS de destination. Valeurs acceptées : • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-destdbdriver sybasedatabasesubsystem`**
`-destdbkey`	Clé du cluster de destination.	**`-destdbkey def5678`**
`-destpassword`	Mot de passe du compte Administrateur sur le CMS de destination.	**`-destpassword Password2`**
`-destusername`	Nom d'utilisateur du compte Administrateur sur le CMS de destination.	**`-destusername Administrator`**
`-password`	Mot de passe du compte Administrateur sur le CMS source.	**`-password MotDePasse1`**
`-username`	Nom d'utilisateur du compte Administrateur sur le CMS source.	**`-username Administrator`**
`-usetempcms`	**Attention** N'utilisez pas ce paramètre si vous utilisez `-cms` Démarre et utilise le CMS temporaire. **Remarque** Utilisez un CMS temporaire lorsque votre déploiement n'est pas en cours d'exécution.	**`-usetempcms`**

Informations associées

Déplacement d'un nœud à l'aide d'un script sous Windows [page 497]

Déplacement d'un nœud à l'aide d'un script sous Unix [page 498]

11.13.8 Ajout des dépendances de serveurs Windows

Dans un environnement Windows, chaque instance du SIA (Server Intelligence Agent) dépend du journal des événements et des services d'appel de procédures distantes (RPC).

Dans le cas où un SIA ne fonctionne pas correctement, vérifiez que les deux services apparaissent dans l'onglet *Dépendance* du SIA.

11.13.8.1 Ajout des dépendances de serveurs Windows

1. Utilisez le CCM (Central Configuration Manager) pour arrêtez le SIA (Server Intelligence Agent).
2. Cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*.
3. Cliquez sur l'onglet *Dépendance*.
4. Cliquez sur *Ajouter*.
   La boîte de dialogue *Ajouter une dépendance* s'ouvre et affiche la liste de toutes les dépendances possibles.
5. Sélectionnez une dépendance, puis cliquez sur *Ajouter*.
6. Cliquez sur *OK*.
7. Utilisez le CCM pour redémarrer le SIA.

11.13.9 Modification des références de connexion utilisateur pour un nœud

Vous pouvez utiliser le CCM (Central Configuration Manager) pour spécifier ou mettre à jour les références de connexion au SIA (Server Intelligence Agent) si le mot de passe du système d'exploitation change ou si vous voulez exécuter tous les serveurs d'un nœud sous un compte utilisateur différent.

Tous les serveurs gérés par le SIA s'exécutent sous le même compte. Pour exécuter un serveur à l'aide d'un compte extérieur au système, vérifiez que votre compte est membre du groupe Administrateurs locaux sur l'ordinateur du serveur et qu'il dispose du droit « Remplacer un jeton de niveau processus ».

> **⚠ Restriction**
>
> Sur un ordinateur Unix, vous devez exécuter la plateforme de BI avec le compte utilisé pour l'installation. Pour utiliser un compte différent, réinstallez le déploiement à l'aide d'un compte différent.

11.13.9.1 Modification des références de connexion utilisateur pour un nœud sous Windows

1. Utilisez le CCM (Central Configuration Manager) pour arrêtez le SIA (Server Intelligence Agent).
2. Cliquez avec le bouton droit sur le SIA et sélectionnez *Propriétés*.
3. Désactivez la case à cocher *Compte de système*.
4. Saisissez un nom d'utilisateur et un mot de passe, puis cliquez sur *OK*.
5. Utilisez le CCM pour redémarrer le SIA.

Le SIA et les processus du serveur se connectent à l'ordinateur local avec le nouveau compte utilisateur.

11.14 Renommage d'un ordinateur dans un déploiement de plateforme de BI

11.14.1 Modification du nom des clusters

Meilleures pratiques pour renommer les clusters :

> ⚠ Attention
>
> Ne jamais déployer plusieurs clusters ayant le même nom.

Condition	Action
Le nom du cluster change.	Informez vos utilisateurs du nouveau nom de cluster et demandez-leur de l'utiliser (après la première connexion au CMS en utilisant la syntaxe `<nomhôte>:<port>`). Au niveau Web, mettez à jour le nom du cluster dans les fichiers de propriétés de tous les serveurs d'applications Web.
Vous installez une version différente de la plateforme de BI sur un ordinateur qui exécutait auparavant un CMS ou vous ajoutez l'ordinateur à un cluster différent.	• vérifiez que le nouveau CMS s'exécute sur un port différent. • Utilisez des mots de passe distincts pour les différents clusters afin d'empêcher les utilisateurs de se connecter à un cluster erroné.

11.14.2 Modification des adresses IP

Pour éviter des changements de configuration découlant de modifications de l'adresse IP de l'ordinateur, sélectionnez *Propriétés du serveur* dans l'onglet *Serveurs* de la CMC, puis vérifiez que tous les serveurs sont liés à des noms d'hôte ou utilisez l'option *Affecter automatiquement*. En outre, respectez ces meilleures pratiques :

Condition	Action
Vous utilisez ODBC avec la base de données du CMS ou la base de données d'audit.	Vérifiez que le DSN utilise le nom d'hôte du serveur de la base de données du CMS.
Vous utilisez un autre type de connexion avec la base de données du CMS ou la base de données d'audit.	Utilisez le CCM pour mettre à jour la base de données afin qu'elle utilise le nom d'hôte du serveur de base de données.
La base de données du CMS ou la base de données d'audit se trouve sur le même hôte que le CMS.	Utilisez `localhost` comme nom de l'ordinateur.
Vous utilisez l'URL des applications Web de la plateforme de BI auxquelles les utilisateurs accèdent à l'aide de navigateurs Web (par exemple, la CMC).	Utilisez des noms d'hôte au lieu d'adresses IP pour l'URL par défaut. Pour mettre à jour l'URL du visualiseur par défaut, sélectionnez les *Paramètres de traitement* de l'application sélectionnée. Par exemple, pour Open Document, cliquez sur l'onglet *Applications* dans la CMC, cliquez avec le bouton droit sur *Open Document* et sélectionnez *Paramètres de traitement*.
Vous utilisez l'URL des clients de la plateforme de BI basés sur des services Web (par exemple, Crystal Reports pour Java ou LiveOffice).	
Vous utilisez OpenDocument.	

Règles alternatives

> **ⓘ Remarque**
>
> Suivez ces règles uniquement si vous ne pouvez pas respecter les meilleures pratiques décrites ci-dessus.

Pour les ordinateurs hébergeant des serveurs

Condition	Action
L'hôte héberge des serveurs de la plateforme de BI qui doivent être liés à des adresses IP spécifiques.	Modifiez les adresses IP dans l'onglet *Serveurs* de la CMC, mais ne redémarrez pas les serveurs tant que tout n'a pas été mis à jour sur l'ordinateur. Redémarrez ensuite l'ordinateur et non chaque serveur de la plateforme de BI.
Une connexion de base de données doit utiliser une adresse IP.	Modifiez l'adresse IP.
Une adresse IP est requise dans un réseau IP statique.	Modifiez l'adresse IP de l'ordinateur de la plateforme de BI. **→ Conseil** Connectez-vous à la CMC pour vérifier que la plateforme de BI est opérationnelle.

> **→ N'oubliez pas**
>
> Redémarrez l'ordinateur après exécution d'une action.

Pour les ordinateurs hébergeant le serveur d'applications Web

Condition	Action
L'URL du visualiseur OpenDocument par défaut doit utiliser une adresse IP.	Mettez à jour l'adresse IP dans le champ *URL du visualiseur par défaut* de la section *Paramètres de traitement* dans l'onglet *Applications* de la CMC.
Vos utilisateurs accèdent aux applications Web de la plateforme de BI (la CMC, par exemple) en fournissant dans leurs navigateurs une URL qui comporte une adresse IP.	Informez les utilisateurs de la nouvelle adresse IP.
Les clients de la plateforme de BI basés sur des services Web (par exemple, Crystal Reports pour Java ou LiveOffice) doivent utiliser des adresses IP.	Configurez tous les clients pour qu'ils utilisent la nouvelle adresse IP.

Informations associées

Sélection d'une base de données CMS (nouvelle ou existante) [page 515]

11.14.3 Renommage des ordinateurs

Vous pouvez renommer les ordinateurs d'un déploiement de la plateforme de BI à tout moment en arrêtant tous les serveurs de la plateforme de BI hébergés par l'ordinateur, puis en renommant ce dernier. Meilleures pratiques pour renommer les ordinateurs :

Condition	Action
Vous vous connectez pour la première fois.	Utilisez le nom de l'ordinateur du CMS (plutôt que le nom du cluster).
Votre déploiement comporte plusieurs ordinateurs.	Vérifiez que tous les serveurs de CMS sur tous les autres ordinateurs sont en cours d'exécution pendant le renommage.

11.14.3.1 Niveau serveur

> **ⓘ Remarque**
>
> Avant de renommer l'ordinateur du CMS, inspectez la configuration de tous les serveurs hébergés sur l'ordinateur que vous désirez renommer dans l'onglet « Gestion des serveurs » de la CMC. Si la propriété *Nom d'hôte* utilise l'ancien nom d'hôte du CMS, actualisez-la en lui donnant le nouveau nom d'hôte du CMS.

> **→ N'oubliez pas**
>
> Ne redémarrez pas les serveurs tant que vous n'avez pas terminé toutes les procédures de renommage des ordinateurs.

Suivez ces instructions pour renommer les ordinateurs du niveau serveur :

Condition	Action
L'ordinateur renommé héberge un CMS et les utilisateurs se sont connectés auparavant en fournissant le nom de l'ancien ordinateur.	Informez les utilisateurs du nom de l'ordinateur du CMS et demandez-leur de l'utiliser.
L'ordinateur renommé héberge un CMS et les fichiers de propriétés par défaut des applications Web de la plateforme de BI contiennent l'ancien nom d'hôte du CMS dans la propriété `cms.default`.	Mettez à jour le nom de l'ordinateur du CMS dans la propriété `cms.default` de tous les fichiers de propriétés personnalisés sur tous les ordinateurs du niveau Web. Sous Tomcat, les fichiers de propriétés que vous créez se trouvent par défaut à l'emplacement `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`. **Remarque** S'il n'existe aucun fichier de propriétés personnalisé, créez-en. Copiez les fichiers de propriétés par défaut dans un dossier personnalisé, puis supprimez tout le contenu, sauf la ligne `cms.default` des fichiers de propriétés personnalisés.
Vous utilisez des kits d'intégration de portail ou des applications personnalisées.	Configurez les kits d'intégration de portail ou les applications personnalisées afin qu'elles utilisent le nouveau nom d'hôte du CMS.
Votre déploiement répond à toutes les conditions suivantes : • Un cluster comporte plusieurs nœuds. • Tous les serveurs du CMS s'exécutent uniquement sur l'ordinateur ayant été renommé. • Au moins un des nœuds n'héberge pas le CMS. • Vous renommez un ordinateur comportant au moins un nœud. • L'adresse IP est modifiée durant le processus de renommage.	Utilisez le CCM pour appliquer le workflow « Recréer le nœud »à tous les nœuds, sauf celui qui héberge le CMS, puis démarrez tous les nœuds de la plateforme de BI existant dans le déploiement. Pour en savoir plus, voir le chapitre « Gestion des nœuds ».

→ N'oubliez pas

Redémarrez l'application Web ou le serveur d'applications après avoir exécuté une action.

Informations associées

Recréation d'un nœud [page 487]

11.14.3.2 Niveau Web

Si vous renommez l'ordinateur qui héberge le serveur d'applications Web de la plateforme de BI, suivez ces instructions :

Condition	Action
Vous modifiez le nom de l'ordinateur qui héberge le serveur d'applications Web de la plateforme de BI et l'URL du visualiseur OpenDocument par défaut utilise un nom d'hôte de serveur d'applications Web.	Connectez-vous à la CMC et mettez à jour l'URL du visualiseur par défaut dans *Applications* > *CMC* > *Paramètres de traitement*.
Vous modifiez le nom de l'ordinateur qui héberge le serveur d'applications Web de la plateforme de BI et vos utilisateurs accèdent aux applications Web de la plateforme de BI en utilisant une URL qui comprend un nom d'hôte de serveur d'applications Web.	Demandez à vos utilisateurs d'accéder aux applications Web de la plateforme de BI en utilisant une URL qui comprend le nouveau nom d'hôte de serveur d'applications Web.
Vous modifiez le nom de l'ordinateur qui héberge le serveur d'applications Web de la plateforme de BI et les clients basés sur les services Web de la plateforme de BI utilisent des noms d'hôte de serveur d'applications Web dans l'URL.	Reconfigurez tous les clients basés sur les services Web de la plateforme de BI pour qu'ils utilisent le nouveau nom d'hôte du serveur d'applications Web.

11.14.3.3 Bases de données

Si vous renommez l'ordinateur hébergeant la base de données système du CMS ou la base de données d'audit, respectez ces meilleures pratiques :

Condition	Action
Vous voulez éviter de mettre à jour l'adresse IP.	Utilisez le nom de l'ordinateur hébergeant la base de données du CMS ou la base de données d'audit dans le nom de source de données (DSN).
La base de données du CMS ou la base de données d'audit se trouve sur le même hôte que le CMS.	Utilisez `localhost` dans le DSN pour éviter une mise à jour si le nom d'hôte est modifié.

Base de données système du CMS

Condition	Action
Vous renommez un ordinateur qui héberge la base de données système du CMS et vous utilisez ODBC.	Mettez à jour le DSN de la base de données du CMS en lui donnant le nouveau nom d'hôte du serveur de base de données.
Vous renommez un ordinateur qui héberge la base de données système du CMS et vous utilisez un type de connexion autre qu'ODBC.	Utilisez le CCM pour mettre à jour la base de données du CMS en lui donnant le nouveau nom d'hôte du serveur de base de données dans chaque nœud du cluster.

Base de données d'audit

Condition	Action
Vous renommez un ordinateur qui héberge la base de données d'audit et vous utilisez ODBC.	Mettez à jour le DSN de la base de données d'audit en lui donnant le nouveau nom d'hôte du serveur de base de données.
Vous renommez un ordinateur qui héberge la base de données d'audit et vous utilisez un type de connexion autre qu'ODBC.	Mettez à jour le nom d'ordinateur du serveur de base de données en lui donnant le nouveau nom d'hôte du serveur de base de données dans l'onglet *Audit* de la CMC.

11.14.3.4 File Repository Servers

Si vous renommez l'ordinateur qui héberge le stockage de fichiers du FRS, vous devez mettre à jour les serveurs de l'*Input File Repository* et de l'*Output File Repository* dans la page « Gestion des serveurs » de la CMC, puis vérifier que les propriétés *Répertoire de stockage des fichiers* et *Répertoire temporaire* utilisent le nouveau chemin du stockage de fichiers avant de redémarrer les serveurs.

11.15 Utilisation des bibliothèques tierces 32 bits et 64 bits avec la plateforme de BI

Les serveurs de la plateforme de BI sont une combinaison de processus 32 bits et 64 bits. Certains serveurs lancent en outre des processus enfant 32 bits et 64 bits. Pour utiliser la bonne version des bibliothèques tierces (32 bits ou 64 bits) avec les processus de la plateforme de BI, vous devez définir des variables d'environnement 32 bits et 64 bits distinctes sur les ordinateurs hébergeant la plateforme de BI. Vous devez alors définir une variable d'environnement supplémentaire qui contient une liste séparée par des virgules des variables d'environnement qui ont des versions 32 bits et 64 bits. Lorsqu'un processus est lancé par la plateforme de BI, il sélectionne la variable correspondante selon qu'il s'agit d'un processus 32 bits ou 64 bits.

- `<FIRST_ENV_VAR>`= La valeur à utiliser par les processus 64 bits de la plateforme de BI.
- `<FIRST_ENV_VAR32>` = La valeur à utiliser par les processus 32 bits.
- `<SECOND_ENV_VAR>` = La valeur à utiliser par les processus 64 bits.
- `<SECOND_ENV_VAR32>` = La valeur à utiliser par les processus 32 bits.
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

Par exemple, si vous avez installé la plateforme de BI sur un ordinateur AIX ainsi que les clients Oracle 32 bits et 64 bits et que vous devez définir la variable LIBPATH, définissez les variables suivantes :

- ORACLE_HOME=`<répertoire d'accueil de la version 64 bits du client Oracle>`
- ORACLE_HOME32=`<répertoire d'accueil de la version 32 bits>`
- LIBPATH=`<chemin d'accès à la bibliothèque de la version 64 bits>`
- LIBPATH32=`<chemin d'accès à la bibliothèque de la version 32 bits>`
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Remarque**
>
> Sous Linux et Solaris, n'utilisez pas BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH pour séparer les chemins 32 bits et 64 bits. Ajoutez plutôt les chemins 32 bits et 64 bits à LD_LIBRARY_PATH.

11.16 Gestion des espaces réservés de nœuds et de serveurs

11.16.1 Visualisation des espaces réservés de serveur

Dans la zone de gestion *Serveurs* de la CMC, cliquez avec le bouton droit de la souris sur un serveur et sélectionnez *Espaces réservés*.
La boîte de dialogue *Espaces réservés* affiche la liste des espaces réservés de tous les serveurs situés sur le même cluster que le serveur sélectionné. Pour modifier la valeur d'un espace réservé, modifiez l'espace réservé du nœud.

Informations associées

Espaces réservés de nœud et de serveur [page 1230]

11.16.2 Visualisation et modification des espaces réservés d'un nœud

1. Dans la zone de gestion *Serveurs* de la CMC (Central Management Console), cliquez avec le bouton droit de la souris sur le nœud pour lequel vous voulez modifier les espaces réservés, puis sélectionnez *Espaces réservés*.
2. Pour modifier l'un des paramètres des espaces réservés, apportez les modification souhaitées, puis cliquez sur *Enregistrer* pour continuer.

   > **Attention**
   >
   > Les espaces réservés non destinés à la modification ne doivent en aucun cas être modifiés. L'administrateur système doit s'assurer que seule la personne appropriée du groupe d'administrateurs (qui assure la gestion des nœuds) dispose de droits de modification sur le nœud. Tous les autres utilisateurs, y compris les autres membres du groupe d'administrateurs, doivent disposer de droits limités à l'affichage/la gestion des objets du nœud. Les droits de sécurité appropriés doivent donc s'appliquer. Si l'une des valeurs d'espace réservé est accidentellement corrompue et que le CMS n'apparaît pas, reportez-vous à la note SAP 3269127.

> **Remarque**
>
> Reportez-vous à l'article 3278916 de la base de connaissances SAP pour savoir comment limiter la modification des espaces réservés et ainsi éviter toute interférence malveillante avec l'infrastructure BI.

Informations associées

Espaces réservés de nœud et de serveur [page 1230]

12 Gestion des bases de données du Central Management Server (CMS)

12.1 Gestion des connexions à la base de données système du CMS

Si la base de données système du CMS n'est pas disponible, en raison d'une défaillance matérielle, d'un problème logiciel ou d'un problème réseau par exemple, le CMS passe à l'état « En attente de ressources ». Si le déploiement de la plateforme de BI comporte plusieurs CMS, les requêtes suivantes issues des autres serveurs sont transmises aux CMS qui figurent dans le cluster ayant une connexion active à la base de données système. Lorsqu'un CMS est « En attente de ressources », toutes les requêtes en cours ne nécessitant pas d'accès à la base de données continuent à être traitées, mais les requêtes nécessitant un accès à la base de données du CMS échouent.

Par défaut, un CMS « En attente de ressources » essaie régulièrement de rétablir le nombre de connexions spécifié dans la propriété « Connexions à la base de données système requises ». Dès qu'au moins une connexion à la base de données est établie, le CMS synchronise toutes les données nécessaires, passe à l'état « En cours d'exécution » et reprend les opérations normales.

Dans certains cas, vous pouvez vouloir empêcher le CMS de rétablir automatiquement une connexion à la base de données. Par exemple, vous pouvez vouloir vérifier l'intégrité de la base de données avant que les connexions à la base de données ne soient rétablies. Pour ce faire, dans la page *Propriétés* du CMS, désactivez la case à cocher *Reconnexion automatique à la base de données système*.

Informations associées

Pour modifier les propriétés d'un serveur [page 468]

12.1.1 Sélection de SQL Anywhere comme base de données du CMS

Pour utiliser SQL Anywhere comme base de données du CMS, vous devez procéder comme suit :

1. Arrêtez tous les nœuds du système.
2. Exécutez l'application appropriée.
   - Sous UNIX, exécutez `./cmsdbsetup.sh`.
   - Sous Windows, démarrez le CCM (Central Configuration Manager).

3. Copiez vos données à partir de la base de données du CMS par défaut en sélectionnant SQL Anywhere comme base de données de destination. Pour en savoir plus, voir le lien associé « Copie de données d'une base de données système du CMS dans une autre ».
4. Sur les déploiements de nœuds multiples, mettez à jour la source de données du CMS sur tous les nœuds (sauf celui où vous copiez la base de données) afin d'indiquer la nouvelle base de données SQL Anywhere. Pour en savoir plus, voir le lien associé « Sélection d'une base de données du CMS (nouvelle ou existante) »
5. Vérifiez que le déploiement est opérationnel (par exemple, connectez-vous à la CMC et visualisez un rapport).

Informations associées

Copie de données d'une base de données système d'un CMS dans une autre [page 520]
Sélection d'une base de données CMS (nouvelle ou existante) [page 515]

12.1.2 Sélection de SAP HANA comme base de données du CMS

Pour utiliser SAP HANA comme base de données du CMS, vous devez procéder comme suit.

1. Installez la plateforme de BI avec la base de données du CMS par défaut.
2. Installez le client SAP HANA.
3. Créez une connexion vers SAP HANA.
   - Sur Unix, vérifiez la variable d'environnement `ODBCINI`. Si la variable existe et qu'elle pointe vers un fichier `odbc.ini` existant, ajoutez les lignes suivantes à ce fichier :

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>
     [NewDB]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` correspond à la version de SAP HANA, par exemple « NewDB 1.0 », `<HANA Server IP address>` correspond à l'adresse IP du serveur SAP HANA et `<HANA server port #>` correspond au numéro de port du serveur SAP HANA.
     Si la variable d'environnement `ODBCINI` n'existe pas, créez un fichier `odbc.ini` dans le répertoire `<REPINSTALL>/sap_bobj/enterprise_xi40/`, ajoutez les lignes ci-dessus au fichier, puis définissez la variable d'environnement `ODBCINI` comme suit :

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

     Vérifiez que la variable d'environnement ODBCINI est définie dans le profil de l'utilisateur qui démarre les serveurs de BI.
   - Sous Windows, créez une connexion ODBC vers SAP HANA.

> **Remarque**
>
> Pour les modifications de connexion ODBC, assurez-vous que vous exécutez la version 64 bits de l'administrateur de source de données ODBC : *Démarrer* > *Panneau de configuration* > *Outils d'administration* > *Sources de données (ODBC)*.

4. Assurez-vous que les connexions vers le serveur SAP HANA peuvent être établies.
   - Sous UNIX, vous pouvez tester la connexion au serveur SAP HANA en exécutant la commande suivante : Les variables de l'exemple suivant font référence à l'installation de SAP HANA :

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
     <NONADMINUSER> <NONADMINPASSWORD>
     ```

   - Sous Windows, vous pouvez utiliser l'administrateur de sources de données ODBC pour tester la connexion ODBC SAP HANA.
5. Sous Unix, vérifiez que les variables d'environnement `LD_LIBRARY_PATH` et `LIBPATH` contiennent le chemin d'accès à `libodbcHDB.so`. Pour en savoir plus, consultez les notes SAP 2792543, 1886746 et 2721890.
6. Installez le produit à l'aide de l'assistant et sélectionnez SAP HANA comme base de données du CMS ou d'audit.
7. Vérifiez que le déploiement est opérationnel (par exemple, connectez-vous à la CMC et visualisez un rapport).

> **Remarque**
>
> Cette procédure ne s'applique pas si vous passez d'une base de données existante à une base de données SAP HANA. Si tel est le cas, utilisez la procédure de copie de la source de données. Pour en savoir plus, voir Copie de données d'une base de données système d'un CMS dans une autre [page 520].

Informations associées

Copie de données d'une base de données système d'un CMS dans une autre [page 520]
Sélection d'une base de données CMS (nouvelle ou existante) [page 515]

12.2 Sélection d'une base de données CMS (nouvelle ou existante)

Vous pouvez utiliser le CCM ou `cmsdbsetup.sh` pour spécifier une base de données système du CMS nouvelle ou existante pour un nœud. En principe, vous n'aurez à accomplir ces étapes que dans des situations assez précises :

- Si vous avez modifié le mot de passe de la base de données système actuelle du CMS, ces étapes vous permette de vous déconnecter de la base de données actuelle, puis de vous y reconnecter. Dès que vous y êtes invité, vous pouvez fournir le nouveau mot de passe au CMS.

- Si vous voulez sélectionner et initialiser une base de données vide pour la plateforme de BI, ces étapes vous permettent de sélectionner la nouvelle source de données.
- Si vous avez restauré une base de données système du CMS à partir d'une sauvegarde (à l'aide des outils et procédures d'administration de base de données standard) et que la connexion à la base de données d'origine n'est pas valide, vous devez reconnecter le CMS à la base de données restaurée. (Cela risque de se produire, par exemple, si vous avez restauré la base de données d'origine du CMS sur un serveur de base de données récemment installé.)

> **Remarque**
>
> Si vous utilisez IBM DB2 comme base de données du CMS et que vous le mettez à niveau à partir d'une version antérieure à 9.5 Fix Pack 5 vers la version 9.5 Fix Pack 5 ou plus récente (pour la gamme 9.5), ou si vous mettez à niveau à partir d'une version antérieure à 9.7 Fix Pack 1 vers la version 9.7 Fix Pack 1 ou plus récente (pour la gamme 9.7), au prochain redémarrage du nœud de la plateforme de BI ou du CMS, le schéma de base de données du CMS sera automatiquement mis à jour par le CMS pour qu'il prenne en charge un schéma compatible HADR.
>
> Il peut s'agir d'un processus assez long, pendant lequel le système de la plateforme de BI ne sera pas disponible pour utilisation. N'interrompez pas le processus de mise à jour pour éviter de corrompre la base de données du CMS. Il est vivement recommandé de sauvegarder la base de données du CMS avant d'effectuer cette opération. De plus, ne tentez pas d'utiliser IBM HADR avec une base de données du CMS IBM DB2 d'une version antérieur à 9.5 Fix Pack 5 (pour la gamme 9.5) ou 9.7 Fix Pack 1 (pour la gamme 9.7).

> **Remarque**
>
> Ne configurez pas une installation de la plateforme de BI de manière à ce qu'elle utilise une base de données système du CMS appartenant à un cluster différent, sauf si vous exécutez un workflow de copie du système.
>
> Une corruption du système peut se produire si les versions et niveaux de correctif des installations de la plateforme de BI et des bases de données du CMS sont différents, ou bien si les chemins d'installation ou les composants installés diffèrent, etc.
>
> Pour éviter la corruption, n'essayez pas de migrer le contenu BI d'un système à un autre en dirigeant le déploiement de la plateforme de BI vers une base de données du CMS d'un autre système de plateforme de BI, en particulier si sa version et son niveau de correctif sont différents.

> **Remarque**
>
> La plateforme de Business Intelligence prend en charge la communication SSL entre le CMS et les bases de données comme les bases de données d'audit et du CMS. Pour la communication SSL,
>
> - Vous devez utiliser SQL Anywhere, SQL Server et les bases de données SAP HANA comme une base de données du CMS ou d'audit pour communiquer en toute sécurité avec le CMS.
> - Vous devez activer le protocole SSL dans les serveurs de bases de données respectifs. Reportez-vous à la documentation correspondant à votre base de données.
> - Vous devez créer une connexion ODBC et transmettre le certificat du serveur de base de données via cette connexion ODBC.
> - Vous devez utiliser la même connexion ODBC pour vous connecter à la base de données du CMS et à la base de données d'audit.

12.2.1 Pour sélectionner une base de données de CMS nouvelle ou existante sous Windows

1. Utilisez le CCM pour arrêter le Serveur Intelligence Agent (SIA).
2. Sélectionnez le SIA et cliquez sur le bouton *Spécifier la source de données du CMS*.
3. Sélectionnez *Mettre à jour les paramètres de la source de données* et cliquez sur *OK*.
4. Sélectionnez un pilote de base de données, puis cliquez sur *OK*.
5. Ces étapes dépendent du type de connexion sélectionné :
   - Si vous avez sélectionné ODBC, la boîte de dialogue Windows « Sélectionner la source de données » s'ouvre. Sélectionnez la source de données ODBC que vous voulez utiliser comme base de données du CMS, puis cliquez sur *OK*. (Cliquez sur *Nouveau* pour configurer un nouveau DSN). Lorsque vous y êtes invité, précisez vos références de connexion à la base de données, puis cliquez sur *OK*.
   - Si vous avez sélectionné un pilote natif, un message vous demande le nom de votre serveur de base de données, votre ID de connexion et votre mot de passe. Saisissez ces informations, puis cliquez sur *OK*.
6. Spécifiez la clé de cluster.
7. Redémarrez le Server Intelligence Agent.

12.2.2 Pour sélectionner une base de données de CMS nouvelle ou existante sous UNIX

Utilisez le script `cmsdbsetup.sh`. Pour en savoir plus, voir la rubrique « Scripts Unix » dans le chapitre Administration de la ligne de commande du *Guide d'administration de la plateforme de BI*.

1. Exécutez le script `cmsdbsetup.sh` (situé par défaut à l'emplacement `<REPINSTALL>/sap_bobj/`).
2. Sélectionnez l'action de mise à jour (option 6).
3. Lorsque vous y êtes invité, fournissez le type de la nouvelle base de données du CMS.
4. Fournissez les informations de base de données (par exemple : nom de l'hôte, nom d'utilisateur, mot de passe et clé de cluster).
   Un message de notification s'affiche une fois que la base de données du CMS pointe vers le nouvel emplacement.
5. Si vous êtes invité à régénérer le SIA (Server Intelligence Agent), fournissez le mot de passe d'administrateur ainsi que le numéro de port sur lequel vous souhaitez que le CMS communique.

> **Remarque**
>
> Vous serez invité à fournir ces informations uniquement si vous indiquez une redirection vers une base de données CMS vide.

Informations associées

Scripts UNIX [page 1113]

12.3 Recréation de la base de données système du CMS

Cette procédure explique comment recréer (ou réinitialiser) la base de données système actuelle du CMS. En procédant ainsi, vous détruisez toutes les données qui se trouvent actuellement dans la base de données. Cette procédure s'avère très utile, par exemple, si vous avez installé la plateforme de BI dans un environnement de développement consacré à la conception et au test de vos propres applications Web personnalisées. Vous pouvez réinitialiser la base de données système du CMS dans l'environnement de développement à chaque fois que vous devez supprimer toutes les données du système.

> ⚠ Attention
>
> En suivant les étapes décrites dans ce workflow, vous supprimerez toutes les données de la base de données du CMS ainsi que les objets tels que les rapports et les utilisateurs. N'effectuez pas ces opérations sur un déploiement de production.

Il est très important d'effectuer une copie de sauvegarde de tous les paramètres de configuration du serveur avant de réinitialiser la base de données système du CMS. Lorsque vous recréerez la base de données, les paramètres de configuration du serveur seront effacés ; vous devez donc disposer d'une copie de sauvegarde afin de pouvoir restaurer ces informations.

Lorsque vous recréez la base de données, vos clés de licence actuelles doivent être conservées dans la base de données. Cependant, si vous devez à nouveau saisir des clés de licence, connectez-vous à la CMC avec le compte administrateur par défaut. Accédez à la zone de gestion Autorisation et saisissez les informations voulues dans l'onglet Clés de licence.

> ⓘ Remarque
>
> Si vous réinitialisez la base de données système du CMS, toutes les données qu'elle contient sont détruites. Pensez à sauvegarder votre base de données actuelle avant de commencer. Si nécessaire, contactez l'administrateur de votre base de données.

Informations associées

Sauvegarde des paramètres du serveur [page 572]

12.3.1 Pour recréer la base de données système du CMS sous Windows

1. Utilisez le CCM pour arrêter le Serveur Intelligence Agent (SIA).

   > ⓘ Remarque
   >
   > Pour cette procédure, vous ne pouvez pas exécuter le CCM sur un ordinateur distant. Il doit être exécuté sur un ordinateur comportant au moins un nœud valide. Les fichiers binaires du CMS doivent également être installés sur cet ordinateur.

2. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*.
3. Dans la boîte de dialogue *Propriétés*, accédez à l'onglet *Configuration* et cliquez sur *Spécifier*.
4. Dans la boîte de dialogue *Configuration de la base de données CMS*, cliquez sur *Recréer la source de données en cours*.

   > **Remarque**
   >
   > Les serveurs et objets de l'ordinateur sur lequel vous avez exécuté le CCM à l'étape 1 sont également recréés. Cependant, seuls les principaux objets par défaut sont recréés et non l'ensemble des objets. Par exemple, les modèles de rapports ne sont pas recréés.

5. Cliquez sur *OK* puis, lorsque le message de confirmation apparaît, cliquez sur *Oui*.
6. Indiquez le mot de passe de la base de données système du CMS, puis cliquez sur *OK*.

   > **Remarque**
   >
   > Assurez-vous que vous avez défini un nouveau mot de passe d'administrateur. Par défaut, le compte Administrateur ne comporte pas de mot de passe.

   Le CCM vous informe une fois la configuration de la base de données système CMS terminée.
7. Cliquez sur *OK*.

   Le CCM apparaît de nouveau.
8. Redémarrez le Server Intelligence Agent et activez les services.

   Lors du processus de démarrage, le Server Intelligence Agent démarre le CMS. Le CMS écrit les données système requises dans la source de données récemment vidée.
9. Si votre déploiement comprend plusieurs ordinateurs, vous devez recréer les nœuds sur les autres ordinateurs.

12.3.2 Pour recréer la base de données système du CMS sous UNIX

Utilisez le script `cmsdbsetup.sh`. Pour en savoir plus, voir la rubrique « Scripts Unix » dans le chapitre Administration de la ligne de commande du *Guide d'administration de la plateforme de BI*.

1. Exécutez `cmsdbsetup.sh` (à l'emplacement par défaut `<REPINSTALL>/sap_bobj/`).
2. Sélectionnez l'option "réinitialiser" (option 5), puis confirmez votre choix.
   Le script `cmsdbsetup.sh` commence à recréer la base de données système du CMS.
3. Fournissez le mot de passe de la base de données système du CMS.
4. Une fois la création de la base de données terminée, quittez le script `cmsdbsetup.sh`.
5. Fournissez les informations de base de données (par exemple : nom d'hôte, nom d'utilisateur et mot de passe).
   Un message de notification s'affiche une fois que la base de données du CMS pointe vers le nouvel emplacement.
6. Si vous êtes invité à régénérer le Server Intelligence Agent (SIA), fournissez le mot de passe d'administrateur ainsi que le numéro de port sur lequel vous souhaitez que le CMS communique.

> **Remarque**
>
> Vous serez invité à fournir ces informations uniquement si vous indiquez une redirection vers une base de données CMS vide.

7. Dans le répertoire `<REPINSTALL>/sap_bobj/`, utilisez la commande suivante pour démarrer le nœud.

```
ccm.sh -start <nomdunoeud>
```

8. Pour activer les services, utilisez la commande suivante :

```
ccm.sh -enable all -cms <NOMCMS:PORT> -username administrator -password <mot
de passe>
```

> **Remarque**
>
> Etant donné que vous venez de recréer la base de données du CMS, le mot de passe d'administrateur est vide.

Informations associées

Scripts UNIX [page 1113]

12.4 Copie de données d'une base de données système d'un CMS dans une autre

Vous pouvez utiliser le CCM (Central Configuration Manager) ou `cmsdbsetup.sh` pour copier les données système d'un serveur de base de données dans un autre. Par exemple, si vous souhaitez remplacer la base de données par une autre parce que vous effectuez la mise à niveau de la base de données ou passez d'un type de base de données à un autre, vous pouvez copier le contenu de la base de données existante dans la nouvelle base de données avant de la désactiver.

La base de données de destination est initialisée avant la copie des nouvelles données afin que le contenu qui s'y trouve soit définitivement détruit (toutes les tables de la plateforme de BI sont tout d'abord supprimées, puis recréées). Une fois les données copiées, la base de données de destination devient la base de données officielle et active du CMS.

> **Attention**
>
> N'essayez jamais d'utiliser une base de données du CMS depuis un autre cluster de la plateforme de BI. Avant de débuter ce workflow, assurez-vous que la base de données du CMS source a été utilisée avec ce cluster de la plateforme de BI, et non pas avec un autre.

> **Attention**
>
> N'essayez jamais d'effectuer une mise à niveau avec un workflow de copie de la base de données du CMS. Le workflow de copie de la base de données du CMS est conçu pour déplacer une base de données du CMS

d'un serveur de base de données vers un autre. Il n'est pas conçu pour mettre à niveau la base de données du CMS. Avant de démarrer ce workflow, assurez-vous que la base de données du CMS source a été utilisée avec ce cluster de la plateforme de BI, et que sa version et ses niveaux de correctifs sont identiques à ceux de l'installation de la plateforme de BI actuelle.

12.4.1 Préparation de la copie d'une base de données système du CMS

Avant de copier une base de données système du CMS, mettez les environnements source et de destination hors ligne en désactivant puis arrêtant successivement tous les serveurs. Sauvegardez les deux bases de données CMS et les répertoires racine utilisés par tous les Input et Output File Repository Servers. Si nécessaire, contactez votre administrateur de base de données ou réseau.

Assurez-vous de posséder un compte utilisateur de base de données ayant les droits pour lire toutes les données dans la base de données source et un compte utilisateur pour la base de données de destination possédant les droits Créer, Supprimer et Mettre à jour. Vérifiez également que vous pouvez vous connecter aux deux bases de données (par le biais de votre logiciel client de base de données ou d'ODBC, selon la configuration adoptée) à partir de la machine CMS dont vous voulez remplacer la base de données.

Si vous copiez une base de données CMS à partir de son emplacement d'origine vers un serveur de base de données différent, votre base de données CMS active est l'environnement source. Son contenu est copié vers la base de données de destination qui devient ensuite la base de données active du CMS courant : C'est également la procédure à suivre lorsque vous voulez déplacer la base de données du CMS de la base de données par défaut existante à un serveur de base de données dédié tel que Microsoft SQL Server, Informix, Oracle, DB2 ou Sybase. Connectez-vous avec un compte administratif à la machine exécutant le CMS dont vous souhaitez déplacer la base de données.

> **Remarque**
>
> Lorsque vous copiez les données d'une base de données vers une autre, la base de données de destination est initialisée avant la copie des nouvelles données. Cela signifie que, si votre base de données de destination ne contient pas les tables système de la plateforme de BI, ces tables sont créées. Si la base de données de destination contient les tables système de la plateforme de BI, celles-ci sont définitivement supprimées, de nouvelles tables système sont créées et les données de la base de données source sont copiées dans les nouvelles tables. Les autres tables de la base de données ne sont pas affectées.

> **Remarque**
>
> Si vous copiez une base de données système du CMS sur une base de données de destination MaxDB sous Windows, vous devez vous assurer que le chemin d'accès au client MaxDB a été ajouté à la variable d'environnement `<PATH>`. Par exemple, `;C:\Program Files\sdb\MAXDB1\pgm`.

12.4.2 Pour copier une base de données système du CMS sous Windows

Avant de copier le contenu de la base de données du CMS, vérifiez que vous pouvez vous connecter à la base de données de destination avec un compte disposant des autorisations nécessaires pour ajouter ou supprimer des tables et pour ajouter, supprimer ou modifier les données de ces tables.

1. Ouvrez le CCM (Central Configuration Manager) et arrêtez le SIA (Server Intelligence Agent).
2. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*.
3. Cliquez sur l'onglet *Configuration*, puis sur *Spécifier*.
4. Choisissez *Copier*, puis cliquez sur *OK*.
5. Sélectionnez le type de la base de données CMS source, puis indiquez les informations associées (notamment le nom de l'hôte, le nom d'utilisateur et le mot de passe).
6. Sélectionnez le type de la base de données CMS de destination, puis indiquez les informations associées (notamment le nom de l'hôte, le nom d'utilisateur et le mot de passe).
7. Lorsque la base de données CMS a terminé la copie, cliquez sur *OK*.

12.4.3 Copie de données d'une base de données système du CMS sous UNIX

Avant de copier le contenu de la base de données du CMS, vérifiez que vous pouvez vous connecter à la base de données de destination avec un compte disposant des autorisations nécessaires pour ajouter ou supprimer des tables et pour ajouter, supprimer ou modifier les données de ces tables.

> **Remarque**
>
> Sous UNIX, vous ne pouvez pas effectuer un transfert direct depuis un environnement source qui utilise une connexion ODBC vers la base de données CMS. Si votre base de données CMS source utilise ODBC, vous devez d'abord mettre à niveau ce système vers un pilote natif pris en charge.

1. Arrêtez le CMS en saisissant la commande suivante :

   ```
   ./ccm.sh -stop <nom de nœud>
   ```

2. Exécutez `cmsdbsetup.sh` (à l'emplacement par défaut `<REPINSTALL>/sap_bobj/`).
3. Sélectionnez l'option « copier » (option 4), puis confirmez votre choix.
4. Sélectionnez le type de la base de données CMS source, puis spécifiez ses informations de base de données (notamment le nom de l'hôte, le nom d'utilisateur et le mot de passe).
5. Sélectionnez le type de la base de données CMS de destination, puis spécifiez ses informations de base de données (notamment le nom de l'hôte, le nom d'utilisateur et le mot de passe).
   La base de données du CMS est copiée sur la base de données de destination. Une fois la copie terminée, un message s'affiche.

12.5 Pilote de base de données du CMS (Central Management Server)

Vous pouvez désormais accéder à la base de données du référentiel CMS de la plateforme de BI pour l'analyse du reporting en exploitant les fonctionnalités existantes de la plateforme (serveur de connexion, couche sémantique, clients du reporting). Le pilote d'accès aux données SAP BusinessObjects permet d'utiliser un univers pour interroger la base de données CMS. Pour en savoir plus, voir http://scn.sap.com/docs/DOC-74580.

13 Gestion des serveurs conteneurs d'applications Web (WACS)

13.1 WACS

13.1.1 Serveur conteneur d'applications Web (WACS)

Les serveurs conteneurs d'applications Web (WACS) fournissent une plateforme permettant d'héberger des applications Web de la plateforme SAP BusinessObject Business Intelligence. Par exemple, un serveur WACS peut héberger une CMC.

Les serveurs WACS simplifient l'administration du système grâce à la suppression de plusieurs workflows qui étaient auparavant requis pour la configuration des serveurs d'applications et le déploiement d'applications Web, ainsi qu'à une interface d'administration simplifiée et cohérente.

Les applications Web sont automatiquement déployées sur un serveur WACS. Le serveur WACS ne prend pas en charge le déploiement manuel ou WDeploy de la plateforme de BI, ni les applications Web externes.

13.1.1.1 Ai-je besoin d'un serveur WACS ?

Si vous ne souhaitez pas utiliser un serveur d'applications Java pour héberger vos applications Web SAP BusinessObjects, vous pouvez les héberger sur le serveur WACS.

Si vous prévoyez d'utiliser un serveur d'applications Java pris en charge pour déployer les applications Web de la plateforme de BI ou si vous installez la plateforme de BI sur un système UNIX, vous n'avez pas besoin d'installer ni d'utiliser de serveur WACS.

13.1.1.2 Quels sont les avantages de l'utilisation des serveurs WACS ?

L'utilisation d'un serveur WACS pour héberger la CMC vous offre un grand nombre d'avantages.

- Les serveurs WACS sont extrêmement simples à installer, maintenir et configurer.
- Toutes les applications hébergées sont prédéployées sur les serveurs WACS, si bien qu'aucune opération manuelle supplémentaire n'est requise.
- Le serveur WACS est pris en charge par SAP.
- Le serveur WACS ne requiert aucune compétence en administration et maintenance de serveurs d'applications Java.
- Le serveur WACS fournit une interface d'administration compatible avec d'autres serveurs de la plateforme de BI.

13.1.1.3 Tâches courantes

Tâche	Description	Sujet
Comment puis-je améliorer les performances des applications Web ou des services Web hébergés sur le serveur WACS ?	Vous pouvez améliorer les performances des applications Web ou des services Web en installant des serveurs WACS sur plusieurs ordinateurs.	• Ajout ou suppression de serveurs WACS à votre déploiement [page 527] • Clonage d'un serveur WACS [page 529]
Puis-je améliorer la disponibilité de mon Web Tier ?	Créez un serveur WACS supplémentaire dans votre déploiement de façon à ce qu'en cas de défaillance matérielle ou logicielle de l'un des serveurs, un autre serveur puisse continuer à répondre aux demandes.	Ajout ou suppression de serveurs WACS à votre déploiement [page 527]
Comment puis-je créer un environnement dans lequel je puisse facilement effectuer une restauration à partir d'une CMC incorrectement configurée ?	Créez un deuxième serveur WACS arrêté et utilisez-le pour définir un modèle de configuration. Ainsi, si le premier serveur WACS est incorrectement configuré, vous pouvez utiliser le deuxième serveur jusqu'à que vous ayez reconfiguré le premier serveur ou vous pouvez appliquer le modèle de configuration au premier serveur.	Ajout ou suppression de serveurs WACS à votre déploiement [page 527]
Comment puis-je améliorer la sécurité des communications entre les clients et les serveurs WACS ?	Configurez HTTPS sur les serveurs WACS.	• Configuration HTTPS/SSL [page 532] • Utilisation des serveurs WACS avec des pare-feu [page 558]
Comment puis-je améliorer la sécurité des communications entre les serveurs WACS et d'autres serveurs de la plateforme de BI de mon déploiement ?	Configurez la communication SSL entre les serveurs WACS et les autres serveurs de la plateforme de BI de votre déploiement.	• Configuration des serveurs principaux pour SSL [page 186] • Utilisation des serveurs WACS avec des pare-feu [page 558]
Puis-je utiliser un serveur WACS avec HTTPS et un serveur proxy inverse ?	Vous pouvez utiliser un serveur WACS avec HTTPS et un serveur proxy inverse si vous créez deux serveurs WACS, puis les configurez tous deux avec HTTPS. Utilisez le premier serveur WACS pour communiquer au sein de votre réseau interne et utilisez le deuxième pour communiquer avec un réseau externe via un serveur proxy inverse.	Pour configurer un serveur WACS de façon à ce qu'il prenne en charge le protocole HTTPS à l'aide d'un serveur proxy inverse [page 558]

Tâche	Description	Sujet
Comment les serveurs WACS s'intègrent-ils dans un environnement informatique ?	Les serveurs WACS peuvent être déployés dans un environnement informatique comportant des serveurs Web existant, des équilibreurs de charge matériels, des serveurs proxy inverses et des pare-feu.	• Utilisation d'un serveur WACS avec d'autres serveurs Web [page 557] • Utilisation des serveurs WACS avec un équilibreur de charge [page 557] • Utilisation d'un serveur WACS avec un serveur proxy inverse [page 557] • Utilisation des serveurs WACS avec des pare-feu [page 558]
Puis-je utiliser un serveur WACS dans un déploiement comportant un équilibreur de charge ?	Vous pouvez utiliser des serveurs WACS dans un déploiement qui utilise un équilibreur de charge matériel. Cependant, les serveurs WACS eux-mêmes ne peuvent pas être utilisés en tant qu'équilibreur de charge.	Utilisation des serveurs WACS avec un équilibreur de charge [page 557]
Puis-je utiliser un serveur WACS dans un déploiement comportant un serveur proxy inverse ?	Vous pouvez utiliser des serveurs WACS dans un déploiement qui utilise un serveur proxy inverse. Cependant, les serveurs WACS eux-mêmes ne peuvent pas être utilisés en tant que serveur proxy inverse.	Utilisation d'un serveur WACS avec un serveur proxy inverse [page 557]
Comment puis-je dépanner les serveurs WACS ?	En cas de faibles performances des serveurs WACS, vous pouvez en déterminer les raisons en visualisant les fichiers journaux et les métriques système.	• Pour configurer le suivi sur un serveur WACS [page 560] • Affichage des métriques de serveur [page 560]
Je n'obtiens aucune page à partir d'un port particulier. Quel est le problème ?	Vous pouvez avoir des difficultés à vous connecter à vous connecter au serveur WACS pour plusieurs raisons. Vérifiez les points suivants : • Les ports HTTP, HTTP via proxy et HTTPS que vous avez spécifiés pour le serveur WACS ne sont-ils pas utilisés par d'autres applications ? • La mémoire allouée au serveur WACS est-elle suffisante ? • Les serveurs WACS autorisent-ils suffisamment de demandes simultanées ? • Si nécessaire, restaurez les paramètres système par défaut des serveurs WACS.	• Pour résoudre les conflits de ports HTTP [page 561] • Pour modifier les paramètres de la mémoire [page 562] • Pour modifier le nombre de demandes simultanées [page 563] • Pour restaurer les valeurs par défaut du système [page 563]

Tâche	Description	Sujet
Comment puis-je configurer les propriétés des applications Web hébergées sur le serveur WACS ?	La procédure de configuration des propriétés pour les applications Web dépend de la propriété même et de l'application Web. Pour en savoir plus, voir la section « Configuration des propriétés d'applications Web » de ce chapitre.	Configuration des propriétés d'applications Web [page 559]
Où puis-je trouver la liste des propriétés de serveur WACS ?	La section « Annexe relative aux propriétés des serveurs » de ce guide contient la liste des propriétés WACS.	Propriétés des services principaux [page 1178]

13.1.2 Ajout ou suppression de serveurs WACS à votre déploiement

L'ajout de serveurs WACS à votre déploiement présente un certain nombre d'avantages :

- Restauration plus rapide à partir d'un serveur incorrectement configuré.
- Plus grande disponibilité du serveur.
- Amélioration de l'équilibrage de charge.
- Amélioration des performances globales.

Il existe trois moyens d'ajouter des serveurs WACS à votre déploiement :

- Installer un serveur WACS sur un ordinateur.
- Créer un serveur WACS.
- Clôner un serveur WACS.

> **Remarque**
>
> Nous vous recommandons de n'exécuter qu'un seul serveur WACS sur le même ordinateur à la fois en raison de l'utilisation importante des ressources que cette opération implique. Toutefois, vous pouvez déployer plusieurs serveurs WACS sur le même ordinateur mais n'exécuter qu'un seul d'entre eux. Il vous sera ainsi plus facile d'effectuer ne restauration si l'un de ces serveurs est incorrectement configuré.

13.1.2.1 Installation d'un serveur WACS

L'installation d'un serveur WACS sur un ordinateur distinct peut améliorer les performances et l'équilibrage de la charge de votre déploiement, ainsi que la disponibilité du serveur. Si votre déploiement contient au moins deux serveurs WACS sur des ordinateurs distincts, la disponibilité des applications Web et des services Web ne peut pas être affectée en cas de défaillances logicielles ou matérielles sur un ordinateur spécifique, dans la mesure où l'autre serveur WACS continue à fournir les services.

Vous pouvez installer un serveur WACS à l'aide du programme d'installation de la plateforme de BI. Il existe deux façons de procéder à cette installation :

- Dans une installation complète, dans l'écran *Sélectionner le serveur d'applications Web Java*, sélectionnez *Installer le serveur conteneur d'applications Web et déployer automatiquement les applications Web*. En revanche, si vous sélectionnez un serveur d'applications Java, aucun serveur WACS n'est installé.
- Dans une installation personnalisée/étendue, vous pouvez choisir d'installer un serveur WACS à partir de l'écran *Sélection des fonctions* en développant *Serveurs* > *Services de plateforme* et en sélectionnant *Serveur conteneur de l'application Web*.

Lorsque vous installez un serveur WACS, le programme d'installation crée automatiquement un serveur appelé `<NŒUD>.WebApplicationContainerServer`, `<NŒUD>` correspondant au nom de votre nœud. Les applications et les services Web de la plateforme de BI sont alors déployés sur ce serveur. Aucune étape manuelle n'est requise pour le déploiement ou la configuration de la CMC. Le système est prêt à être utilisé.

Lorsque vous installez un serveur WACS, le programme d'installation vous demande de fournir un numéro de port HTTP pour le serveur. Assurez-vous que le numéro de port spécifié n'est pas déjà utilisé. Le numéro de port par défaut est 6405. Si vous envisagez d'autoriser les utilisateurs qui se trouvent en dehors du pare-feu à se connecter au serveur WACS, vous devez veiller à ce que le numéro de port HTTP du serveur soit ouvert sur le pare-feu.

> **Remarque**
>
> Les applications Web hébergées par un serveur WACS se déploient automatiquement lorsque vous installez un serveur WACS ou que vous appliquez des mises à jour ou des hotfixes (correctifs) à un serveur WACS ou aux applications Web hébergées par un serveur WACS. Le déploiement des applications Web prend quelques minutes. Le serveur WACS reste à l'état « Initialisation en cours » jusqu'à ce que le déploiement des applications Web soit terminé. Les utilisateurs ne peuvent pas accéder aux applications Web hébergées sur un WACS avant le déploiement complet des applications Web. N'arrêtez pas le serveur tant que le déploiement initial n'est pas terminé. Vous pouvez afficher le statut du serveur WACS par le biais du Central Configuration Manager (CCM).
>
> Ce retard ne se produit qu'au premier démarrage du serveur WACS après son installation ou après l'application de mises à jour le concernant. Il ne se produit pas lors des redémarrages suivants du serveur WACS.
>
> Il est impossible de déployer manuellement des applications Web sur un serveur WACS. Vous ne pouvez pas utiliser WDeploy pour déployer des applications Web sur un serveur WACS.

13.1.2.2 Ajout d'un serveur WACS

> **Remarque**
>
> Nous vous recommandons de n'exécuter qu'un seul serveur WACS sur le même ordinateur à la fois en raison de l'utilisation importante des ressources que cette opération implique. Toutefois, vous pouvez déployer plusieurs serveurs WACS sur le même ordinateur mais n'exécuter qu'un seul d'entre eux. Il vous sera ainsi plus facile d'effectuer ne restauration si l'un de ces serveurs est incorrectement configuré.

1. Accédez à la zone de gestion *Serveurs* de la CMC.

2. Sélectionnez *Gérer* > *Nouveau* > *Nouveau serveur*.
   L'écran *Créer un serveur* s'affiche.
3. Dans la liste *Catégorie de service*, sélectionnez *Services principaux*.
4. Dans la liste *Sélectionner le service*, sélectionnez les services devant être hébergés par le WACS, puis cliquez sur *Suivant*.
   - Si vous souhaitez que le WACS héberge des applications Web telles que la CMC, la zone de lancement BI ou Open Document, sélectionnez le *Service de l'application Web BOE*.
   - Si vous souhaitez que le WACS héberge des services Web tels que Live Office ou Query as a Web Service (QaaWS), sélectionnez *SDK des services Web et service QaaWS*.
   - Si vous souhaitez que le WACS héberge des services Web BI du processus de gestion, sélectionnez *Service Web BI du processus de gestion*.
5. Dans l'écran *Créer un serveur* suivant, sélectionnez les services supplémentaires devant être hébergés par le WACS, puis cliquez sur *Suivant*.
6. Dans l'écran *Créer un serveur* suivant, sélectionnez le nœud auquel ajouter le serveur, saisissez le nom et la description du serveur, puis cliquez sur *Créer*.

   > **Remarque**
   >
   > Seuls les nœuds sur lesquels un serveur WACS a été installé figurent dans la liste *Noeud*.

7. Dans l'écran *Serveurs*, cliquez deux fois sur le nouveau serveur WACS.
   L'écran *Propriétés* s'affiche.
8. Si vous ne souhaitez pas que le WACS démarre automatiquement au redémarrage du système, dans le volet *Paramètres courants*, assurez-vous que la case *Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent* n'est pas cochée.
9. Cliquez sur *Enregistrer et fermer*.

Un nouveau serveur WACS est créé. Les paramètres et les propriétés par défaut sont appliqués au serveur.

13.1.2.3 Clonage d'un serveur WACS

Le clonage constitue une autre façon d'ajouter un nouveau serveur WACS. Il peut être réalisé sur le même ordinateur que celui sur lequel se trouve le serveur source ou sur un ordinateur différent. Contrairement à la méthode d'ajout qui consiste à créer un serveur WACS en lui attribuant les paramètres par défaut, le clonage applique les paramètres du serveur source au serveur cloné.

Les serveurs ne peuvent être clonés que sur des ordinateurs sur lesquels un serveur WACS est déjà installé.

> **Remarque**
>
> Nous vous recommandons de n'exécuter qu'un seul serveur WACS sur le même ordinateur à la fois en raison de l'utilisation importante des ressources que cette opération implique. Toutefois, vous pouvez déployer plusieurs serveurs WACS sur le même ordinateur mais n'exécuter qu'un seul d'entre eux. Il vous sera ainsi plus facile d'effectuer ne restauration si l'un de ces serveurs est incorrectement configuré.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Sélectionnez le serveur WACS à cloner, effectuez un clic droit, puis sélectionnez *Cloner un serveur*.

L'écran *Cloner un serveur* affiche la liste des nœuds de votre déploiement sur lesquels vous pouvez cloner le serveur. Seuls les nœuds sur lesquels un serveur WACS est déjà installé figurent dans la liste *Cloner sur le nœud*.

3. Dans l'écran *Cloner un serveur*, saisissez le nom du nouveau serveur, sélectionnez le nœud sur lequel effectuer le clonage, puis cliquez sur *OK*.

Un nouveau serveur WACS est créé. Le nouveau serveur contient les mêmes services que le serveur à partir duquel il a été cloné. Le nouveau serveur et les services qu'il héberge comportent les mêmes paramètres que le serveur à partir duquel il a été cloné, à l'exception du nom.

> **Remarque**
>
> Si vous clonez un serveur WACS sur le même ordinateur que celui sur lequel se trouve le serveur source, vous pouvez être confronté à des conflits de port avec le serveur à partir duquel vous avez effectué le clonage. Si cela se produit, vous devez changer les numéros de port sur l'instance de serveur que vous venez de cloner.

Informations associées

Pour résoudre les conflits de ports HTTP [page 561]

13.1.2.4 Suppression d'un serveur WACS de votre déploiement

Vous ne pouvez supprimer un serveur WACS qu'à condition de ne pas l'utilisez pas en tant que CMC à ce moment là. Si vous souhaitez supprimer un serveur WACS de votre déploiement, vous devez vous connectez à une CMC à partir d'un autre serveur WACS ou d'un serveur d'applications Java. Vous ne pouvez pas supprimer un serveur WACS actuellement utilisé en tant que CMC.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Arrêtez le serveur que vous voulez supprimer en cliquant sur celui-ci avec le bouton droit de la souris, puis en cliquant sur *Arrêter le serveur*.
3. Cliquez avec le bouton droit de la souris sur ce serveur, puis sélectionnez *Supprimer*.
4. Lorsque le système vous invite à confirmer votre choix, cliquez sur *OK*.

13.1.3 Ajout ou suppression de services aux serveurs WACS

13.1.3.1 Ajout d'une application Web ou d'un service Web à un serveur WACS

L'ajout d'applications Web ou de services Web de la plateforme de BI à un serveur WACS implique l'arrêt de celui-ci. Par conséquent, vous devez disposer d'au moins une autre CMC, hébergée sur un serveur WACS de

votre déploiement, qui fournisse un service de l'application Web BOE durant l'arrêt et l'ajout d'un service à l'autre serveur WACS.

Lorsque vous ajoutez un service au serveur WACS, il est automatiquement déployé sur le WACS au redémarrage du serveur.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS auquel vous voulez ajouter le service, puis visualisez les propriétés du serveur afin de vous assurer que le service que vous voulez ajouter n'est pas déjà présent.
3. Cliquez sur *Annuler* pour revenir à l'écran *Serveurs*.
4. Arrêtez le serveur en cliquant sur celui-ci avec le bouton droit de la souris, puis en cliquant sur *Arrêter le serveur*.

   Si vous essayez d'arrêter le serveur WACS qui fonctionne en tant que CMC à ce moment-là, un message d'avertissement s'affiche. Ne poursuivez pas la procédure d'arrêt si au moins un autre service de l'application Web BOE n'est pas en cours d'exécution sur un autre serveur WACS de votre déploiement. Dans ce cas, cliquez sur *OK*, connectez-vous à un autre serveur WACS, puis reprenez cette procédure à partir du début.
5. Cliquez avec le bouton droit de la souris sur le serveur, puis choisissez *Sélectionner des services*. L'écran *Sélectionner des services* s'affiche.
6. Sélectionnez le service que vous voulez ajouter au serveur, puis ajoutez-le en cliquant sur > et sur *OK*.
7. Démarrez le serveur WACS en cliquant sur celui-ci avec le bouton droit de la souris, puis en cliquant sur *Démarrer le serveur*.

Le service est ajouté au serveur WACS. Les paramètres et propriétés par défaut du service sont appliqués.

13.1.3.2 Suppression d'une application Web ou d'un service Web d'un serveur WACS

Pour supprimer une application Web ou un service Web d'un serveur WACS, vous devez vous connecter à la CMC d'un autre serveur WACS ou d'un serveur d'applications Java. Vous ne pouvez pas arrêter le serveur WACS qui vous fournit actuellement la CMC.

Vous ne pouvez pas supprimer le dernier service d'un serveur WACS. Par conséquent, si vous supprimez un service Web d'un serveur WACS, vous devez vous assurer que le serveur héberge au moins un autre service.

Pour supprimer le dernier service d'un serveur WACS, supprimer le serveur WACS lui-même.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS dont vous souhaitez supprimer le service Web, puis visualisez les propriétés du serveur afin de vous assurer que le service Web que vous voulez supprimer existe.
3. Cliquez sur *Annuler* pour revenir à l'écran *Serveurs*.
4. Arrêtez le serveur WACS en cliquant sur celui-ci avec le bouton droit de la souris, puis sur *Arrêter le serveur*.

   Si vous essayez d'arrêter le serveur WACS qui fonctionne en tant que CMC à ce moment-là, un message d'avertissement s'affiche. Ne poursuivez pas la procédure d'arrêt si au moins un autre service de l'application Web BOE n'est pas en cours d'exécution sur un autre serveur WACS de votre déploiement. Dans ce cas, cliquez sur *OK*, connectez-vous à un autre serveur WACS, puis reprenez cette procédure à partir du début.

5. Cliquez avec le bouton droit de la souris sur le serveur WACS, puis choisissez *Sélectionner des services*. L'écran *Sélectionner des services* s'affiche.
6. Sélectionnez le service à supprimer, cliquez sur <, puis sur *OK*.
7. Démarrez le serveur WACS en cliquant sur celui-ci avec le bouton droit de la souris, puis en cliquant sur *Démarrer le serveur*.

Le service est supprimé du serveur WACS.

13.1.4 Configuration HTTPS/SSL

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) et HTTP pour toutes les communications réseau établies entre clients et serveurs WACS au sein de votre déploiement de la plateforme de BI. Les certificats SSL/HTTPS cryptent le trafic réseau et permettent de bénéficier d'une sécurité renforcée.

Il existe deux types de certificats SSL :

- Les certificats SSL utilisés entre les serveurs de la plateforme de BI, y compris le serveur WACS et les autres serveurs de la plateforme de BI de votre déploiement. On les appelle SSL CORBA. Pour en savoir plus sur l'utilisation de SSL entre les serveurs de la plateforme de BI de votre déploiement, consultez la section « Description de la communication entre les composants de la plateforme de BI » du chapitre « Utilisation des pare-feu » du *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.
- Les certificats HTTP sur SSL, utilisés entre les serveurs WACS et les clients (par exemple, les navigateurs) qui communiquent avec ces serveurs.

> **Remarque**
>
> Si vous déployez des serveurs WACS dans un déploiement comportant un proxy ou un proxy inverse et si vous souhaitez utiliser SSL pour sécuriser la communication réseau dans votre déploiement, vous devez créer deux serveurs WACS. Pour en savoir plus, voir *Utilisation d'un serveur WACS avec un serveur proxy inverse*.

Pour configurer HTTPS/SSL sur un serveur WACS, vous devez suivre les étapes suivantes :

- Générez ou obtenez un fichier de stockage de certificats PKCS12 ou un fichier de stockage de clés JKS contenant vos certificats et vos clés privées. Pour générer un fichier PCKS12, vous pouvez utilisez les Services Internet (IIS) de Microsoft et la console MMC (Microsoft Management Console). Pour générer un fichier de stockage de clés, vous pouvez utiliser openssl ou l'outil de ligne de commande keytool de Java.
- Si vous souhaitez que seuls certains clients puissent se connecter à un serveur WACS, vous devez générer un fichier comportant une liste de certificats de confiance.
- Lorsque vous disposerez d'un fichier de stockage de certificats et, si nécessaire, d'une liste de certificats de confiance, copiez les fichiers sur l'ordinateur hébergeant le serveur WACS.
- Configurez le certificat HTTPS sur le serveur WACS.

Informations associées

Description de la communication entre les composants de la plateforme de BI [page 197]

Utilisation d'un serveur WACS avec un serveur proxy inverse [page 557]

13.1.4.1 Pour générer un fichier de stockage des certificats PKCS12

Il existe plusieurs façons de générer un fichier de stockage de certificats PKCS12 ou un fichier de stockage de clés Java et vous pouvez utiliser plusieurs outils. La méthode utilisée dépend des outils auxquels vous avez accès et de votre degré de maîtrise de ces outils.

L'exemple suivant montre comment générer un fichier PKCS12 à l'aide des services IIS (Internet Information Services) de Microsoft et de la MMC (Microsoft Management Console), pour Windows Server 2008.

1. Connectez-vous à l'ordinateur qui héberge le serveur WACS en tant qu'administrateur.
2. Dans IIS, demandez un certificat provenant de l'autorité de certification. Pour en savoir plus sur la façon de procéder, voir les documents d'aide d'IIS.
3. Démarrez la MMC en cliquant sur *Démarrer* > *Exécuter*, en tapant `mmc.exe`, puis en cliquant sur *OK*.
4. Ajoutez le composant logiciel enfichable Certificats à la MMC :
   a. Dans le menu *Fichier*, clique sur *Ajouter/Supprimer un composant logiciel enfichable*.
      L'écran *Ajouter ou supprimer des composants logiciels enfichables* apparaît.
   b. Dans la liste *Composants logiciels enfichables disponibles*, sélectionnez *Certificats*, puis cliquez sur *Ajouter*.
   c. Sélectionnez *Compte d'ordinateur*, puis cliquez sur *Suivant*.
   d. Sélectionnez *Ordinateur local*, puis cliquez sur *Terminer*.
   e. Cliquez sur *OK*.

   Le composant enfichable Certificats est ajouté à la console MMC.
5. Dans la console MMC, développez *Certificats*, puis sélectionnez le certificat à utiliser.
6. Dans le menu *Action*, sélectionnez *Toutes les tâches* > *Exporter*.
   L'*Assistant Exportation de certificat* démarre.
7. Cliquez sur *Suivant*.
8. Sélectionnez *Oui, exporter la clé privée* , puis cliquez sur *Suivant*.
9. Sélectionnez *Échange d'informations personnelles - PKCS #12 (.pfx)*, puis cliquez sur *Suivant*.
10. Saisissez le mot de passe utilisé lors de la création du certificat, puis cliquez sur *Suivant*. Vous devez spécifier ce mot de passe dans le champ *Mot de passe d'accès aux clés privées de la liste de certificats de confiance* lorsque vous configurez HTTPS pour les serveurs WACS.

Un fichier de stockage des certificats PKCS12 est créé.

13.1.4.2 Pour générer une liste de certificats de confiance

1. Connectez-vous à l'ordinateur qui héberge le serveur WACS en tant qu'administrateur.
2. Démarrez la console MMC (Microsoft Management Console).
3. Ajoutez le composant enfichable des Services Internet (IIS) :

a. Dans le menu *Fichier*, sélectionnez *Ajouter/Supprimer un composant logiciel enfichable*.
b. Dans la liste *Composants logiciels enfichables disponibles*, sélectionnez *Gestionnaire des services Internet (IIS)*, puis cliquez sur *Ajouter*.
c. Cliquez sur *OK*.
Le composant enfichable IIS est ajouté à la console MMC.

4. Suivez les étapes décrites ici pour créer une liste de certificats de confiance :http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard

13.1.4.3 Pour configurer HTTPS/SSL

Avant de configurer HTTPS/SSL sur votre serveur WACS, assurez-vous que vous avez déjà créé un fichier PCKS12 ou un fichier de stockage de clés JKS et que vous avez copié ou déplacé le fichier sur l'ordinateur hébergeant déjà le serveur WACS.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS pour lequel vous souhaitez activer HTTPS.
L'écran *Propriétés* s'affiche.
3. Dans la section *Configuration HTTPS*, activez la case à cocher *Activer HTTPS*.
4. Dans le champ *Lier au nom d'hôte ou à l'adresse IP*, spécifiez l'adresse IP pour laquelle les certificats ont été émis et à laquelle le serveur WACS sera lié.
Les services HTTPS seront fournis via l'adresse IP spécifiée.
5. Dans le champ *Port HTTPS*, spécifiez le numéro de port permettant au serveur WACS de fournir un service HTTPS. Vous devez vous assurer que ce port est disponible. Si vous envisagez d'autoriser les utilisateurs qui se trouvent en dehors du pare-feu à se connecter au serveur WACS, vous devez également vous assurer que ce port est ouvert sur le pare-feu.
6. Si vous configurez SSL avec un serveur proxy inverse, indiquez le nom d'hôte et le port du serveur proxy dans les champs *Nom d'hôte du proxy* et *Port du proxy*.
7. Dans la liste *Protocole*, sélectionnez un protocole. Les options disponibles sont les suivantes :
   - *SSL*
   SSL (Secure Sockets Layer) est un protocole permettant de crypter le trafic réseau.
   - *TLS*
   TLS (Transport Layer Security) est un protocole plus récent auquel des améliorations ont été apportées. Les différences entre ces deux protocoles (SSL et TLS) sont mineures mais les algorithmes de cryptage du protocole TLS sont plus élaborés.
8. Dans le champ *Type de stockage des certificats*, spécifiez le type de fichier du certificat. Les options disponibles sont les suivantes :
   - *PKCS12*
   Sélectionnez PKCS12 si vous utilisez généralement des outils Microsoft.
   - *JKS*
   Sélectionnez JKS si vous utilisez généralement des outils Java.
9. Dans le champ *Emplacement du fichier de stockage des certificats*, spécifiez le chemin d'accès à l'emplacement où vous avez copié ou déplacé le fichier de stockage des certificats ou le fichier de stockage des clés Java.
10. Dans le champ *Mots de passe d'accès aux clés privées*, indiquez le mot de passe.

Les fichiers de stockage des certificats PKCS12 et les fichiers de stockage des clés JKS contiennent des clés privés protégées par mot de passe afin d'empêcher tout accès non autorisé. Vous devez spécifier le mot de passe permettant d'accéder aux clés privés afin que les serveurs WACS puissent accéder à ces clés privées.

11. Nous vous recommandons d'utiliser un fichier de stockage de certificats ou un fichier de stockage de clés contenant un seul certificat, ou dans lequel le certificat que vous souhaitez utiliser figure en tête de liste. Toutefois, si vous utilisez un fichier de stockage de certificats ou un fichier de stockage des clés contenant plusieurs certificats et si le certificat à utiliser ne figure pas en tête de liste, vous devez indiquer son alias dans le champ *Alias du certificat*.
12. Si vous souhaitez que le serveur WACS accepte uniquement les demandes HTTPS émanant de certains clients, activez l'authentification client.

    L'authentification du client n'authentifie pas les utilisateurs. Il permet de s'assurer que le serveur WACS répond aux demandes HTTPS de certains clients seulement.

    a. Activez la case à cocher *Activer l'authentification client*.
    b. Dans le champ *Emplacement du fichier de la liste de certificats de confiance*, spécifiez l'emplacement du fichier PCKS12 ou du fichier de stockage des clés JKS contenant le fichier de la liste des certificats.

    > **Remarque**
    >
    > Le type de la liste des certificats de confiance doit être identique au type du fichier de stockage des certificats.

    > **Remarque**
    >
    > Pour plus d'informations sur l'établissement d'une authentification sécurisée à l'aide de certificats X.509, voir Services Web RESTful [page 418].

    > **Remarque**
    >
    > Vous pouvez importer le certificat d'un système ABAP dans la plateforme BI en exécutant la commande : `keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` . Reportez-vous au tableau ci-dessous pour comprendre la commande :
    >
    > | Commande | Description |
    > | --- | --- |
    > | -alias | Nom de l'alias |
    > | -file | Chemin d'accès au fichier du certificat du système ABAP |
    > | -keystore | Chemin d'accès au fichier de de stockage des clés approuvé |

    c. Dans le champ *Mot de passe d'accès aux clés privées de la liste de certificats de confiance*, saisissez le mot de passe qui protège l'accès aux clés privés dans le fichier de la liste de certificats de confiance.

> **Remarque**
>
> Lorsque vous activez l'authentification client et qu'un navigateur ou un consommateur de service Web n'est pas authentifié, la connexion HTTPS échoue.

13. Cliquez sur *Enregistrer et fermer*.
14. Accédez à l'écran *Métriques*, puis assurez-vous que le connecteur HTTPS figure sous *Liste des connecteurs WACS en cours d'exécution*. S'il n'y figure pas, assurez-vous que le connecteur HTTPS est correctement configuré.

13.1.5 Méthodes d'authentification prises en charge

Les serveurs WACS prennent en charge les méthodes d'authentification suivantes :

- Enterprise
- LDAP
- AD Kerberos

Les serveurs WACS ne prennent pas en charge les méthodes d'authentification suivantes :

- NT
- AD NTLM
- LDAP avec connexion unique

13.1.6 Configuration d'AD Kerberos pour un serveur WACS

Pour configurer l'authentification AD Kerberos pour un serveur WACS, vous devez d'abord configurer votre ordinateur pour la prise en charge d'AD. Vous devez effectuer les opérations suivantes :

- Activation du plug-in de sécurité Windows AD.
- Mappage d'utilisateurs et de groupes.
- Configuration d'un compte de service.
- Configuration d'une restriction de délégation.
- Activation de l'authentification Kerberos dans le plug-in Windows AD pour le serveur WACS.
- Création des fichiers de configuration.

Après avoir configuré l'ordinateur d'hébergement du serveur WACS pour l'utilisation de l'authentification AD Kerberos, vous devez procéder à une configuration supplémentaire par le biais de la CMC.

Si vous configurez une connexion unique par le bais d'AD Kerberos pour le SDK Services Web et QaaWS, vous devez aussi configurer le serveur WACS et l'ordinateur qui l'héberge.

Informations associées

Plug-in de sécurité Windows AD [page 303]
Pour mapper des utilisateurs et groupes Windows AD [page 304]
Configuration d'un compte de service pour l'authentification AD avec Kerberos [page 302]
Exécution du SIA sous le compte de service de la plateforme de BI [page 311]
Activation de l'authentification Kerberos dans le plug-in Windows AD pour le serveur WACS [page 537]
Création des fichiers de configuration [page 538]
Configuration d'un serveur WACS pour l'AD Kerberos [page 541]
Configuration de la connexion unique Kerberos AD [page 544]

13.1.6.1 Activation de l'authentification Kerberos dans le plug-in Windows AD pour le serveur WACS

Pour que Kerberos soit pris en charge, vous devez configurer le plug-in de sécurité Windows AD dans la CMC de manière à ce qu'il utilise l'authentification Kerberos. Cette opération inclut les étapes suivantes :

- S'assurer que l'authentification Windows AD est activée.
- Saisir le compte d'administration AD.

  > ⓘ Remarque
  >
  > Ce compte requiert uniquement le droit de lecture sur Active Directory (aucun autre droit n'est nécessaire).

- Activation de l'authentification Kerberos et de la connexion unique lorsque la connexion unique est souhaitée
- Saisir le nom principal de service du compte de service.

13.1.6.1.1 Prérequis

Avant de configurer le plug-in de sécurité Windows AD pour Kerberos, vous devez avoir terminé les tâches suivantes :

- Configuration d'un compte de service pour l'authentification AD avec Kerberos [page 302]
- Exécution du SIA sous le compte de service de la plateforme de BI [page 311]
- Pour mapper des utilisateurs et groupes Windows AD [page 304]

13.1.6.1.2 Pour configurer le plug-in de sécurité Windows AD pour Kerberos

1. Accédez à la zone de gestion *Authentification* de la CMC.
2. Cliquez deux fois sur *Windows AD*.
3. Vérifiez que la case *Activer Windows Active Directory (AD)* est cochée.
4. Sous *Options d'authentification*, sélectionnez *Utiliser l'authentification Kerberos*.
5. Si vous souhaitez configurer la connexion unique à une base de données, cochez la case *Contexte de sécurité de la mémoire cache* (obligatoire pour une connexion unique à la base de données).
6. Dans le champ *Nom principal du service*, saisissez le compte et le domaine du compte de service ou le mappage SPN au compte de service.

   Utilisez le format suivant, où `<cptsvc>` correspond au nom de votre compte de service ou SPN créé précédemment et `<DNS.COM>` au domaine complet (en majuscules). Par exemple, le compte de service peut être cptsvc@DNS.COM et le SPN BOBJCentralMS/nom_quelconque@DOMAINE.COM

   > ⓘ Remarque
   >
   > - Si vous envisagez d'autoriser les utilisateurs d'autres domaines que le domaine par défaut à se connecter, vous devez fournir le nom SPN que vous avez précédemment mappé.
   > - Le compte de service respecte la casse. La casse du compte saisi ici doit correspondre à celle que vous avez définie dans votre domaine Active Directory.
   > - Il doit s'agir du même compte que celui utilisé pour exécuter les serveurs de la plateforme de BI ou du SPN mappant à ce compte.

7. Pour configurer une connexion unique, sélectionnez *Activer la connexion unique pour le mode d'authentification sélectionné*.

   > ⓘ Remarque
   >
   > Si vous avez choisi d'activer la connexion unique, vous devez configurer le serveur WACS.

Informations associées

Configuration de la connexion unique Kerberos AD [page 544]

13.1.6.2 Création des fichiers de configuration

La procédure générale de configuration de Kerberos sur votre serveur d'applications comprend les opérations suivantes :

- Création du fichier de configuration Kerberos.
- Création du fichier de configuration de connexion JAAS.

> **Remarque**
>
> - Le domaine Active Directory par défaut doit être au format DNS et en majuscules.
> - Vous n'avez pas besoin de télécharger ni d'installer MIT Kerberos pour Windows. Le fichier keytab n'est plus requis pour votre compte de service.

13.1.6.2.1 Pour créer le fichier de configuration Kerberos

Procédez comme suit pour créer le fichier de configuration Kerberos.

1. Créez le fichier `krb5.ini` si nécessaire et stockez-le sous `C:\Windows` pour Windows.

   > **Remarque**
   >
   > Vous pouvez stocker ce fichier à un emplacement différent. Toutefois, dans ce cas, vous devez spécifier l'emplacement dans le champ *Emplacement du fichier Krb5.ini* sur la page *Propriétés* du serveur WACS, dans la CMC.

2. Ajoutez les informations requises suivantes dans le fichier de configuration Kerberos :

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

   > **Remarque**
   >
   > `DNS.COM` est le nom DNS du domaine. Vous devez le saisir en majuscules au format FQDN.

   > **Remarque**
   >
   > `kdc` est le nom d'hôte du contrôleur de domaine.

> **Remarque**
>
> Vous pouvez ajouter plusieurs entrées de domaine à la section [realms] si les utilisateurs se connectent à partir de plusieurs domaines. Pour consulter un exemple de fichier avec plusieurs entrées de domaine, voir Exemples de fichiers Krb5.ini [page 540].

> **Remarque**
>
> Dans une configuration comportant plusieurs domaines, sous `[libdefaults]`, la valeur `default_realm` peut être n'importe lequel des domaines souhaités. La meilleure solution consiste à utiliser le domaine comportant le plus grand nombre d'utilisateurs qui seront authentifiés à l'aide de leurs comptes AD.

13.1.6.2.2 Pour créer le fichier de configuration de connexion JAAS

1. Créez un fichier nommé `bscLogin.conf` si nécessaire, puis stockez-le à l'emplacement par défaut : `C:\Windows`.

   > **Remarque**
   >
   > Vous pouvez stocker ce fichier à un emplacement différent. Toutefois, dans ce cas, vous devez spécifier l'emplacement dans le champ *Emplacement du fichier bscLogin.conf* sur la page *Propriétés* du serveur WACS, dans la CMC.

2. Ajoutez le code suivant au fichier de configuration JAAS `bscLogin.conf` :

   ```
   com.businessobjects.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required;
   };
   ```

3. Enregistrez le fichier et fermez-le.

13.1.6.2.3 Exemples de fichiers Krb5.ini

Exemple de fichier Krb5.ini avec plusieurs domaines

Voici un exemple de fichier avec plusieurs domaines :

```
[domain_realm]
        .domain03.com = DOMAIN03.COM
        domain03.com = DOMAIN03.com
        .child1.domain03.com = CHILD1.DOMAIN03.COM
        child1.domain03.com = CHILD1.DOMAIN03.com
        .child2.domain03.com = CHILD2.DOMAIN03.COM
        child2.domain03.com = CHILD2.DOMAIN03.com
        .domain04.com = DOMAIN04.COM
        domain04.com = DOMAIN04.com
[libdefaults]
```

```
        default_realm = DOMAIN03.COM
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        DOMAIN03.COM = {
         admin_server = testvmw2k07
         kdc = testvmw2k07
         default_domain = domain03.com
        }
     CHILD1.DOMAIN03.COM = {
            admin_server = testvmw2k08
            kdc = testvmw2k08
            default_domain = child1.domain03.com
        }
        CHILD2.DOMAIN03.COM = {
            admin_server = testvmw2k09
            kdc = testvmw2k09
            default_domain = child2.domain03.com
        }
        DOMAIN04.COM = {
            admin_server = testvmw2k011
            kdc = testvmw2k011
            default_domain = domain04.com
        }
```

Exemple de fichier Krb5.ini avec un seul domaine

Voici un exemple de fichier krb5.ini avec un seul domaine.

```
[libdefaults]
        default_realm = ABCD.MFROOT.ORG
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        ABCD.MFROOT.ORG = {
            kdc = ABCDIR20.ABCD.MFROOT.ORG
            kdc = ABCDIR21.ABCD.MFROOT.ORG
            kdc = ABCDIR22.ABCD.MFROOT.ORG
            kdc = ABCDIR23.ABCD.MFROOT.ORG
            default_domain = ABCD.MFROOT.ORG
        }
```

13.1.6.3 Configuration d'un serveur WACS pour l'AD Kerberos

Une fois que vous avez configuré l'ordinateur d'hébergement du serveur WACS pour l'authentification AD Kerberos, vous devez configurer le serveur WACS lui-même, par le biais de la CMC.

13.1.6.3.1 Pour configurer un serveur WACS pour l'AD Kerberos

1. Accédez à la zone de gestion *Serveurs* de la CMC.

2. Cliquez deux fois sur le serveur WACS pour lequel vous souhaitez configurer l'AD.
   L'écran *Propriétés* s'affiche.
3. Dans le champ *Emplacement du fichier Krb5.ini*, spécifiez le chemin d'accès au fichier de configuration `krb5.ini`.
4. Dans le champ *Emplacement du fichier bscLogin.conf*, spécifiez le chemin d'accès au fichier de configuration `bscLogin.conf`.
5. Cliquez sur *Enregistrer et fermer*.
6. Redémarrez le serveur WACS.

13.1.6.4 Dépannage de Kerberos

Ces deux procédures peuvent vous aider si vous rencontrez des difficultés lors de la configuration de Kerberos :

- Activation de la journalisation
- Test de la configuration Kerberos

13.1.6.4.1 Pour activer la journalisation Kerberos

1. Démarrez le CCM (Central Configuration Manager), puis cliquez sur *Gérer les serveurs*.
2. Indiquez les références de connexion.
3. Dans l'écran *Gérer les serveurs*, arrêtez le serveur WACS.
4. Cliquez sur *Configuration du niveau Web*.

   > **Remarque**
   >
   > L'icône *Configuration du niveau Web* n'est activée que lorsque vous sélectionnez un serveur WACS arrêté.

   L'écran *Configuration du niveau Web* s'affiche.
5. Sous *Paramètres de ligne de commande*, copiez le texte suivant à la fin des paramètres :

   ```
   « -Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.Kerberos.debug=true »
   ```
6. Cliquez sur *OK*.
7. Dans l'écran *Gérer les serveurs*, démarrez le serveur WACS.

13.1.6.4.2 Pour tester la configuration Kerberos

Exécutez la commande suivante pour tester la configuration Kerberos, `cptserv` correspondant au compte de service et au domaine sous lesquels s'exécute le CMS et `Password` au mot de passe associé au compte de service.

```
<INSTALLDIR>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Par exemple :

```
 C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM
Password
```

Si le problème persiste, vérifiez que la casse du domaine et du nom de service principal correspond exactement à celle définie dans Active Directory.

13.1.6.4.3 Utilisateur AD mappé dans l'impossibilité de se connecter à la plateforme de BI sur le serveur WACS

Les deux problèmes suivants peuvent survenir même si les utilisateurs sont mappés à la plateforme de BI :

13.1.6.4.3.1 Echec de la connexion dû à des noms UPN et SAM différents dans AD

L'ID Active Directory d'un utilisateur a été correctement mappé à la plateforme de BI. Malgré cela, l'utilisateur ne peut pas se connecter à la CMC ou à InfoView avec l'authentification AD et Kerberos au format suivant : `DOMAIN\ABC123`

Ce problème peut se produire lorsque l'utilisateur est configuré dans Active Directory avec un nom UPN et un nom SAM qui ne sont pas identiques, que ce soit au niveau de la casse ou autre. Voici deux exemples qui peuvent causer un problème :

- Le nom UPN est abc123@company.com mais le nom SAM est DOMAIN\ABC123.
- Le nom UPN est jsmith@company mais le nom SAM est DOMAIN\johnsmith.

Il y a deux façons de traiter ce problème :

- Demandez aux utilisateurs de se connecter à l'aide de leurs noms UPN plutôt que de leurs noms SAM.
- Vérifiez que le nom de compte SAM et le nom UPN sont identiques.

13.1.6.4.3.2 Erreur de pré-authentification

Un utilisateur qui a pu se connecter au préalable ne parvient plus à le faire. Il obtient le message d'erreur suivant : Informations de compte non reconnues. Les journaux WACS font état de l'erreur suivante : `"Pre-authentication information was invalid (24)"` (Informations de pré-authentification non valides).

Ceci peut se produire lorsque la base de données d'utilisateurs Kerberos n'a pas été mise à jour après un changement d'UPN dans AD. Ceci peut également indiquer que la base de données d'utilisateurs Kerberos et les informations AD ne sont pas synchronisées.

Pour résoudre ce problème, réinitialisez le mot de passe de l'utilisateur dans AD. Ainsi, les modifications seront correctement diffusées.

13.1.7 Configuration de la connexion unique Kerberos AD

Si vous configurez la connexion unique Kerberos AD pour la zone de lancement BI ou le SDK des services Web et QaaWS, vous devez aussi vérifier que vous avez configuré le serveur WACS et l'ordinateur qui l'héberge pour l'authentification Kerberos AD.

Pour configurer le WACS pour une connexion unique Kerberos AD, vous devez d'abord configurer l'ordinateur qui héberge le WACS, puis le serveur WACS lui-même.

> **Remarque**
>
> Si vous prévoyez d'utiliser la connexion unique dans un environnement avec proxy inverse, lisez les informations de sécurité de ce guide.

Informations associées

Présentation de la sécurité [page 157]
Configuration d'AD Kerberos pour un serveur WACS [page 536]
Configuration de l'ordinateur pour la connexion unique Kerberos AD [page 544]
Configuration du serveur WACS pour la connexion unique Kerberos AD [page 545]

13.1.7.1 Configuration de l'ordinateur pour la connexion unique Kerberos AD

Pour configurer une connexion unique Kerberos AD à SDK Services Web et QaaWS, vous devez d'abord configurer le serveur WACS et l'ordinateur qui l'héberge :

- Configuration d'une restriction de délégation pour la connexion unique Vintela [page 327]
- Configuration du compte de service pour la connexion unique Vintela [page 324]

- Configuration de plusieurs SPN [page 545]
- Pour augmenter la limite de taille d'en-tête de votre WACS [page 545]

Les sections suivantes expliquent comment réaliser chacune de ces étapes.

13.1.7.1.1 Configuration de plusieurs SPN

L'utilisation de plusieurs SPN n'est pas prise en charge.

13.1.7.1.2 Pour augmenter la limite de taille d'en-tête de votre WACS

Active Directory crée un jeton Kerberos utilisé lors de la procédure d'authentification. Ce jeton est stocké dans l'en-tête HTTP. Votre WACS disposera d'une taille d'en-tête HTTP par défaut qui sera suffisante pour la plupart des utilisateurs. La taille d'en-tête peut être configurée.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le WACS dont vous souhaitez changer la taille d'en-tête HTTP.
   L'écran *Propriétés* s'affiche.
3. Sous la section *Configuration HTTP*, *Configuration du port HTTP via un proxy* ou *Configuration HTTPS*, spécifiez une valeur dans le champ *Taille maximale de l'en-tête HTTP (octets)*.
4. Cliquez sur *Enregistrer et fermer*.
5. Redémarrez le serveur.

13.1.7.2 Configuration du serveur WACS pour la connexion unique Kerberos AD

Vous pouvez configurer un serveur WACS (Web Application Container Server) pour utiliser une connexion unique Kerberos AD. La connexion unique Kerberos AD est prise en charge. NTLM AD n'est pas pris en charge.

Avant de configurer le WACS, vous devez configurer la connexion unique Kerberos AD pour l'ordinateur qui héberge le WACS.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS que vous souhaitez configurer.
   L'écran *Propriétés* s'affiche.
3. Cochez *Activer la connexion unique Kerberos Active Directory*.
4. Spécifier les valeurs des propriétés Domaine AD par défaut, Nom principal du service et Fichier Keytab, puis cliquez sur *Enregistrer et fermer*.
5. Redémarrez le serveur WACS.

La connexion unique Active Directory est prête à être utilisée.

13.1.7.3 Configuration de Kerberos et de la connexion unique aux bases de données

La connexion unique à la base de données est prise en charge pour les déploiements répondant à toutes les exigences suivantes :

- Le déploiement de la plateforme de BI se situe sur le serveur WACS.
- Le serveur WACS a été configuré avec AD et Kerberos.
- La base de données pour laquelle une connexion unique est requise est une version prise en charge de SQL Server ou Oracle.
- Les groupes ou utilisateurs devant accéder à la base de données doivent disposer de droits d'accès à SQL Server ou Oracle.
- La case à cocher Contexte de sécurité de la mémoire cache (obligatoire pour une connexion unique à la base de données) est activée dans la page Authentification AD de la CMC.

L'étape finale consiste à modifier le fichier `krb5.ini` afin de prendre en charge la connexion unique à la base de données.

> **Remarque**
>
> Les instructions suivantes expliquent comment configurer une connexion unique à la base de données. Si vous souhaitez configurer une connexion unique de bout en bout à la base de données, vous devez appliquer la configuration requise par la connexion unique Vintela. Pour en savoir plus, voir Configuration de la connexion unique Kerberos AD [page 544].

13.1.7.3.1 Activation de la connexion unique aux bases de données

1. Ouvrez le fichier `krb5.ini` utilisé pour le déploiement de la plateforme de BI.

   L'emplacement par défaut de ce fichier est le répertoire C:\Windows du serveur d'applications Web.
2. Accédez à la section `[libdefaults]` du fichier.
3. Entrez la chaîne suivante avant le début de la section `[realms]` du fichier :

   ```
   forwardable = true
   ```
4. Enregistrez le fichier et fermez-le.
5. Redémarrez le serveur WACS.

13.1.8 Configuration des services Web RESTful

Le SDK des services Web RESTful de la plateforme de Business Intelligence permet d'accéder à la plateforme de BI à l'aide du protocole HTTP. Cela permet aux utilisateurs de naviguer vers le référentiel de la plateforme de BI et de planifier des objets à l'aide d'un langage de programmation prenant en charge les requêtes HTTP. Les services Web RESTful sont installés dans le cadre d'un WACS.

Cette section explique comment administrer des services Web RESTful. Pour en savoir plus sur les services Web RESTful, voir le *Guide du développeur des services Web RESTful de la plateforme de Business Intelligence*.

13.1.8.1 Applications

13.1.8.1.1 Pour configurer l'URL de base pour les services Web de type RESTful

Si le déploiement de la plateforme de BI utilise un serveur proxy ou contient plusieurs instances du serveur conteneur d'applications Web (WACS), vous devrez peut-être configurer l'URL de base à utiliser avec les services Web de type RESTful. Avant de configurer l'URL de base, vous devez connaître le nom du serveur et le numéro de port qui écoute les requêtes de services Web de type RESTful.

L'URL de base est utilisée dans le cadre de chaque requête de service Web de type RESTful. Les développeurs trouvent l'URL de base par programme et l'utilisent pour rediriger les requêtes de services Web de type RESTful vers le serveur et le port adéquats. L'URL de base est également utilisée dans les réponses de services Web de type RESTful pour définir des hyperliens vers d'autres ressources RESTful.

> **Remarque**
>
> Dans les installations par défaut de la plateforme de BI, l'URL de base est définie de la façon suivante : `http://<servername>:6405/biprws`. Remplacez `<servername>` par le nom du serveur qui héberge les services Web de type RESTful.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Dans la CMC, cliquez sur *Applications*.
   Une liste d'applications apparaît.
3. Cliquez avec le bouton droit sur *Service Web de type RESTFul* > *Propriétés*.
   La boîte de dialogue *Propriétés* : *service Web RESTful* s'affiche. La case à cocher *Utiliser un chemin d'accès relatif* est maintenant disponible afin de prendre en compte l'URL de votre navigateur pour lancer le service Web RESTful. Pour en savoir plus, consultez la note SAP 3048101.
4. Dans la zone de texte *URL d'accès*, saisissez le nom de l'URL de base pour les services Web de type RESTful.
   Saisissez par exemple `http://<servername>:<portnumber>/biprws`. Remplacez `<servername>` et `<portnumber>` par le nom du serveur et le port qui écoute les requêtes de services Web de type RESTful.

   > **Attention**
   >
   > - **Les serveurs Tomcat, WACS, JBoss, SAP NetWeaveret et WebSphere sont pris en charge** pour les API des services Web RESTful.
   > - L'*URL d'accès* affiche l'URL WACS **par défaut**. Pour utiliser les API des services Web RESTful dans le serveur Web Tomcat, veillez à modifier les valeurs requises `<server>` et `<port>` en conséquence.

5. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Si nous activons *Utiliser un chemin d'accès relatif*, le système utilise l'URL relative du navigateur.

13.1.8.2 Propriétés des serveurs WACS

13.1.8.2.1 Configuration des paramètres de la ligne de commande Méthodes et en-têtes

En tant qu'administrateur, vous pouvez restreindre les méthodes et en-têtes pouvant être utilisés par les services Web RESTful an ajoutant les options appropriées aux *Paramètres de ligne de commande* dans les propriétés de votre serveur conteneur d'applications Web (WACS). Un redémarrage du service WACS est nécessaire après modification des paramètres.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Paramètres de ligne de commande*, saisissez les méthodes et en-têtes à autoriser.

   Chaque groupe d'options est encadré par des guillemets. Utilisez d'autres méthodes que `GET`, `HEAD` et `POST`. Utilisez des virgules pour séparer les valeurs d'option telles que `PUT` et `DELETE`, comme l'illustre l'exemple suivant.

   ```
   "-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
   "-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
   Authenticate"
   ```

   > **Remarque**
   >
   > La valeur par défaut utilisée pour autoriser toutes les méthodes et tous les en-têtes est * (astérisque). L'omission de tous les paramètres de ligne de commande a le même effet.

5. Cliquez sur *Enregistrer et fermer*.
6. Redémarrez le service en cliquant avec le bouton droit sur le nom du serveur WACS, par exemple `MySIA.WebApplicationContainerServer`, puis cliquez sur *Redémarrer le serveur*.

13.1.8.2.2 Configuration des propriétés système

13.1.8.2.2.1 Activation de la pile de messages d'erreur

En tant qu'administrateur, vous pouvez configurer les messages d'erreur renvoyés par les services Web de type RESTful pour qu'ils incluent la pile d'erreurs. La pile d'erreurs fournit des informations de débogage supplémentaires qui peuvent être utilisées pour comprendre d'où proviennent les erreurs.

> **Remarque**
>
> Il n'est pas toujours souhaitable d'activer la pile d'erreurs dans les scénarios de production, car elle peut fournir des informations sur la plateforme de BI que vous ne voulez pas révéler aux utilisateurs finaux. Il est recommandé d'activer la pile d'erreurs dans les scénarios de production pour le débogage, puis de la désactiver une fois l'opération terminée.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Service Web de type RESTful*, sélectionnez *Afficher la pile d'erreurs*.
5. Cliquez sur *Enregistrer et fermer*.

Les informations de la pile d'erreurs figurent dans les messages d'erreur du service Web de type RESTful.

13.1.8.2.2.2 Définition du nombre d'entrées par défaut affichées sur chaque page

Lorsqu'une réponse de service Web de type RESTful contient un flux avec de nombreuses entrées, la réponse peut être divisée en plusieurs pages. Vous pouvez configurer le nombre d'entrées par défaut à afficher sur chaque page. Lorsque les développeurs effectuent des requêtes de services Web de type RESTful, ils peuvent spécifier le nombre d'entrées à afficher sur chaque page. S'ils ne spécifient aucune valeur, la taille de page par défaut est utilisée.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Service Web de type RESTful*, saisissez la taille de page par défaut dans la zone de texte *Nombre d'objets par défaut sur une page*.
5. Cliquez sur *Enregistrer et fermer*.

13.1.8.2.2.3 Définition de la valeur de dépassement du délai d'attente d'un jeton de connexion

Lorsqu'ils ne sont pas utilisés, les jetons de connexion expirent au bout d'un certain délai. Vous pouvez définir la durée de validité d'un jeton de connexion inutilisé.

> **Remarque**
>
> Par défaut, la valeur de dépassement du délai d'attente d'un jeton de connexion est d'une heure.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone de texte *Délai d'expiration du jeton de session de l'entreprise (minutes)* du champ *Service Web de type RESTful*, saisissez le nombre de minutes pendant lesquelles un jeton de connexion reste valide.
5. Cliquez sur *Enregistrer et fermer*.

13.1.8.2.2.4 Configuration des paramètres du groupe de sessions

Vous pouvez améliorer les performances du serveur en utilisant un groupe de sessions. Le groupe de sessions met en cache les sessions de services Web actives de type RESTful afin qu'elles puissent être réutilisées lorsqu'un utilisateur envoie une autre requête qui utilise le même jeton de connexion dans l'en-tête de requête HTTP. La taille du groupe de sessions définit le nombre de sessions mises en cache à stocker en même temps et la valeur du délai d'expiration de la session contrôle la durée de mise en cache d'une session.

Vous pouvez définir la taille du groupe de sessions et la valeur du délai d'expiration de la session :

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Saisissez le nombre maximum de sessions à mettre en cache dans la zone de texte *Taille du groupe de sessions* du champ *Service Web de type RESTful*.
5. Saisissez la valeur du délai d'expiration du groupe de sessions dans la zone de texte *Délai d'expiration du groupe de sessions (minutes)* du champ *Service Web de type RESTful*.
6. Cliquez sur *Enregistrer et fermer*.
7. Cliquez avec le bouton droit sur le serveur WACS, par exemple `MySIA.WebApplicationContainerServer`, puis cliquez sur *Redémarrer le serveur*.

13.1.8.2.2.5 Activation de l'authentification HTTP élémentaire

L'authentification HTTP élémentaire permet aux utilisateurs d'effectuer des requêtes de services Web de type RESTful sans fournir de jeton de connexion. Si l'authentification HTTP élémentaire est activée, les utilisateurs sont invités à indiquer leur nom d'utilisateur et leur mot de passe la première fois qu'ils effectuent une requête de service Web de type RESTful.

> **Remarque**
>
> Les noms d'utilisateur et les mots de passe ne sont pas transmis de manière sécurisée avec l'authentification HTTP élémentaire, sauf si elle est utilisée conjointement avec HTTPS.

Lorsque vous activez l'authentification HTTP élémentaire, vous définissez le type d''authentification HTTP élémentaire par défaut sur SAP, Enterprise, LDAP ou WinAD. Les utilisateurs peuvent remplacer le type d'authentification HTTP élémentaire par défaut lorsqu'ils se connectent.

La connexion à la plateforme de BI à l'aide de l'authentification HTTP élémentaire utilise une licence. Si la mise en cache du groupe de sessions est utilisée, la requête utilise la licence associée à sa session mise en mémoire cache. Si la mise en cache du groupe de sessions n'est pas utilisée, une licence est utilisée lorsque la requête est en cours de traitement et libérée une fois la requête terminée.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveur* > *Listes des serveurs* >.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Service Web de type RESTful*, sélectionnez *Activer l'authentification HTTP élémentaire*.
5. (Facultatif) Dans la liste *Plan d'authentification par défaut pour HTTP élémentaire*, sélectionnez le type d'authentification HTTP élémentaire par défaut.
6. Cliquez sur *Enregistrer et fermer*.

Lorsqu'un utilisateur final se connecte en utilisant l'authentification HTTP élémentaire, il peut spécifier le type d'authentification à utiliser. Dans un navigateur Web, les types d'utilisateur `<type d'authentification>\<nom d'utilisateur>` dans l'invite de nom d'utilisateur et `<mot de passe>` dans l'invite de mot de passe.

Pour se connecter en utilisant l'authentification HTTP élémentaire par programme, les utilisateurs ajoutent l'attribut `Autorisation` à l'en-tête de requête HTTP et définissent la valeur sur `Basic <type d'authentification>\<nom d'utilisateur>:<mot de passe>`.

Remplacez `<type d'authentification>` par le type d'authentification, `<nom d'utilisateur>` par le nom d'utilisateur et `<mot de passe>` par le mot de passe. Le type d'authentification, le nom d'utilisateur et le mot de passe doivent être codés en Base64 tel que défini par RFC 2617. Les noms d'utilisateur contenant le caractère `:` ne peuvent pas être utilisés avec l'authentification HTTP élémentaire.

Informations associées

Configuration des paramètres du groupe de sessions [page 550]

13.1.8.2.3 Cross-Origin Resource Sharing

13.1.8.2.3.1 Configuration de CORS (Cross-Origin Resource Sharing)

Le paramètre *Configuration de Cross-Origin Resource Sharing* (CORS) permet d'ajouter une liste de noms de domaines de façon à ce que les utilisateurs puissent extraire des données à partir de sources multiples dans des pages Web de type JavaScript. Cela est nécessaire pour contourner la politique de sécurité employée par

les langages JavaScript et Ajax afin d'empêcher les accès multi-domaines. Pour éviter de compromettre la sécurité, seuls les sites Web pour lesquels l'accès est autorisé sont ajoutés aux propriétés *Autoriser les origines* du serveur WACS dans la CMC.

Un paramètre *Age maximum (minutes)* est également disponible pour ajuster l'heure d'expiration du cache, permettant de définir le nombre maximum de minutes pendant lesquelles les navigateurs peuvent conserver les requêtes HTTP.

> **Remarque**
>
> Par défaut, l'accès à tous les domaines est autorisé avec un astérisque (*).

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveur* > *Listes des serveurs* >.
3. Cliquez avec le bouton droit sur le serveur conteneur d'applications Web (WACS), par exemple sur `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Service Web de type RESTFul*, repérez la zone de texte *Configuration de Cross-Origin Resource Sharing* située en regard de l'option *Autoriser les origines :* et remplacez l'astérisque (*) par votre liste de noms de domaines, en séparant chacun d'eux par une virgule. Par exemple : `http://origin1.server:8080, http://origin2.server:8080`
5. Dans la zone de texte *Age maximum (minutes) :,* saisissez le nombre maximum de minutes pendant lesquelles vous souhaitez que les navigateurs conservent les requêtes HTTP dans la mémoire cache.
6. Cliquez sur *Enregistrer et fermer*.

13.1.8.2.4 Authentification

13.1.8.2.4.1 Configuration de web.xml pour activer la connexion unique WinAD

La configuration des services Web RESTful en vue de reconnaître la connexion unique Windows Active Directory (connexion unique WinAD) nécessite d'apporter des modifications au fichier de configuration `web.xml` , situé sur le serveur de la plateforme de BI. Pour de plus amples informations, consultez « Utilisation du SDK > Authentification > Obtention d'un jeton de connexion à l'aide d'un compte à connexion unique Active Directory (connexion unique AD) » dans le *Guide du développeur de services Web RESTful pour plateforme de Business Intelligence*.

Pour que les références de connexion unique WinAD d'une machine client soient reconnues par le serveur de plateforme de BI, vous devez retirer les commentaires de la section `Filtre Kerberos du serveur proxy` du fichier `web.xml` et mettre à jour les valeurs correspondant à`idm.realm`, `idm.princ` et `idm.keytab` qui indiquent l'environnement Active Directory utilisé.

1. Accédez au fichier de configuration `web.xml` en passant par `<racine boe>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. Le chemin d'accès suivant a valeur d'exemple.

   ```
   C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
   4.0\java\
   ```

```
pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. Dans le fichier `web.xml`, retirez le commentaire de la section Filtre Kerberos du serveur proxy en ajoutant une étiquette de fermeture de commentaire `-->` avant la balise `<filtre>`, puis supprimez la balise de fermeture de commentaire `-->`

```
  <!-- Kerberos Proxy Filter
    - Uncomment this filter and the corresponding filter-mapping to enable
Kerberos SSO
    - for Windows AD (secWinAD) authentication.
    - The following options must be specified (the rest are optional):
    -   idm.realm
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->
  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>
  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>

</web-app>
```

3. Mettez à jour la `<valeur de paramètre>` en remplaçant chaque paramètre `idm.realm`, `idm.princ` et `idm.keytab` par ceux qui sont utilisés dans votre environnement Active Directory.

```
    <init-param>
      <param-name>idm.realm</param-name>
      <param-value>ADDOM.COM</param-value>
      <description>
          Required: Set this value to the Kerberos realm to use.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.princ</param-name>
      <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>
      <description>
          Set this value to the Kerberos service principal to use.
          This will be a name of the form HTTP/fully-qualified-host.
          For example, HTTP/example.vintela.com
          If not set, defaults to the server's hostname and the
          idm.realm  property above.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.kdc</param-name>
      <param-value></param-value>
      <description>
          The KDC against which secondary credentials must be validated
          This can be used for BASIC fallback or credential delegation.
          By default the KDC will be discovered automatically and this
          parameter must only be used if automatic discovery fails, or
          if a different KDC to the one discovered must automatically be used.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.keytab</param-name>
      <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
      <description>
          The file containing the keytab that Kerberos will use for
          user-to-service authentication. If unspecified, SSO will default
```

```
        to using an in-memory keytab with a password specified in the
        com.wedgetail.idm.sso.password environment variable.
    </description>
  </init-param>
```

> **Remarque**
>
> La valeur `idm.keytab` se rapporte à un chemin d'accès présent sur le serveur de plateforme de BI. Les valeurs de `idm.realm` et de `idm.prince` peuvent être affichées à partir de la Central Management Console. Dans l'onglet *Authentification* de la CMC, cliquez deux fois sur *Windows AD*. La valeur de `idm.realm` est définie avec le paramètre *Domaine AD par défaut*, sous *Synthèse de configuration d'AD*. La valeur de `idm.prince` est définie avec le paramètre *Nom principal du service*, sous *Options d'authentification*.

4. Redémarrez le service WACS de sorte que les modifications apportées au fichier `web.xml` soient reconnues.
5. Utilisez une machine client pour vérifier que le jeton de connexion unique AD peut être extrait via l'API des services Web RESTful, (par exemple, `http://<hôte boe>:6405/biprws/logon/adsso`).
6. Testez le jeton à l'aide d'une requête `GET` incluant `X-SAP-LogonToken` dans son en-tête et utilisant l'API `/infostore`.

13.1.8.2.4.2 Activation et configuration de l'authentification sécurisée

L'authentification sécurisée est activée et configurée via la CMC (Central Management Console) dans les domaines qui incluent *Authentification > Entreprise*, où elle est activée. Un fichier clé de secret partagé est généré, *Utilisateurs et groupes > Liste des utilisateurs*, dans lequel un compte est créé pour un utilisateur sécurisé dans le chemin d'accès suivant *Serveurs > Liste des serveurs > WACS > Propriétés*. Ici, l'option *Méthode d'extraction* est sélectionnée pour les requêtes de jeton de connexion à l'API de type `/logon/trusted`.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Accédez à *Authentification* > *Entreprise*, puis cliquez sur *L'authentification sécurisée est activée*.
3. Cliquez sur *Nouveau secret partagé*, puis cliquez sur *Télécharger le secret partagé*.
4. Cliquez sur *Enregistrer*, puis placez le fichier `TrustedPrincipal.conf` à l'emplacement par défaut, `<EnterpriseDir>\<platform>`.
   L'emplacement peut être par exemple :

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI
4.0\win64_x64\"
```

> **Remarque**
>
> Vous pouvez modifier l'emplacement par défaut du fichier de secret partagé `TrustedPrincipal.conf` en ajoutant une entrée de ligne de commande dans la CMC par le chemin suivant *Serveurs > Liste des serveurs > WACS > Propriétés > Paramètres de ligne de commande*, puis en redémarrant le service WACS. Par exemple, avec une entrée de ligne de commande utilisant `-Dbobj.trustedauth.home=` et en plaçant le dossier `SharedSecrets` à la racine du lecteur `C:\` du serveur de plateforme de BI, l'emplacement apparaît comme suit :
>
> ```
> "-Dbobj.trustedauth.home=C:\SharedSecrets"
> ```

> **Remarque**
>
> Vous pouvez laisser l'option *Période de validité du secret partagé (jours)* sur sa valeur par défaut de zéro (0) de manière à n'appliquer aucune expiration. L'option *Une requête de connexion sécurisée expire au bout de N milliseconde(s) (0 signifie qu'il n'existe pas de limite)* peut être laissée sur sa valeur par défaut de zéro (0) de manière à n'appliquer aucune expiration aux requêtes de connexion sécurisée.

5. Cliquez sur *Mettre à jour* pour enregistrer la modification.
6. Ajoutez un nouvel utilisateur et un nouveau mot de passe, par exemple `bob` et `Passw0rd` dans *Utilisateurs et groupes* > *Liste des utilisateurs* en accédant à *Gérer > Nouveau > Nouvel utilisateur*. Désélectionnez l'option *L'utilisateur doit modifier le mot de passe à la prochaine session*, puis cliquez sur *Créer et fermer*.

> **Remarque**
>
> Vous pouvez également créer un utilisateur en cliquant sur l'icône *Créer un utilisateur* ou en cliquant avec le bouton droit dans une zone ouverte de la fenêtre dressant la liste des utilisateurs, puis sélectionnez *Nouveau* > *Nouvel utilisateur*.

7. Accédez à *Serveurs* > *Services principaux* > *WACS* > *Propriétés*, faites défiler l'arborescence jusqu'à la section *Configuration de l'authentification sécurisée* et utilisez le menu *Méthode d'extraction* pour sélectionner *HTTP_HEADER*, *QUERY_STRING* ou *COOKIE*.

> **Remarque**
>
> Si vous le souhaitez, pour le *Paramètre du nom d'utilisateur*, vous pouvez remplacer l'étiquette par défaut de `X-SAP-TRUSTED-USER` par toute étiquette appropriée (par exemple `UserName`, `bankteller` ou `nurse`) devant être utilisée par les développeurs des services Web RESTful.

8. Redémarrez le service en cliquant avec le bouton droit sur le nom du serveur WACS, par exemple `MySIA.WebApplicationContainerServer`, puis cliquez sur *Redémarrer le serveur*.

> **Remarque**
>
> Une modification ultérieure de l'option *Méthode d'extraction* comme indiqué dans l'étape 7 ne nécessite pas un redémarrage du serveur WACS.

9. Vérifiez que vous parvenez à extraire un jeton de connexion à l'aide de l'API `.../biprsw/logon/trusted/` et en envoyant une requête `GET` avec l'étiquette d'en-tête par défaut de `X-SAP-TRUSTED-USER` et le nom d'utilisateur créé à l'étape 6.

13.1.8.2.4.3 Configuration du paramètre de ligne de commande en vue de déplacer le fichier de configuration du secret partagé `TrustedPrincipal.conf`

Les services Web RESTful incluent un paramètre de ligne de commande permettant de choisir un autre emplacement pour le fichier `TrustedPrincipal.conf` de l'authentification sécurisée.

Le fichier `TrustedPrincipal.conf` contient une clé secrète partagée générée via la CMC : cliquez sur *Authentification*, puis cliquez deux fois sur *Enterprise*. Sélectionnez*L'authentification sécurisée est activée*, puis cliquez sur le bouton *Nouveau secret partagé*. Enregistrez le fichier en cliquant sur *Télécharger le secret partagé* et en sauvegardant le fichier dans l'emplacement partagé.

Mettez à jour la ligne de commande du serveur conteneur d'applications Web (WACS) en indiquant l'emplacement de votre choix pour le fichier `TrustedPrincipal.conf`, comme suit :

1. Connectez-vous à la CMC (Central Management Console) en tant qu'administrateur.
2. Cliquez sur *Serveurs*, puis sur *Liste des serveurs*.
3. Cliquez avec le bouton droit sur votre service WACS, par exemple `MySIA.WebApplicationContainerServer`, puis cliquez sur *Propriétés*.
   L'onglet *Propriétés* du serveur WACS s'affiche.
4. Dans la zone *Paramètres de ligne de commande*, saisissez le chemin d'accès au répertoire devant contenir le fichier `TrustedPrincipal.conf`.

   Cette chaîne est encadrée par des guillemets, comme l'illustre l'exemple suivant.

   ```
   "-Dbobj.trustedauth.home=C:\SharedSecrets"
   ```

   > **Remarque**
   >
   > L'emplacement par défaut du fichier `TrustedPrincipal.conf` est `<RépEnterprise>\<plateforme>`. L'emplacement peut être par exemple :
   >
   > ```
   > C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise
   > XI 4.0\win64_x64
   > "
   > ```
5. Cliquez sur *Enregistrer et fermer*.
6. Redémarrez le service en cliquant avec le bouton droit sur le nom du serveur WACS, par exemple `MySIA.WebApplicationContainerServer`, puis cliquez sur *Redémarrer le serveur*.

13.1.9 Configuration des serveurs WACS dans votre environnement informatique

Cette section explique comment configurer un serveur WACS dans un environnement complexe.

13.1.9.1 Utilisation d'un serveur WACS avec d'autres serveurs Web

Lorsqu'un serveur WACS est installé, il fonctionne comme un serveur d'applications et un serveur Web sans nécessiter de configuration supplémentaire. Vous pouvez configurer les serveurs Web pris en charge tels qu'IIS et Apache afin qu'ils puissent transférer des URL vers le serveur WACS.

> ⓘ Remarque
>
> Le transfert de demandes à partir d'ISS à l'aide d'un filtre ISAPI vers les serveurs WACS n'est pas pris en charge.

Les serveurs WACS ne prennent pas en charge les scénarios de déploiement dans lesquels un serveur Web héberge du contenu statique et un serveur WACS héberge du contenu dynamique. Les contenus statiques et dynamiques doivent toujours résider sur les serveurs WACS.

13.1.9.2 Utilisation des serveurs WACS avec un équilibreur de charge

Pour utiliser un serveur WACS dans un environnement comportant un équilibreur de charge matériel ou logiciel, vous devez configurer ce dernier de façon à ce qu'il utilise le routage IP ou les cookies actifs. Ensuite, lorsqu'une session utilisateur est établie sur un serveur WACS, toutes les demandes suivantes émanant du même utilisateur sont envoyées au même serveur WACS.

Les serveurs WACS ne sont pas pris en charge avec des équilibreurs de charge utilisant des cookies passifs.

Si votre équilibreur de charge matériel transmet des demandes HTTPS cryptées avec SSL, vous devez configurer HTTPS sur les serveurs WACS et installer des certificats SSL sur chacun de ces serveurs.

Si votre équilibreur de charge matériel décrypte le trafic HTTPS et transmet des demandes HTTP décryptées à vos serveurs WACS, aucune configuration de serveur WACS supplémentaire n'est nécessaire.

Informations associées

Configuration HTTPS/SSL [page 532]

13.1.9.3 Utilisation d'un serveur WACS avec un serveur proxy inverse

Vous pouvez utiliser un serveur WACS dans un déploiement comportant un serveur proxy ou un serveur proxy inverse. Vous ne pouvez pas utiliser le serveur WACS lui-même en tant que serveur proxy.

13.1.9.3.1 Pour configurer un serveur WACS de façon à ce qu'il prenne en charge le protocole HTTP à l'aide d'un serveur proxy inverse

Pour utiliser un serveur WACS dans un déploiement comportant un serveur proxy inverse, configurez votre serveur WACS de façon à ce que le port HTTP soit utilisé pour communiquer à l'intérieur d'un pare-feu (sur un réseau sécurisé, par exemple) et le port HTTP via proxy pour communiquer à l'extérieur du pare-feu (sur internet, par exemple).

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS que vous souhaitez configurer.
   L'écran *Propriétés* s'affiche.
3. Dans la section *Configuration du port HTTP via proxy*, procédez comme suit :
   a. Activez la case à cocher *Activer HTTP via proxy*.
   b. Spécifiez le port HTTP devant être utilisé par le serveur WACS pour communiquer via le serveur proxy.
   c. Spécifiez le nom d'hôte et le port du serveur proxy.
4. Cliquez sur *Enregistrer et fermer*.

13.1.9.3.2 Pour configurer un serveur WACS de façon à ce qu'il prenne en charge le protocole HTTPS à l'aide d'un serveur proxy inverse

Vous pouvez configurer certains équilibreurs de charge et serveurs proxy inverses de façon à ce qu'ils décryptent le trafic HTTPS, puis transfèrent le trafic décrypté vers vos serveurs d'applications. Dans ce cas, vous pouvez configurer le serveur WACS de sorte qu'il utilise HTTP ou HTTP via proxy.

Si votre équilibreur de charge ou serveur proxy inverse transmet le trafic HTTPS et si vous souhaitez configurer HTTPS avec un serveur proxy inverse, créez deux serveurs WACS. Configurez un serveur WACS pour HTTPS dédié au trafic externe via le serveur proxy inverse et l'autre serveur WACS dédié à la communication avec les clients faisant partie de votre réseau interne via HTTPS.

13.1.9.4 Utilisation des serveurs WACS avec des pare-feu

Le déploiement de serveurs WACS dans un environnement informatique comportant des pare-feu est pris en charge.

Par défaut, les serveurs WACS sont liés à toutes les adresses IP de l'ordinateur sur lequel ils sont installés. Si vous envisagez d'utiliser un pare-feu entre les clients et votre serveur WACS, vous devez forcer la liaison du serveur à une adresse IP spécifique pour HTTP ou HTTP via proxy. Pour ce faire, désactivez la case à cocher *Lier à toutes les adresses IP*, puis spécifiez le nom d'hôte ou l'adresse IP auquel ou à laquelle lier le serveur.

Si vous envisagez d'utiliser un pare-feu entre un serveur WACS et les autres serveurs de la plateforme de BI de votre déploiement, consultez la section « Description de la communication entre les composants de la plateforme de BI » du *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.

Informations associées

Description de la communication entre les composants de la plateforme de BI [page 197]

13.1.9.5 Configuration d'un serveur WACS sur un ordinateur multirésidents

Un ordinateur multirésidents est un ordinateur qui possède plusieurs adresses réseau. Par défaut, une instance de serveur WACS lie son port HTTP à toutes les adresses IP. Si vous souhaitez lier le serveur WACS à une carte d'interface réseau spécifique, par exemple, pour lier le port HTTP du serveur à une carte d'interface réseau et lier la le port de requêtes à une autre carte d'interface réseau :

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS que vous souhaitez configurer.
   L'écran *Propriétés* s'affiche.
3. Dans la section *Configuration du port HTTP via proxy* du volet *Service conteneur d'applications Web*, décochez la case *Lier à toutes les adresses IP*, puis saisissez l'adresse IP à laquelle lier le serveur WACS.
4. Dans la section *Configuration HTTPS*, décochez la case *Lier à toutes les adresses IP*, puis saisissez une adresse IP ou un nom d'hôte auxquels lier le serveur WACS.
5. Sous *Paramètres courants*, désélectionnez *Affecter automatiquement*, puis spécifiez le nom d'hôte ou l'adresse IP de la carte d'interface réseau utilisée pour communiquer entre le serveur WACS et les autres serveurs de la plateforme de BI de votre déploiement.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez le serveur WACS.

13.1.10 Configuration des propriétés d'applications Web

Les propriétés d'applications Web hébergées sur un serveur WACS peuvent être configurées comme suit :

- Les propriétés qui sont souvent modifiées sont présentées comme des propriétés de services configurables pour le serveur WACS. Pour modifier ces propriétés, ouvrez la page *Propriétés* du WACS dans la Central Management Console (CMC), modifiez la valeur de la propriété appropriée et cliquez sur *Enregistrer*.
- Pour modifier les délais d'expiration de session pour les applications Web hébergées sur serveur WACS, déterminez d'abord si l'application Web a des propriétés pouvant être configurées dans la CMC.
  Si l'application Web a des propriétés pouvant être modifiées dans la CMC, modifiez alors le fichier `web_xml.ino` pour l'application Web. Le fichier est `<NomAppWeb>_web_xml.ino`, où `<NomAppWeb>` est le nom de l'application Web et se trouve dans le répertoire `<RépertoireEnterprise>/java/pjs/services/<NomAppWeb>`.
  Si l'application Web n'a pas de propriétés pouvant être modifiées dans la CMC, modifiez le fichier `web.xml` pour l'application Web. Vous pouvez trouver ce fichier sous `<RépertoireEnterprise>/warfile/webapps/<NomAppWeb>`, où `<NomAppWeb>` est le nom de l'application Web.
- Pour modifier des propriétés autres que le délai d'expiration de session ou les propriétés s'affichant dans l'écran *Propriétés* du WACS dans la CMC, modifiez le fichier `.properties` de l'application Web. Pour en

savoir plus, voir la section « Gestion des applications via les propriétés du fichier BOE.war » du *Guide d'administration de la plateforme SAP Business Intelligence*.

> **Remarque**
>
> Ne modifiez pas les fichiers `web.xml`, `web_xml.ino` ou `.properties` dans le répertoire `<RépertoireEnterprise>/java/pjs/container/work/<NomServeurConvivial>`, car votre modification serait écrasée à chaque démarrage ou redémarrage du serveur WACS.

> **Remarque**
>
> Après avoir modifié les propriétés d'un WACS, vous devez toujours le redémarrer.

Informations associées

Pour modifier les propriétés d'un serveur [page 468]
Fichier war BOE [page 771]

13.1.11 Dépannage

13.1.11.1 Pour configurer le suivi sur un serveur WACS

Pour configurer le suivi d'un serveur WACS, voir Journalisation des traces de composant [page 1088]

13.1.11.2 Affichage des métriques de serveur

Vous pouvez visualiser les métriques du serveur WACS à partir de la CMC (Central Management Console).

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez avec le bouton droit de la souris sur le serveur WACS, puis cliquez sur *Métriques*.

Informations associées

Métriques de serveurs conteneurs d'applications Web [page 1223]

13.1.11.3 Visualisation de l'état d'un serveur WACS

Pour visualiser l'état d'un serveur WACS, accédez à la zone *Serveurs* de la CMC. La *liste des serveurs* comprend une colonne *Etat* qui indique l'état de chaque serveur figurant dans la liste.

Il existe un état applicable aux serveurs WACS appelé « Exécution avec des erreurs ». Cet état signifie que le WACS est en cours d'exécution, mais qu'il comporte une ou plusieurs des conditions d'erreur suivantes :

- Un connecteur HTTP, HTTP via proxy ou HTTPS est mal configuré.
- Un service qui s'exécute sur WACS, tel que le service de journal de suivi, ne s'exécute pas correctement.
- Une application Web n'a pas réussi le déploiement dans WACS.

Voir aussi la page *Propriétés* du WACS pour connaître les services ayant échoué.

13.1.11.4 Résolution des conflits de ports

Si vous n'obtenez aucune page lorsque vous essayez de vous connecter à la CMC via un port particulier, assurez-vous qu'aucune autre application n'utilise les ports HTTP, HTTP via proxy ou HTTPS spécifiés pour le serveur WACS.

Il existe deux moyens de détecter les conflits de ports liés aux serveurs WACS. Si votre déploiement comporte plusieurs serveurs WACS, connectez-vous à la CMC, puis vérifiez les connecteurs WACS en cours d'exécution ainsi que les métriques d'échec lors du démarrage des connecteurs WACS. Si les connecteurs HTTP, HTTP via proxy ou HTTPS ne figurent pas dans la liste des connecteurs WACS en cours d'exécution, ils ne peuvent pas démarrer en raison d'un conflit de ports.

Si votre déploiement ne comporte qu'un seul serveur WACS, ou si vous ne parvenez pas à accéder à la CMC via l'un de vos serveurs WACS, utilisez un utilitaire tel que netstat afin de déterminer si une autre application utilise le port de serveur WACS.

13.1.11.4.1 Pour résoudre les conflits de ports HTTP

1. Démarrez le CCM (Central Configuration Manager), puis cliquez sur l'icône *Gérer les serveurs*.
2. Indiquez les références de connexion.
3. Dans l'écran *Gérer les serveurs*, arrêtez le serveur WACS.
4. Cliquez sur l'icône *Configuration du niveau Web*.

   > **Remarque**
   >
   > L'icône *Configuration de niveau Web* n'est activée que lorsque vous sélectionnez un serveur WACS arrêté.

   L'écran *Configuration de niveau Web* s'affiche.
5. Dans le champ *Port HTTP*, spécifiez un port HTTP disponible pouvant être utilisé par le serveur WACS, puis cliquez sur *OK*.
6. Dans l'écran *Gérer les serveurs*, démarrez le serveur WACS.

13.1.11.4.2 Pour résoudre les conflits de ports HTTP via proxy ou HTTPS

Si vous ne pouvez pas accéder à un serveur WACS via le port HTTP via proxy ou le port HTTPS, mais parvenez tout de même à vous connecter à la CMC (Central Management Console) via le port HTTP, changez les numéros de port par le biais de la CMC.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Pour arrêter les serveurs WACS, cliquez avec le bouton droit de la souris sur le serveur devant être configuré, puis cliquez sur *Arrêter le serveur*.
3. Cliquez deux fois sur le serveur WACS que vous souhaitez configurer.
   L'écran *Propriétés* s'affiche.
4. Dans la section *Configuration du port HTTP via proxy*, spécifiez un nouveau de port HTTP.
5. Pour changer le port HTTPS, dans la section *Configuration HTTPS*, saisissez une nouvelle valeur dans le champ *Port HTTPS*.
6. Cliquez sur *Enregistrer et fermer*.
7. Pour démarrer le serveur WACS, cliquez avec le bouton droit de la souris sur le serveur, puis cliquez sur *Démarrer le serveur*.

13.1.11.5 Pour modifier les paramètres de la mémoire

Afin d'améliorer les performances des serveurs WACS, vous pouvez modifier la quantité de mémoire allouée au serveur via le CCM (Central Configuration Manager).

1. Démarrez le CCM, puis cliquez sur l'icône *Gérer les serveurs*.
2. Indiquez les références de connexion pour le CCM.
3. Dans l'écran *Gérer les serveurs*, arrêtez le serveur WACS.
4. Cliquez sur l'icône *Configuration du niveau Web*.

   > **Remarque**
   >
   > L'icône *Configuration de niveau Web* n'est activée que lorsque vous sélectionnez un serveur WACS arrêté.

   L'écran *Configuration de niveau Web* s'affiche.
5. Sous *Paramètres de ligne de commande*, spécifiez une nouvelle valeur pour la mémoire en modifiant la ligne de commande :
   a. Recherchez l'option `-Xmx`. Normalement, une valeur lui est déjà attribuée.
      Par exemple « -Xmx1g ». Ce paramètre alloue un gigaoctet de mémoire au serveur.
   b. Spécifiez une nouvelle valeur pour ce paramètre.
      - Pour spécifier une valeur en mégaoctets, utilisez « m ». Par exemple, « **`-Xmx640m`** » alloue 640 mégaoctets de mémoire au serveur WACS.
      - Pour spécifier une valeur en gigaoctets, utilisez « g ». Par exemple, « **`-Xmx2g`** » alloue deux gigaoctets de mémoire au serveur WACS.

c. Cliquez sur *OK*.

6. Dans l'écran *Gérer les serveurs*, démarrez le serveur WACS.

13.1.11.6 Pour modifier le nombre de demandes simultanées

Par défaut, les serveurs WACS sont configurés pour gérer 150 demandes HTTP simultanées. Ce nombre est suffisant pour la plupart des scénarios de déploiement. Toutefois, afin d'améliorer les performances des serveurs WACS, vous pouvez augmenter le nombre maximal de demandes HTTP simultanées. Attention cependant à ne pas définir une valeur trop élevée, sous peine d'obtenir l'effet inverse. Le nombre idéal dépend du matériel, des logiciels et des configurations requises.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Pour arrêter les serveurs WACS, cliquez avec le bouton droit de la souris sur le serveur devant être configuré, puis cliquez sur *Arrêter le serveur*.
3. Cliquez deux fois sur le serveur WACS que vous souhaitez configurer.
   L'écran *Propriétés* s'affiche.
4. Sous *Paramètres d'accès simultané (par connecteur)*, dans le champ *Nombre maximal de demandes simultanées*, saisissez le nombre souhaité, puis cliquez sur *Enregistrer et fermer*.
5. Pour démarrer le serveur WACS, cliquez avec le bouton droit de la souris sur le serveur, puis cliquez sur *Démarrer le serveur*.

13.1.11.7 Pour restaurer les valeurs par défaut du système

En cas de configuration incorrecte d'un serveur WACS, vous pouvez restaurer les valeurs par défaut du système via le CCM (Central Configuration Manager).

1. Démarrez le CCM, puis cliquez sur l'icône *Gérer les serveurs*.
2. Indiquez les références de connexion.
3. Dans l'écran *Gérer les serveurs*, arrêtez le serveur WACS.
4. Cliquez sur l'icône *Configuration de niveau Web*.

   > **Remarque**
   >
   > L'icône *Configuration de niveau Web* n'est activée que lorsque vous sélectionnez un serveur WACS arrêté.

   L'écran *Configuration de niveau Web* s'affiche.
5. Cliquez sur *Restaurer les paramètres par défaut du système*.
6. Si nécessaire, indiquez un port HTTP disponible, puis cliquez sur *OK*.
7. Dans l'écran *Gérer les serveurs*, démarrez le serveur WACS.

13.1.11.8 Pour empêcher les utilisateurs de se connecter au serveur WACS via HTTP

Dans certains cas, il se peut que vous souhaitiez autoriser uniquement les utilisateurs de l'ordinateur local à se connecter au serveur WACS via HTTP ou HTTPS. Par exemple, bien que vous ne puissiez pas fermer le port HTTP, il se peut que vous souhaitiez configurer votre serveur WACS de façon à ce qu'il accepte uniquement les demandes HTTP émanant des clients situés sur le même ordinateur que le serveur WACS. Ainsi, vous pouvez effectuer des tâches de gestion ou de configuration sur le serveur WACS via un navigateur à partir du même ordinateur que celui sur lequel se trouve le serveur, tout en empêchant les autres utilisateurs d'accéder à ce serveur.

1. Accédez à la zone de gestion *Serveurs* de la CMC.
2. Cliquez deux fois sur le serveur WACS à modifier.
   L'écran *Propriétés* s'affiche.
3. Dans la section *Service conteneur d'applications Web*, décochez la case *Lier à toutes les adresses IP*.
4. Dans le champ *Lier au nom d'hôte ou à l'adresse IP*, saisissez **`127.0.0.1`**, puis cliquez sur *Enregistrer et fermer*.
5. Pour démarrer le serveur WACS, cliquez avec le bouton droit de la souris sur le serveur, puis cliquez sur *Démarrer le serveur*.
   Le serveur WACS configuré de cette façon n'accepte que les connexions de l'ordinateur local.

13.1.12 Propriétés des serveurs WACS

Pour obtenir la liste complète des propriétés de configuration générales, HTTP, HTTP via proxy et HTTPS pouvant être définis pour les serveurs WACS, voir la section « Paramètres de serveur principaux » dans l'« Annexe relative aux propriétés des serveurs ».

Informations associées

Propriétés des services principaux [page 1178]

14 Sauvegarde et restauration de votre système

14.1 Présentation de la sauvegarde et de la restauration

Ce chapitre explique comment sauvegarder la plateforme de BI et restaurer le système après défaillance matérielle ou logicielle et perte de données. Pour exécuter un plan de sauvegarde et de restauration, il faut un professionnel SAP BusinessObjects expérimenté, un administrateur système et un administrateur de base de données.

Informations associées

Sauvegarde du système entier [page 569]
Sauvegarde du contenu BI [page 575]
Pour sauvegarder les paramètres du serveur à l'aide du CCM sous Windows [page 573]
Pour sauvegarder des paramètres de serveur sous UNIX [page 574]
Présentation de la copie du système [page 590]

14.2 Terminologie

Terme	Définition
Réplication de données	La réplication de données est le processus de création d'une ou plusieurs copies des données. Les copies sont mises à jour en temps réel, par exemple en utilisant des disques en miroir. Elle offre une protection des données en temps réel contre les dommages physiques occasionnés aux données, mais les disques étant constamment mis à jour, il n'est pas possible de restaurer votre système à un état antérieur si les données viennent à être corrompues ou supprimées par erreur.

Terme	Définition
Gestion des versions	Le versionnement crée plusieurs versions d'un ou plusieurs fichiers spécifiques sur votre système. Dans ce cas, il est possible de restaurer un état antérieur de votre système. Toutes les versions des données sont généralement stockées sur le même système hôte. Si ce système est compromis ou endommagé, vous risquez de perdre aussi bien la version actuelle que les anciennes versions. De même, les fonctions Annuler la suppression conservent des copies des fichiers "supprimés" pour une restauration ultérieure, mais celles-ci aussi sont généralement stockées sur le même système hôte que les données d'origine. Cela n'offre aucune protection contre un dommage physique aux données (par exemple, défaillance de disque).
Sauvegarde système complète	Une sauvegarde système complète est une sauvegarde d'un système de fichiers complet, y compris le système d'exploitation. La sauvegarde système complète est destinée à restaurer un système sauvegardé sur un matériel ne contenant aucun logiciel ni système d'exploitation. Pour les sauvegardes système complètes, en cas de défaillance, le système de fichiers complet (y compris le SE) est restauré sur un matériel identique ou sur tout autre matériel si vos outils de restauration prennent en charge la restauration indépendante du matériel.
Sauvegarde système complète et sauvegarde d'applications	Une sauvegarde système complète crée une copie du système complet, y compris le système d'exploitation. Elle permet de restaurer une version antérieure du système dans son intégralité. Une sauvegarde d'applications sauvegarde les fichiers concernant des applications individuelles. La plateforme de BI prend en charge les sauvegardes système complètes, mais pas les sauvegardes d'applications. Pour les sauvegardes système complètes, en cas de défaillance, le système de fichiers complet (y compris le SE) est restauré sur un matériel identique ou sur tout autre matériel si vos outils de restauration prennent en charge la restauration indépendante du matériel. On appelle jeu de sauvegarde la sauvegarde système complète de la plateforme de BI.
Jeu de sauvegarde	Un jeu de sauvegarde comprend ces sauvegardes individuelles créées au même moment : • une copie de sauvegarde de la base de données système du CMS ; • une sauvegarde système complète de l'ensemble du système de fichiers, y compris le système d'exploitation, de tous les ordinateurs du déploiement de la plateforme de BI ; • une copie de sauvegarde des stockages des fichiers de l'Input FRS et de l'Output FRS (s'ils ne sont pas inclus dans le système de fichiers de la plateforme de BI) ; • une copie de sauvegarde des composants de niveau Web (s'ils ne sont pas inclus dans le système de fichiers de la plateforme de BI) ; • une copie de sauvegarde de la base de données d'audit

Terme	Définition
Sauvegarde à froid et sauvegarde à chaud	Une sauvegarde à froid est effectuée lorsque le système est à l'arrêt et non accessible aux utilisateurs. Une sauvegarde à chaud est effectuée alors que le système est en cours d'exécution, accessible aux utilisateurs et que les données peuvent être modifiées pendant la sauvegarde. L'exécution d'une sauvegarde à chaud requiert de respecter l'ordre des étapes, ce qui n'est pas le cas pour une sauvegarde à froid. La plateforme de BI prend en charge les deux types de sauvegarde, à froid et à chaud. La sauvegarde à chaud est parfois appelée « sauvegarde en ligne ».

14.3 Cas d'utilisation de la sauvegarde et de la restauration

Le tableau suivant décrit les objectifs à atteindre au vu des ressources que vous pouvez posséder et vous oriente vers la solution de sauvegarde la plus appropriée.

Objectif	Ressources requises	Solution
Objectif : restaurer un système 1. Le système de ma plateforme de BI a été corrompu. Je dois donc le restaurer dans l'état de fonctionnement où il se trouvait avant la dernière sauvegarde. 2. Un ordinateur hébergeant la plateforme de BI a été endommagé. Je dois le remplacer par un nouvel ordinateur.	• Un système cible dont le matériel est identique au système source ET • Des sauvegardes du système source	Utilisez le workflow de sauvegarde et restauration système détaillé dans ce guide. Voir la procédure Sauvegarde du système entier [page 569]. Recréer le système cible à partir de sauvegardes du système source.
Objectif : restaurer des objets Je veux récupérer un document ou un autre objet supprimé accidentellement.	• Des sauvegardes des bases de données et fichiers du système source ET • Les informations système détaillées décrites dans Pour exporter depuis un système source [page 594]	A l'aide des sauvegardes, créez une copie du système sur un autre ordinateur à l'aide du workflow Copie du système décrit dans le chapitre « Copie du déploiement de la plateforme de BI ». Utilisez ensuite les outils de la Gestion des promotions pour promouvoir les outils supprimés par erreur à partir de ce nouveau système. Voir le workflow Copie du système en commençant par Planification de la copie du système [page 591] et suivez les instructions du reste du chapitre. **Remarque** Vous pouvez créer votre système cible sur un ordinateur comportant un déploiement existant de la

Objectif	Ressources requises	Solution
		plateforme de BI ayant la même version et le même niveau de Support Package et de correctif, ou sur un ordinateur "propre" sans installation de la platefoeme de BI.
Objectif : restaurer des objets 2 Je veux récupérer un document ou un autre objet supprimé accidentellement.	Un système où le versionnement de la Gestion des promotions est utilisé	Utilisez l'application Gestion des promotions pour récupérer une version antérieure du document. Pour en savoir plus, voir la rubrique associée sur la Gestion des promotions.

> **Remarque**
>
> **Sauvegarde du système avant et après une mise à niveau logicielle :**
>
> Le CMS est associé à la "version" d'un produit. Vous ne pouvez pas utiliser le système de plateforme SAP BusinessObjects Business Intelligence avec un CMS et un FRS appartenant à une version différente. Vous devez toujours sauvegarder le stockage de fichiers du CMS ainsi que du FRS avant et après toute mise à niveau logicielle. Si vous "restaurez" pour reprendre une mise à niveau logicielle, vous devez vous assurer que le CMS, le FRS et le logiciel appartiennent tous à la même version.

Informations associées

Sauvegardes [page 568]
Planification de la copie du système [page 591]
Présentation [page 602]

14.4 Sauvegardes

Un plan de sauvegarde et de récupération comprend des étapes à suivre en cas de panne du système due à une catastrophe naturelle ou une défaillance inattendue. Le plan vise à minimiser les effets du sinistre sur les opérations quotidiennes afin de pouvoir maintenir ou reprendre rapidement les fonctions stratégiques.

Lorsque vous sauvegardez votre déploiement de la plateforme de BI, vous disposez de trois options.

- Sauvegarder l'intégralité du système, ce qui permet de restaurer l'intégralité du système. Dans ce cas, il est impossible de ne restaurer qu'une partie du système. Pour recréer la plateforme de BI au lieu de la restaurer à partir d'une sauvegarde, voir la rubrique associée décrivant la copie du système.
- Sauvegarder les paramètres du serveur, ce qui permet de ne restaurer que les paramètres du serveur sans restaurer d'autres objets, préservant ainsi l'état actuel du contenu BI de votre système.
- Sauvegarder le contenu BI (par exemple, les documents), ce qui permet de restaurer les parties de votre choix du contenu BI sans devoir restaurer tous les objets.

Pour connaître les détails des trois types de sauvegarde, voir les rubriques associées.

> → Conseil
>
> Effectuez régulièrement des sauvegardes pour éviter de perdre des données.

> → Conseil
>
> Vous pouvez sauvegarder un système de plateforme de BI, puis le restaurer sur le même ordinateur hôte ou sur un autre afin de créer une copie du système.

Informations associées

Sauvegarde du système entier [page 569]
Sauvegarde des paramètres du serveur [page 572]
Sauvegarde du contenu BI [page 575]
Présentation de la copie du système [page 590]

14.4.1 Sauvegarde du système entier

Sauvegardez l'ensemble du système de la plateforme de BI en effectuant une sauvegarde à froid ou à chaud, ce qui crée un jeu de sauvegarde. Le fait de conserver plusieurs jeux de sauvegardes réalisés à différents moments vous offre davantage d'options lors de la restauration du système. Sauvegardez votre système aussi souvent que l'exigent les besoins de votre entreprise.

Vous pouvez choisir d'arrêter le système de votre plateforme de BI et d'effectuer une sauvegarde à froid ou effectuer une sauvegarde à chaud. Avec une sauvegarde à chaud, le système reste opérationnel et disponible pour les utilisateurs durant le processus de sauvegarde. L'avantage est de n'imposer aucun arrêt du système.

> ⓘ Remarque
>
> Il est recommandé d'écrire le journal de transactions dans un système de fichiers autre que le système du serveur de la base de données principale, de sauvegarder régulièrement ce journal de transactions et de le conserver avec les autres fichiers du jeu de sauvegarde.

> ⓘ Remarque
>
> Si vous sauvegardez des données d'audit, vérifiez que vous joignez le journal de transactions de la base de données d'audit au jeu de fichiers de sauvegarde. Il n'est pas nécessaire d'inclure les fichiers temporaires d'audit à la sauvegarde.

14.4.1.1 Sauvegardes à chaud

La fonctionnalité de sauvegarde à chaud permet de sauvegarder le système de votre plateforme de BI tout en permettant aux utilisateurs de continuer à utiliser le système normalement. Si votre activité doit continuer à

fonctionner pendant que votre système effectue la sauvegarde, activez et configurez les sauvegardes à chaud dans la Central Management Console.

Le paramètre *Durée maximale de la sauvegarde à chaud* indique le temps maximum que vous estimez nécessaire pour la sauvegarde, du démarrage de la sauvegarde du CMS jusqu'à la fin de sauvegarde FRS. Si la durée indiquée est trop courte, des fichiers peuvent être supprimés avant que la sauvegarde ait pu les copier. Pour éviter cela, il est plus sûr de surévaluer la durée requise. Équilibrez cette durée par rapport aux ressources système, parce qu'une valeur élevée peut augmenter légèrement la taille de votre stockage de fichiers FRS.

> **ⓘ Remarque**
>
> - Une sauvegarde à chaud n'effectue pas réellement une sauvegarde, elle ne fait que retarder la suppression des fichiers. Lorsque les fichiers sont modifiés ou mis à jour, plusieurs copies sont conservées. Cela signifie que le CMS et le FRS conservent toujours les bonnes relations, permettant la sauvegarde de chacun d'entre eux à des moments différents. Toutefois, cela se produit dans la fenêtre de sauvegarde à chaud.
> - Lorsque vous restaurez le système, le FRS peut finir par contenir de nombreux fichiers supplémentaires, que le Repository Diagnostic Tool doit supprimer.
> - Initiez toujours la sauvegarde du CMS avant la sauvegarde du stockage de fichiers FRS.
>
> La sauvegarde à chaud est activée tant que la case *Activer la sauvegarde à chaud* est cochée dans la CMC, le paramètre *Durée maximale de la sauvegarde à chaud* n'ayant aucune influence sur l'activation de la sauvegarde à chaud.

Le plus simple consiste à restaurer votre système à un moment de sauvegarde spécifique. Par exemple, si vos sauvegardes système sont effectuées quotidiennement à 3 h 00, vous pouvez restaurer facilement le système dans l'état où il était lorsque la sauvegarde du système du CMS a commencé (3 h 00 à la date de votre choix). Après une défaillance de la base de données du CMS ou de la base de données d'audit, si vous avez activé la journalisation des transactions sur celles-ci, vous pouvez restaurer le système dans l'état où il était immédiatement avant la défaillance.

Pour une sécurité maximale, stockez les enregistrements des journaux de transactions à un emplacement différent des enregistrements de sauvegarde de votre base de données principale. En cas de défaillance de la base de données, cela permet de pouvoir la restaurer dans l'état où elle était avant la défaillance.

> **ⓘ Remarque**
>
> En raison d'une limitation sur la taille des journaux de transactions sur les versions antérieures à IBM DB2, la sauvegarde à chaud et les tâches liées au journal des transactions sont prises en charge seulement si la base de données du système CMS est hébergée sur un serveur de base de données DB2 de version 9.5 Fix Pack 5 ou plus récent (pour la gamme 9.5) et 9.7 Fix Pack 1 ou plus récent (pour la gamme 9.7).

> **ⓘ Remarque**
>
> Il est recommandé d'écrire le journal de transactions dans un système de fichiers autre que le système du serveur de la base de données principale, de sauvegarder régulièrement ce journal de transactions et de le conserver avec les autres fichiers du jeu de sauvegarde.

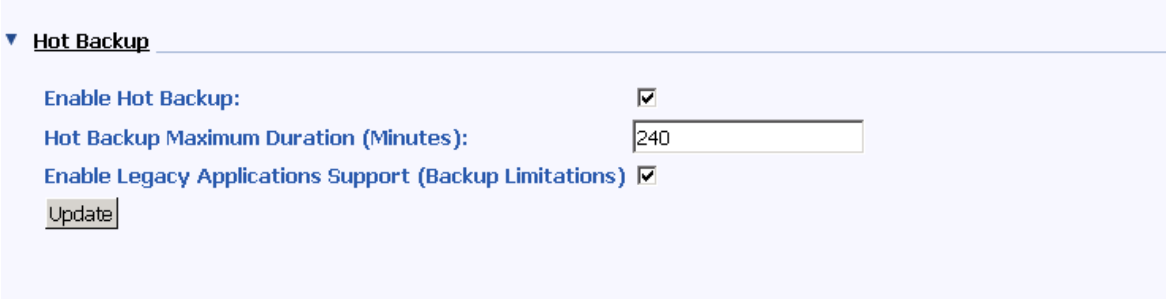
14.4.1.1.1 Activation des sauvegardes à chaud

1. Ouvrez la CMC (Central Management Console).
2. Dans le domaine *Gérer*, ouvrez la page *Paramètres*.
3. Dans la section *Sauvegarde à chaud*, sélectionnez *Activer la sauvegarde à chaud*.
4. Saisissez le nombre maximum de minutes que vous estimez nécessaires pour effectuer la sauvegarde sous *Durée maximale de la sauvegarde à chaud (en minutes)*.

   Assurez-vous d'avoir indiqué le moment souhaité pour la sauvegarde de la base de données du CMS et du système de fichiers de l'ordinateur hôte de la plateforme de BI.

   > **Remarque**
   >
   > Si la durée réelle de la sauvegarde dépasse la limite saisie à cet endroit, des incohérences pourraient survenir dans les données sauvegardées. Pour éviter cela, il est plus sûr de surévaluer la durée requise.

5. Cliquez sur *Mettre à jour*.
   La sauvegarde à chaud est activée.



Une fois que la prise en charge de la sauvegarde à chaud est activée, vous pouvez effectuer des sauvegardes à l'aide des outils de sauvegarde du fournisseur de votre base de données et de votre système de fichiers.

14.4.1.2 Pour exécuter une sauvegarde système à chaud ou à froid

Pour effectuer une sauvegarde à chaud, lisez d'abord la rubrique associée pour connaître les conditions préalables et d'autres informations. Si vous effectuez une sauvegarde à froid, arrêtez tous les nœuds de votre déploiement de la plateforme de BI.

> **Attention**
>
> Si vous effectuez une sauvegarde sans activer la sauvegarde à chaud ni arrêter tous les nœuds, des incohérences de données peuvent se produire entre la base de données du CMS et le stockage de fichiers du FRS.

> **Remarque**
>
> Pour les sauvegardes à chaud, il est important de démarrer les procédures dans l'ordre décrit. Pour les sauvegardes à froid, l'ordre des procédures n'a aucune importance. Dans les deux cas, il n'est pas nécessaire d'attendre la fin de chaque étape de sauvegarde avant de lancer la suivante.

1. Utilisez les outils de votre fournisseur de base de données pour sauvegarder la base de données système du CMS (Central Management Server).

   > **Remarque**
   >
   > Pour les sauvegardes à chaud, utilisez les outils de sauvegarde du fournisseur de base de données en mode atomique connecté.

2. Utilisez les outils de votre fournisseur de base de données en mode atomique connecté pour sauvegarder la base de données d'audit de la plateforme de BI.
3. Sauvegardez l'ensemble du système de fichiers, y compris le système d'exploitation, de tous les ordinateurs du déploiement de la plateforme de BI. Sur les ordinateurs Unix, sauvegardez le répertoire d'installation et répertoire d'accueil du compte d'installation.
   a. Si les emplacements de stockage de fichiers de l'Input File Repository Server et de l'Output File Repository Server ne sont pas inclus dans la sauvegarde de la plateforme de BI (ordinateurs hôte séparés), créez-en une copie de sauvegarde à l'aide de vos outils de sauvegarde de fichiers.
   b. Si les composants de niveau Web ne sont pas inclus dans la sauvegarde de la plateforme de BI (ordinateurs hôte séparés), créez-en une copie de sauvegarde à l'aide de vos outils de sauvegarde de fichiers.

   Dans le cas des sauvegardes à chaud, utilisez les outils de sauvegarde de fichiers atomiques dans la mesure du possible.

Si vous avez effectué une sauvegarde à froid, patientez jusqu'à ce que toutes les sauvegardes soient terminées, puis démarrez les nœuds de la plateforme de BI.

Informations associées

Sauvegardes à chaud [page 569]

14.4.2 Sauvegarde des paramètres du serveur

Pour protéger le système d'une configuration inappropriée des paramètres de serveur, sauvegardez-les régulièrement dans un fichier BIAR. Le fait de disposer de sauvegardes de vos serveurs permet de restaurer les paramètres sans avoir à restaurer la base de données système du CMS (Central Management Server), les référentiels de fichiers ou le contenu Business Intelligence.

Il est indispensable de sauvegarder les paramètres du serveur à chaque modification apportée au déploiement du système. Cela inclut la création, le changement de nom, le déplacement et la suppression de nœuds, ainsi que la création et la suppression de serveurs. Il est recommandé de sauvegarder les paramètres du serveur avant toute modification desdits paramètres, puis une fois les modifications effectuées.

> **Remarque**
>
> Sauvegarder les paramètres du serveur n'est pas une tâche supplémentaire à la sauvegarde du stockage de fichiers CMS et FRS ; par exemple, la restauration du CMS/FRS restaure également les paramètres du serveur. La sauvegarde des paramètres du serveur est un petit sous-ensemble d'une sauvegarde complète

de la base de données CMS. Il n'est pas nécessaire que vous restauriez les paramètres du serveur si vous avez déjà restauré le CMS.

Utilisez le CCM (Central Configuration Manager) ou un script pour sauvegarder les paramètres du serveur de la plateforme de BI dans un fichier BIAR, puis stockez le fichier dans un ordinateur distinct ou sur un support de stockage.

> **Remarque**
>
> Si vous sauvegardez ou restaurez les paramètres de serveur dans un déploiement où SSL est activé, vous devez d'abord désactiver SSL par le biais de la CCM, puis le réactiver après avoir terminé la sauvegarde ou la restauration.

Sous Windows, le script `BackupCluster.bat` se trouve dans le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Sous UNIX, le script `backupcluster.sh` se trouve dans le répertoire `/<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme64>/scripts`.

14.4.2.1 Pour sauvegarder les paramètres du serveur à l'aide du CCM sous Windows

Cette procédure permet de sauvegarder les paramètres de serveur pour l'ensemble du cluster. Il n'est pas possible de sauvegarder les paramètres de serveurs individuels.

> **Remarque**
>
> Si vous utilisez un CMS temporaire, vous devez utiliser le CCM sur un ordinateur où sont installés des fichiers binaires CMS.

1. Démarrez le CCM, puis, dans la barre d'outils, cliquez sur *Sauvegarder la configuration du serveur*. L'*Assistant de sauvegarde de la configuration du serveur* apparaît.
2. Cliquez sur *Suivant* pour lancer l'Assistant.
3. Spécifiez s'il faut utiliser un CMS existant pour sauvegarder les paramètres de configuration du serveur ou créer un CMS temporaire.
   - Pour sauvegarder les paramètres de serveur d'un système en cours d'exécution, sélectionnez *Utiliser le CMS existant en cours d'exécution*, puis cliquez sur *Suivant*.
   - Pour sauvegarder les paramètres de serveur d'un système qui n'est pas en cours d'exécution, sélectionnez *Démarrer un nouveau CMS temporaire*, puis cliquez sur *Suivant*.
4. Si vous utilisez un CMS temporaire, sélectionnez un numéro de port sur lequel exécuter le CMS et spécifiez les informations de connexion à la base de données.

   Pour minimiser le risque d'utilisateurs accédant à votre système pendant sa restauration, spécifiez un numéro de port différent des numéros de port qu'utilise votre CMS existant.
5. Saisissez une clé de cluster, puis cliquez sur *Suivant* pour continuer.
6. A l'invite, connectez-vous au CMS en indiquant le système ainsi que le nom d'utilisateur et le mot de passe d'un compte ayant des droits d'administrateur, puis cliquez sur *Suivant* pour continuer.

7. Indiquez l'emplacement et le nom du fichier BIAR dans lequel vous souhaitez sauvegarder les paramètres de configuration du serveur, puis cliquez sur *Suivant* pour continuer.
   La page *Confirmation* affiche les informations que vous avez fournies.
8. Vérifiez que les informations affichées dans la page *Confirmation* sont correctes, puis cliquez sur *Terminer* pour continuer.
   Le CCM sauvegarde les paramètres de configuration du serveur pour l'ensemble du cluster dans le fichier BIAR que vous avez indiqué. Les détails de la procédure de sauvegarde sont consignés dans un fichier journal. Le nom et le chemin du fichier journal sont affichés dans une boîte de dialogue.
9. Si l'opération de sauvegarde a échoué, consultez le fichier journal pour en déterminer la raison.
10. Cliquez sur *OK* pour fermer l'assistant.

14.4.2.2 Pour sauvegarder des paramètres de serveur sous UNIX

Sous UNIX, utilisez le script `serverconfig.sh` pour sauvegarder les paramètres de serveur du déploiement dans un fichier BIAR.

1. Sélectionnez *5 - Sauvegarder la configuration du serveur* et appuyez sur `Entrée`.

```
-----------------------------------------------------------

           SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]5
```

2. Spécifiez s'il faut utiliser un CMS existant pour sauvegarder les paramètres de configuration du serveur ou créer un CMS temporaire.
   - Pour sauvegarder les paramètres de serveur d'un système en cours d'exécution, sélectionnez *existant* et appuyez sur `Entrée`.
   - Pour sauvegarder les paramètres de serveur d'un système qui n'est pas en cours d'exécution, sélectionnez *temporaire* et appuyez sur `Entrée`.
3. Si vous utilisez un CMS temporaire pour sauvegarder les paramètres de votre serveur, dans les écrans suivants, sélectionnez un numéro de port sur lequel exécuter le CMS temporaire et les informations de connexion à la base de données système du CMS.

Pour minimiser le risque d'utilisateurs accédant à votre système pendant sa restauration, spécifiez un numéro de port différent des numéros de port qu'utilise votre CMS existant.

4. A l'invite, connectez-vous au CMS en spécifiant le nom de système et d'utilisateur ainsi que le mot de passe d'un compte ayant des droits d'administrateur, puis cliquez sur `Entrée`.
5. A l'invite, spécifiez l'emplacement et le nom d'un fichier BIAR dans lequel sauvegarder les paramètres de configuration du serveur et appuyez sur `Entrée`.
   Une page de synthèse affiche les informations fournies.
6. Vérifiez que les informations affichées sont correctes, puis appuyez sur `Entrée` pour continuer.
   Le script `serverconfig.sh` sauvegarde les paramètres de configuration du serveur pour tout le cluster dans le fichier BIAR que vous spécifiez. Les détails de la procédure de sauvegarde sont consignés dans un fichier journal. Le nom et le chemin du fichier journal sont affichés.
7. Si l'opération de sauvegarde a échoué, consultez le fichier journal pour en déterminer la raison.

14.4.2.3 Pour sauvegarder les paramètres de serveur avec un script

Vous pouvez sauvegarder les paramètres de serveur de votre déploiement en exécutant le fichier `BackupCluster.bat` sous Windows ou le script `backupcluster.sh` sous Unix.

Sous Windows, le fichier `BackupCluster.bat` se trouve dans le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Sous UNIX, le fichier `backupcluster.sh` se trouve dans le répertoire `/<REPINSTALL>/sap_bobj/enterprise_xi40/<platforme64>/scripts`.

Informations associées

Scripts BackupCluster et RestoreCluster [page 586]

14.4.3 Sauvegarde du contenu BI

Il est recommandé d'utiliser des outils et des procédures standard de sauvegarde de bases de données et de fichiers pour sauvegarder régulièrement :

- La base de données du CMS.
- Les fichiers de stockage Input FRS et Output FRS.

Des sauvegardes régulières du contenu permettent une restauration de Business Intelligence sans avoir à restaurer tout le système ni tous les paramètres du serveur.

Pour en savoir plus sur la sauvegarde de votre système, voir Pour exécuter une sauvegarde système à chaud ou à froid [page 571].

14.5 Restauration du système

Si votre système est endommagé ou corrompu, vous pouvez restaurer le système complet, ce qui restaure la plateforme de BI. Selon l'état du système, il se peut qu'une restauration complète ne soit pas nécessaire. Si le système fonctionne normalement, mais que le contenu est corrompu ou perdu, vous pouvez choisir de ne restaurer que le contenu Business Intelligence (BI). Si le contenu BI est valide, mais que les serveurs de votre plateforme ne sont plus correctement configurés, vous pouvez ne restaurer que les paramètres de serveur.

La procédure est identique pour une restauration à partir d'une sauvegarde à chaud ou à froid.

Informations associées

Restauration de votre système entier [page 576]
Restauration des paramètres de serveur [page 583]
Restauration du contenu BI [page 586]

14.5.1 Restauration de votre système entier

Lorsque vous restaurez le système complet, le cluster de la plateforme de BI est également restauré. Selon l'élément du système ayant connu une défaillance, vous pouvez éventuellement n'avoir à effectuer qu'une restauration partielle.

Si l'un des composants suivants est défaillant ou perdu, vous devez restaurer le système complet.

- Base de données CMS

  > **Remarque**
  >
  > En cas de défaillance du service de base de données, vous pouvez redémarrer le service sans restaurer le système entier.

- Stockage de fichiers du FRS
- Système de fichiers de l'ordinateur

> **Remarque**
>
> Pour une restauration complète, il n'est pas indispensable que la plateforme de BI soit déjà installée sur le système cible.

Si seule la base de données d'audit est corrompue ou perdue, vous pouvez la restaurer sans avoir à restaurer le système complet.

Si le contenu de niveau Web est corrompu ou perdu, vous pouvez le restaurer sans avoir à restaurer le système complet.

Informations associées

Pour restaurer votre système entier [page 577]
Restauration de la base de données d'audit uniquement [page 579]
Pour restaurer le contenu de niveau Web [page 579]
Pour restaurer la base de données du CMS uniquement [page 580]

14.5.1.1 Pour restaurer votre système entier

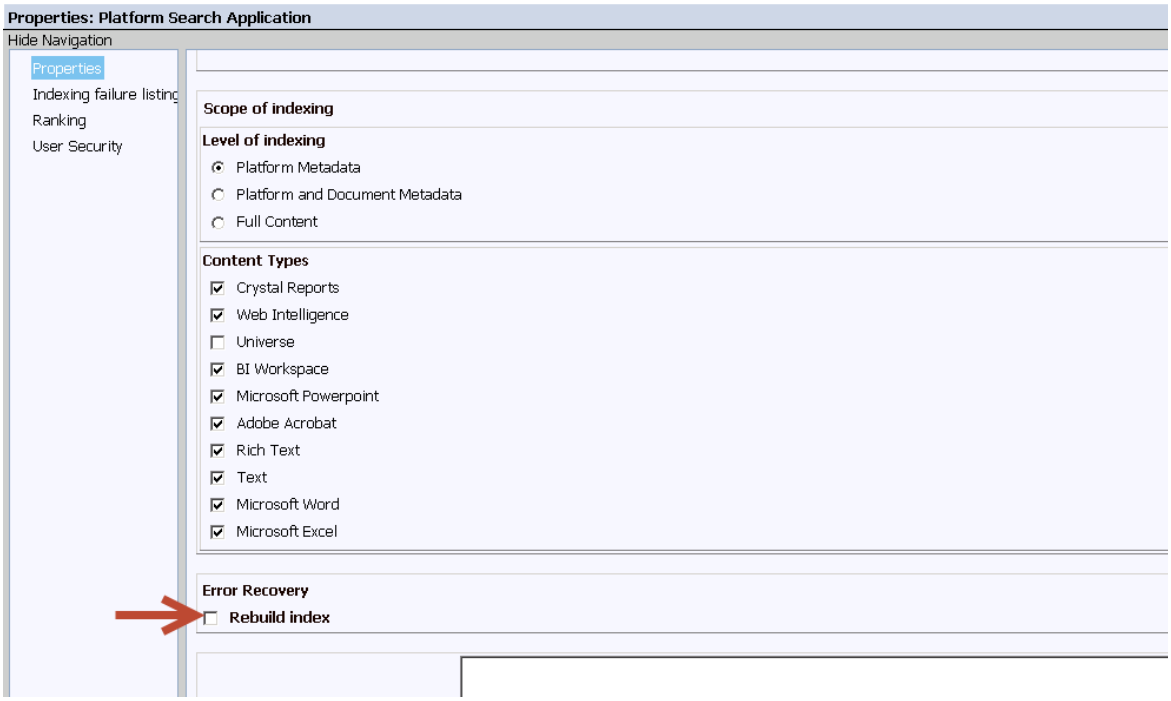
Avant de restaurer votre système, vous devez utiliser le CCM (Central Configuration Manager) pour arrêter tous les nœuds du déploiement de la plateforme de BI et vous devez choisir l'heure à laquelle vous voulez restaurer le système.

> **Remarque**
>
> Si vous voulez restaurer le système à son état actuel, sauvegardez-le avant de le restaurer.

1. Recherchez les fichiers de sauvegarde suivants :
   - Sauvegarde de la base de données du CMS
   - Sauvegardes du stockage de fichiers de l'Input FRS et de l'Output FRS
   - Sauvegardes des systèmes de fichiers de chaque ordinateur hôte du cluster de la plateforme de BI

   > **Remarque**
   >
   > - Veillez à valider les sauvegardes et assurez-vous que tous les fichiers répertoriés ci-dessus font partie du même jeu de sauvegardes.
   > - Lorsque vous effectuez une sauvegarde et une restauration, le CMS et le FRS sont traités comme une seule et même unité. Si vous restaurez l'un, vous devez restaurer l'autre en même temps.
   > - Si le jeu de sauvegarde provient d'une sauvegarde à chaud, vérifiez que l'horodatage de début de la sauvegarde de la base de données du CMS est antérieur à celui du stockage des fichiers FRS, du niveau Web et du système de fichiers de l'ordinateur hôte correspondants. Tous ces fichiers seront nécessaires, même si un seule composant est en panne.
2. Utilisez les outils de restauration de fichiers pour restaurer le système de fichiers de tous les ordinateurs hôte du cluster de la plateforme de BI.
3. Utilisez les outils de restauration de fichiers pour restaurer les stockages de fichiers de l'Input et de l'Output FRS.
4. Utilisez les outils de base de données pour restaurer la base de données du CMS.
5. Si vous avez modifié le mot de passe de la base de données du CMS depuis la création de la copie de sauvegarde, utilisez le CCM pour mettre à jour le mot de passe de la base de données du CMS sur tous les nœuds et ordinateurs hôte de la plateforme de BI.
6. Si vous utilisez la fonctionnalité d'audit, utilisez les outils de base de données pour restaurer la base de données d'audit.
7. Choisissez l'une des options suivantes pour restaurer votre index de recherche :

- Pour exécuter un script de récupération d'index de recherche, reportez-vous à Pour exécuter le script de récupération d'index de recherche [page 582] et suivez-en les instructions. Cela vous fournira un index complet plus rapidement.
- Pour recréer votre index de recherche au lieu d'utiliser le script de récupération, utilisez le CCM afin de redémarrer les nœuds de votre plateforme de BI. Il s'agit là d'une procédure plus simple mais, tant que l'index sera en cours de régénération, vous n'aurez qu'un accès en recherche partiel aux données de la plateforme.



8. Démarrez le système et notez l'heure pour l'utiliser au cours des étapes requises suivantes.
9. Vérifiez que votre système fonctionne comme escompté et effectuez un test de validité.

Une fois le système vérifié, effectuez les actions suivantes :

- Exécutez le Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel) pour supprimer tous les fichiers temporaires non utilisés et vérifiez la cohérence du référentiel. Voir la section Outil de diagnostic de référentiel de ce guide.
- Si vous n'avez pas utilisé le script de récupération d'index, recréez l'index de recherche de votre plateforme.
- Les travaux de publication en cours au moment de la sauvegarde du système s'afficheront comme ayant échoué. Ne réexécutez pas ces instances, démarrez de nouveaux travaux de publication.
- Si votre base de données d'audit a été restaurée, vous devez exécuter une requête SQL pour supprimer tout événement survenant entre la défaillance de la base de données et l'heure de redémarrage (l'heure dont vous avez pris note à l'étape 8). Par exemple : `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

Informations associées

Indexation de contenu dans le référentiel CMS [page 966]

14.5.1.2 Restauration de la base de données d'audit uniquement

Avant de restaurer votre base de données d'audit, utilisez le CCM (Central Configuration Manager) pour arrêter tous les nœuds du déploiement de la plateforme de BI. Vous devez également choisir à quel moment vous souhaitez restaurer la base de données.

> **Remarque**
>
> Effectuez cette tâche uniquement si vous êtes sûr que la base de données d'audit est le seul composant compromis de la plateforme de BI. Si d'autres composants sont concernés, vous devez effectuer une restauration du système complet.

Utilisez les outils de base de données pour restaurer la base de données d'audit.

Informations associées

Pour restaurer votre système entier [page 577]

14.5.1.3 Pour restaurer le contenu de niveau Web

Avant de restaurer le contenu du niveau Web, vous devez arrêter tous les nœuds de votre déploiement de la plateforme de BI à l'aide du CCM (Central Configuration Manager). Vous devez également décider à quel moment vous souhaitez restaurer le contenu du niveau Web.

Pour avoir la possibilité de revenir à l'état actuel du système, vous devez effectuer une sauvegarde du système avant de le restaurer.

Si le niveau Web est corrompu, il peut être restauré individuellement.

1. Utilisez les outils de restauration de fichiers pour restaurer les dossiers de niveau Web sur l'ordinateur hôte de niveau Web.
2. Utilisez le CCM pour redémarrer tous les nœuds du déploiement de la plateforme de BI.

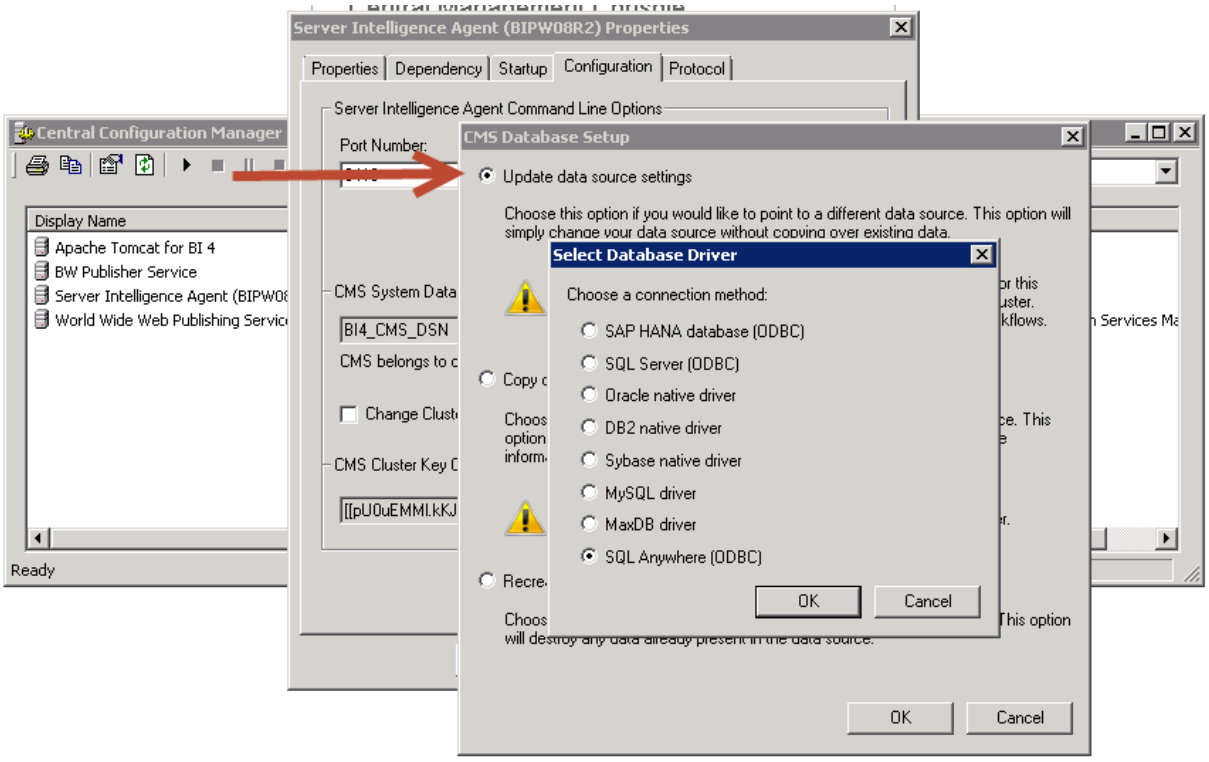
14.5.1.4 Pour restaurer la base de données du CMS uniquement

> **Remarque**
>
> En cas de défaillance du service de base de données, vous pouvez redémarrer le service sans restaurer le système entier. Si la base de données est corrompue ou que d'autres composants ont été compromis, vous devez effectuer une restauration complète du système.

Réparez ou remplacez l'ordinateur hôte de la base de données du CMS. Si vous le remplacez, assurez-vous qu'il a le même nom de système que l'ordinateur hôte précédent ainsi que les mêmes paramètres de port et références de connexion à la base de données.

> **Remarque**
>
> S'il n'est pas possible de restaurer l'ordinateur à l'aide du même nom et des mêmes références de connexion, vous devrez utiliser le CCM (Central Configuration Manager) pour mettre à jour ces informations de connexion à la base de données pour chaque nœud du cluster et redémarrer ces nœuds.

Sous Windows :



Sous UNIX : Exécutez cmsdbsetup.sh, entrez le nom du nœud à l'invite, puis sélectionnez l'option 6 `update`.

```
-----------------------------------------------------------

           SAP BusinessObjects


Current CMS Data Source: BI4_CMS_DSN_1381344842

Current cluster name: LRHEL57x64:6400

Current cluster key: [[pU0uEMMl.kKJPezTK002bw]]


update (Update Data Source Settings)
reinitialize (Recreate the current data surce)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)


[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-----------------------------------------------------------

[update]6
```

1. Arrêtez tous les nœuds de la plateforme de BI à l'aide du CCM.
2. Utilisez les outils de base de données pour restaurer la base de données d'audit.
3. Utilisez le CCM pour démarrer les nœuds de la plateforme de BI.

Une fois que vous avez vérifié que le système fonctionne correctement, effectuez les actions suivantes :

- Exécutez le Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel) pour supprimer tous les fichiers temporaires non utilisés et vérifiez la cohérence du référentiel. Voir la section Outil de diagnostic de référentiel de ce guide.
- Les travaux de publication en cours au moment de la sauvegarde du système s'afficheront comme ayant échoué. Ne réexécutez pas ces instances, démarrez de nouveaux travaux de publication.

Informations associées

Indexation de contenu dans le référentiel CMS [page 966]

14.5.1.5 Récupération d'index de recherche

La fonctionnalité de recherche de plateformes gère une variété de fichiers d'index et d'informations à travers le système afin de l'aider à effectuer plus efficacement ses recherches. S'il est nécessaire de restaurer le système, il se peut que ces fichiers d'informations développent des incohérences. Vous pouvez réparer ces incohérences à l'aide du script de récupération d'index ou en recréant l'index.

La recréation de l'index est une procédure simple mais le processus fait appel à des ressources considérables, son achèvement prend du temps et les recherches effectuées durant la recréation ne renverront de résultats que pour les parties indexées de la base de données. Le script de récupération implique une procédure plus complexe mais vous procurera plus rapidement un index entièrement fonctionnel.

Si vous restaurez un déploiement comportant plusieurs ordinateurs, exécutez le script sur un ordinateur hébergeant le service de recherche. Pour le premier ordinateur d'un cluster, utilisez l'option `-Both`, puis sur tous les ordinateurs suivants de ce cluster, utilisez l'option `-ContentStore`.

Informations associées

Indexation de contenu dans le référentiel CMS [page 966]

14.5.1.5.1 Pour exécuter le script de récupération d'index de recherche

- Vérifiez que le CMS fonctionne et arrêtez tous les serveurs de traitement adaptatif (APS) où est installé le Service de recherche.

  > **Remarque**
  >
  > Vous devez arrêter ces serveurs de traitement adaptatif aussi vite que possible après le démarrage du nœud.

- Définissez également `JAVA-HOME` sur l'emplacement `sapjvm/bin` du répertoire d'installation de la plateforme de BI.
- Le répertoire de données de la recherche de plateformes est accessible à partir de l'ordinateur où est exécuté le script.

1. Sur l'ordinateur hôte du CMS ou de l'APS, ouvrez une fenêtre de ligne de commande (si vous utilisez un système d'exploitation Windows).
2. Passez au répertoire suivant : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib\`.

   Les ordinateurs UNIX utilisent le chemin de fichier UNIX équivalent.
3. Saisissez `java -jar platformSearchOnlineHotbackupRestore.jar` et appuyez sur la touche *Entrée*.
4. Lorsque vous y êtes invité, saisissez les informations suivantes, puis appuyez sur *Entrée* :
   - L'emplacement de votre plateforme de BI (par exemple, `<REPINSTALL>/SAP businessObjects Enterprise XI 4.0`)
   - Vos références de connexion au CMS, notamment le nom du CMS, l'ID et le mot de passe utilisateur ainsi que le type d'authentification. Le type d'authentification présente les options suivantes :
     - `secEnterprise`
     - `secLDAP`
     - `secWinAD`
     - `secSAPR3`
5. Lorsque le type de restauration d'index vous est demandé, saisissez l'une des options suivantes et appuyez sur *Entrée*.

Valeur	Description
`-Both`	Cette valeur est destinée aux déploiements à serveur unique ou, en déploiements à plusieurs ordinateurs, au premier ordinateur hôte de serveur de traitement adaptatif comportant le service de recherche : Sur un système comportant plusieurs serveurs de traitement adaptatif de recherche, lors de la première exécution du script, utilisez la valeur `-Both` (mise à jour de la base de données et du stockage de contenu. Quand le script est exécuté pour tous les autres serveurs de traitement adaptatif de recherche, utilisez la valeur `-ContentStore` (mise à jour du stockage de contenu uniquement).
`-ContentStore`	Cette valeur doit être utilisée lors de l'exécution du script sur les ordinateurs hôte d'APS où est installé le service de recherche, à moins qu'il ne s'agisse du premier ordinateur du cluster où s'exécute le script.
`-Exit`	Permet de quitter le script sans effectuer de restauration d'index.

6. Lorsque le script a fini son exécution, fermez la fenêtre de ligne de commande (pour les ordinateurs Windows).

Démarrez tous les APS arrêtés.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\java\lib>java  -jar platformsearchOnlineHotbackupRestore.jar
Enter the BOE install location :
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0

Enter the CMS Credentials:
CMS NAME: BIPW08R2
USER NAME: Administrator
PASSWORD:
AUTHENTICATION: secEnterprise
BOE Install Location = C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessOb
jects Enterprise XI 4.0 CMS = BIPW08R2  User = Administrator    Authentication =
 secEnterprise

Please verify if the details given above are correct(y/n)...Press 'e' if you wan
t to exit  :y
 What would you like to restore?
 1. Index ?
 2. Content Store ?
 3. Both Index and Content Store (Choose this option only when index and content
 store are present on one node) ?
 4. Exit ?
3_
```

14.5.2 Restauration des paramètres de serveur

Pour restaurer les paramètres de serveur de votre système depuis un fichier BIAR, vous pouvez utiliser le CCM (Central Configuration Manager) ou le script RestaurerCluster. La restauration du contenu des serveurs depuis un fichier BIAR n'affecte pas le contenu Business Intelligence tel que les rapports, les utilisateurs et les groupes ou les paramètres de sécurité.

> **Remarque**
>
> Lors de la restauration des paramètres de serveur, seule la restauration des paramètres de l'ensemble d'un cluster est prise en charge. Il n'est pas possible de restaurer les paramètres de certains serveurs du cluster uniquement.

> **Remarque**
>
> Si vous sauvegardez ou restaurez les paramètres de serveur dans un déploiement où SSL est activé, vous devez d'abord désactiver SSL par le biais de la CCM, puis le réactiver après avoir terminé la sauvegarde ou la restauration.

14.5.2.1 Restauration des paramètres de serveur à l'aide du CCM sous Windows

Vous pouvez utiliser le CCM (Central Configuration Manager) pour restaurer les paramètres de serveur. Une fois les paramètres restaurés, vous devez recréer les nœuds de votre système sur chaque ordinateur du cluster.

1. Arrêtez tous les nœuds de tous les ordinateurs du cluster pour lesquels vous restaurez les paramètres de configuration du serveur en arrêtant le Server Intelligence Agent de chaque nœud.
2. Démarrez le CCM sur un ordinateur hébergeant un CMS.
3. Dans la barre d'outils, cliquez sur *Restaurer la configuration du serveur*.
   L'*Assistant de restauration de la configuration du serveur* apparaît.
4. Cliquez sur *Suivant* pour lancer l'Assistant.
5. A l'invite, indiquez le numéro de port du CMS (Central Management Server) temporaire à utiliser et les informations requises pour la connexion à la base de données système du CMS, puis cliquez sur *Suivant* pour continuer.
6. Saisissez une clé de cluster, puis cliquez sur *Suivant* pour continuer.
7. A l'invite, connectez-vous au CMS en entrant le nom du CMS ainsi que le nom d'utilisateur et le mot de passe d'un compte ayant des droits d'administrateur, puis cliquez sur *Suivant* pour continuer.
8. Indiquez l'emplacement et le nom du fichier BIAR contenant les paramètres de configuration du serveur à restaurer, puis cliquez sur *Suivant* pour continuer.
   Une page de résumé affiche le contenu du fichier BIAR.
9. Cliquez sur *Suivant* pour continuer.
   Une page de résumé affiche le contenu des informations saisies.
10. Cliquez sur *Terminer* pour continuer.
    Un message d'avertissement indique que les paramètres de serveur existants seront remplacés par les valeurs du fichier BIAR et qu'en continuant, les paramètres de serveur actuels seront perdus.
11. Cliquez sur *Oui* pour restaurer les paramètres de configuration du serveur.

    Le CCM restaure les paramètres de configuration du serveur pour l'ensemble du cluster dans le fichier BIAR. Les détails de la restauration sont consignés dans un fichier journal. Le nom et le chemin du fichier journal s'affichent dans une boîte de dialogue.
12. Si l'opération de restauration a échoué, consultez le fichier journal pour en déterminer la raison.
13. Cliquez sur *OK* pour fermer l'assistant.

Les paramètres de serveur du fichier BIAR sot restaurés dans votre système. Les nœuds et les serveurs du fichier BIAR qui n'existaient pas dans le système avant la restauration sont créés.

> **Remarque**
>
> Les nœuds et les serveurs qui existaient dans le système, mais pas dans le fichier BIAR, sont supprimés du référentiel. Les nœuds et les serveurs s'affichent toujours dans le CCM, mais vous pouvez supprimer manuellement les fichiers `dbinfo` et `bootstrap` d'un nœud.

Vous devez recréer les nœuds de votre système sur chaque ordinateur du cluster.

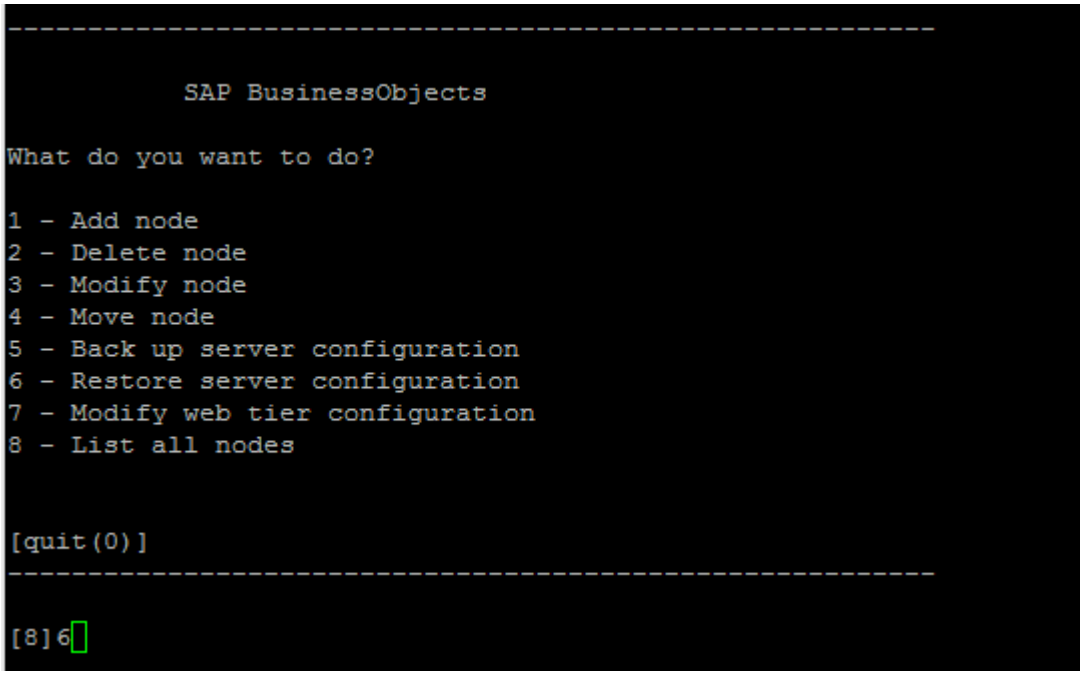
Informations associées

Utilisation des nœuds [page 480]

14.5.2.2 Pour restaurer les paramètres de serveur sous UNIX

Sur les ordinateurs UNIX, utilisez le script `serverconfig.sh` pour restaurer les paramètres de serveur du déploiement à partir d'un fichier BIAR.

1. Sélectionnez *6 : Restaurer la configuration du serveur* et appuyez sur `Entrée`.



2. Saisissez un numéro de port pour le CMS (Central Management Server) temporaire à utiliser et appuyez sur `Entrée`.
3. Dans les écrans suivants, spécifiez les informations de connexion à la base de données système du CMS.
4. A l'invite, connectez-vous au CMS en spécifiant le nom de système et d'utilisateur ainsi que le mot de passe d'un compte ayant des droits d'administrateur, puis cliquez sur `Entrée`.
5. A l'invite, spécifiez l'emplacement et le nom d'un fichier BIAR à partir duquel restaurer les paramètres de configuration du serveur et appuyez sur `Entrée`.

Un écran de synthèse affiche les informations fournies.

6. Vérifiez que les informations figurant à l'écran sont correctes, puis appuyez sur *Entrée* pour continuer. Le script `serverconfig.sh` restaure les paramètres de configuration du serveur pour tout le cluster à partir du fichier BIAR que vous spécifiez. Les détails de la procédure de restauration sont écrits dans le fichier journal. Le nom et le chemin du fichier journal figurent à l'écran.
7. Si l'opération de restauration a échoué, consultez le fichier journal pour en déterminer la raison.

14.5.2.3 Pour restaurer les paramètres de serveur avec un script

Si vous préférez, vous pouvez restaurer les paramètres de serveur de votre déploiement en exécutant le script `RestoreCluster.bat` sous Windows ou le script `restorecluster.sh` sous UNIX.

Sous Windows, le fichier `RestoreCluster.bat` se trouve dans le répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

Sous Unix, le fichier `restorecluster.sh` se trouve dans le répertoire `/<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATFORME64>/scripts`.

Informations associées

Scripts BackupCluster et RestoreCluster [page 586]

14.5.3 Restauration du contenu BI

Si vous avez sauvegardé le contenu Business Intelligence (BI) dans des fichiers LCMBIAR, vous pouvez utiliser l'outil de gestion des promotions pour restaurer le contenu BI et non votre système complet. Pour en savoir plus, voir le chapitre « Gestion des promotions ».

14.6 Scripts BackupCluster et RestoreCluster

Le tableau suivant décrit les paramètres de commande de ligne utilisés avec le script `BackupCluster`.

> **Remarque**
>
> Ce script sauvegarde uniquement les paramètres de serveur d'un cluster. Les autres données doivent être sauvegardées séparément.

Paramètres BackupCluster

Nom	Description	Exemple
`-backup`	Nom et chemin du fichier BIAR devant sauvegarder les paramètres de serveur de votre système à restaurer.	`-backup "C:\Users\Administrator\Desktop\my.biar"`
`-cms`	Nom d'hôte de l'ordinateur sur lequel se trouve le Central Management Server de votre système. Si votre CMS s'exécute sur un autre port que le port par défaut, 6400, vous devez également spécifier le numéro de port.	`-cms mycms:6400`
`-username`	Nom d'utilisateur d'un compte administrateur.	`-username Administrator`
`-password`	Mot de passe d'un compte administrateur.	`-password MotDePasse1`

Le tableau suivant décrit les paramètres de commande de ligne utilisés avec le script `RestoreCluster`.

Paramètres RestoreCluster

Nom	Description	Exemple
`-restore`	Nom et chemin du fichier BIAR contenant les paramètres de configuration de serveur à restaurer.	`-restore "C:\Users\Administrator\Desktop\my.biar"`
`-username`	Nom d'utilisateur d'un compte administrateur.	`-username Administrator`
`-password`	Mot de passe d'un compte administrateur.	`-password MotDePasse1`
`-displaycontents`	Affiche une liste des nœuds et serveurs que contient le fichier BIAR.	`-displaycontents "C:\Users\Administrator\Desktop\my.biar"`

> **Remarque**
>
> Exécutez le script `RestoreCluster` avec le paramètre `-displaycontents` pour afficher le contenu du fichier BIAR avant de restaurer les paramètres de serveur.

Les paramètres suivants sont nécessaires si vous sauvegardez les paramètres de serveur d'un système qui n'est pas en cours d'exécution ou si vous restaurez des paramètres de serveur.

Paramètres utilisés lors de l'utilisation d'un CMS temporaire

Nom	Description	Exemple
`-usetempcms`	Crée un CMS temporaire pour l'opération spécifiée. Une fois l'opération terminée, le CMS temporaire est arrêté.	`-usetempcms`
`-cmsport`	Numéro de port du CMS temporaire.	`-cmsport 6700`

Nom	Description	Exemple
`-dbdriver`	Pilote de la base de données système du CMS. Les valeurs acceptées sont les suivantes : • **`db2databasesubsystem`** • **`maxdbdatabasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`newdbdatabasesubsystem`** **Remarque** Le paramètre **`newdbdatabasesubsystem`** est destiné à être utilisé avec les bases de données SAP HANA.	**`-dbdriver sqlserverdatabasesubsystem`**
`-connect`	Chaîne de connexion de la base de données système du CMS.	**`-connect "DSN=BusinessObjects CMS 1;UID=nom_utilisateur;PWD=mot_de_passe;HOSTNAME=base_de_données;PORT=3306"`**
`-dbkey`	Clé du cluster.	**`-dbkey abc1234`**

Exemple

L'exemple suivant illustre comment sauvegarder vos paramètres de serveur dans un fichier BIAR à l'aide d'un CMS existant.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Exemple

L'exemple suivant illustre comment afficher le contenu d'un fichier BIAR.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Exemple

L'exemple suivant illustre comment restaurer vos paramètres depuis un fichier BIAR. Vous devez toujours utiliser un CMS temporaire lors de la restauration de paramètres de serveur.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```

15 Copie de votre déploiement de la plateforme de BI

15.1 Présentation de la copie du système

ce chapitre décrit la méthode de création d'une copie du déploiement de votre plateforme de BI à des fins de tests, mise en veille ou autre.

Pour en savoir plus, voir 1275068.

Informations associées

Présentation de la sauvegarde et de la restauration [page 565]

15.2 Terminologie

Terme	Définition
Système source	Déploiement d'origine de la plateforme de BI.
Système cible	Nouveau déploiement à créer.
Copie du système	Acte de création d'un double de déploiement de la plateforme de BI existant.
Copie du système homogène	Création d'un double du système où les systèmes source et cible ont le même type de système d'exploitation et de base de données. La plateforme de BI prend en charge uniquement la copie du système homogène.
Copie du système hétérogène	Création d'un double du système où les systèmes source et cible ont des types de système d'exploitation et de base de données différents mais sont basés sur les mêmes données.
Copie de base de données	Création d'un double de la base de données système ou d'audit du CMS à l'aide des outils du fournisseur de contenus de la base de données.

15.3 Cas d'utilisation de la copie du système

Le tableau suivant décrit les objectifs à atteindre au vu des ressources que vous pouvez posséder et vous oriente vers la solution la plus appropriée.

Objectif	Ressources requises	Solution
Objectif : copie identique Je désire créer à des fins de mise en veille ou de test un double du système ayant une configuration matérielle et des adresses IP/noms d'ordinateur identiques.	• Un système cible dont le matériel est identique au système source et • Sauvegardes du système source ou accès au système source pour en effectuer une sauvegarde	Utilisez le workflow de sauvegarde et restauration système détaillé dans ce guide. Voir la procédure Sauvegarde du système entier [page 569]. Recréer le système cible à partir de sauvegardes du système source.
Objectif : Copier Je désire créer à des fins de mise en veille, de test ou de formation un double du système ayant une configuration matérielle et des adresses IP/noms d'ordinateur différents du système source.	• Système source (en cours d'exécution ou arrêté) OU sauvegardes des bases de données et fichiers du système source et • Informations système détaillées décrites dans Pour exporter depuis un système source [page 594].	Utilisez le workflow de copie du système en commençant par Planification de la copie du système [page 591] et suivez les instructions du reste du chapitre. **Remarque** Vous pouvez créer le système cible sur un ordinateur qui comporte un déploiement existant de la plateforme de BI de la même version et le même niveau de Support Package et de correctif, ou sur un ordinateur "propre" sans installation de la plateforme de BI.

Informations associées

Sauvegardes [page 568]
Planification de la copie du système [page 591]

15.4 Planification de la copie du système

Une copie du système ne doit pas refléter obligatoirement le système actuel. Vous pouvez créer une copie du système et attendre quelque temps avant de recréer la copie sur le système source ou bien vous pouvez utiliser une sauvegarde précédente du système source comme base du système cible. Cela signifie que la copie sera celle du système tel qu'il se présentait au moment de la création de la copie. Par exemple, si vous attendez un moi, la copie recrée le système tel qu'il était un mois auparavant.

Après avoir examiné les cas d'utilisateur de la section précédente et décidé laquelle vous convenait le mieux, développez un plan de copie de système.

Créer un plan de copie de système

Lors de la planification d'une copie de système, vous devez décider à l'avance des points suivants :

- Le système source sera-t-il arrêté ou actif lors de la réalisation de la copie ? (La procédure peut être réalisée dans les deux cas.)
  - Si le système source est arrêté, combien de temps d'arrêt sera nécessaire ?
  - Prévoyez un certain temps de test pour vous assurer de l'intégrité du système cible.
- Les outils de base de données à utiliser pour la sauvegarde et la restauration de la base de données.
- Les ordinateurs sur lesquels le système cible sera déployé et l'emplacement où sera hébergé chaque nœud.
- Les composants facultatifs à copier.
- Le type à utiliser pour la base de données du CMS cible et toutes les autres bases de données facultatives à copier.

Prenez également en compte les sujets suivants :

- Les composants de plateforme de BI que votre système source a installés. Vous pouvez utiliser la fonction *Ajouter/Supprimer* > *Modifier* du programme d'installation pour afficher la liste des composants actuellement installés.
- Si le système cible est installé sur une configuration matérielle différente de celle du système source, il peut être nécessaire d'affiner les réglages du système cible pour améliorer les performances. Voir les informations relatives à l'optimisation des performances de votre système dans le guide *SAP BusinessObjects Business Intelligence sizing companion guide*
- Vous voulez éventuellement que le système cible crée des rapports à partir de bases de données de reporting autres que celles du système source. Dans ce cas, vous devrez modifier les informations de connexion des base de données de reporting. Pour ce faire, conservez le nom DSN mais en faisant pointer le DSN du système cible vers une autre base de données.

Composants du système source requis

- Base de données système du CMS
- Stockage de fichiers du FRS
- Fichiers de configuration de couche sémantique
- Base de données d'audit (facultatif)
- Base de données de surveillance (facultatif)
- Base de données des sous-versions de la gestion des promotions (facultatif)

15.5 Remarques et restrictions

Vous devez être informé des remarques suivantes lors de la copie du déploiement de votre plateforme de BI.

Zone	Remarque
Intégrations de SAP Business Warehouse	Si vous utilisez la plateforme de BI et SAP ERP ou BW dans un environnement intégré, lisez la documentation relative à la copie de système SAP avant de réaliser la copie de votre système. Les guides sur la copie du système sont disponibles à l'adresse http://www.sdn.sap.com/irj/sdn/systemcopy (connexion SMP requise). Choisissez votre version de SAP NetWeaver ; les guides de copie correspondants se trouvent dans le dossier des guides d'installation.
Version du programme	Les systèmes source et cible doivent être au même niveau de version, Support Package et correctif.
Contenu et paramètres de configuration	Seule l'intégralité du système source peut être copiée. Il n'est pas possible de copier sélectivement du contenu ou des paramètres de configuration système.
Chemin d'installation	Le chemin d'installation des emplacements source et cible doit être identique : Par exemple, si vous avez installé le système source sous `C:\SAP BusinessObjects Enterprise XI 4.0`, le système cible doit être installé sous `C:\SAP BusinessObjects Enterprise XI 4.0`.
Système d'exploitation hôte	Les systèmes d'exploitation source et cible doivent être identiques.
Type de logiciel de la base de données du CMS	Les bases de données du CMS source et cible doivent être du même type. Vous aurez la possibilité de changer de type de base de données prise en charge après la copie du système.
Type de logiciel de la base de données d'audit	Si vous copiez la base de données d'audit, les bases de données d'audit source et cible doivent être du même type. Après création de la copie, vous pouvez établir une nouvelle base de données de type différent. **Remarque** Si vous établissez une nouvelle base de données, les événements existants n'y sont pas copiés, seuls les nouveaux événements y seront enregistrés.
Personnalisation du niveau Web	La procédure ne copie pas les composants du niveau Web du système source. Si vous avez personnalisé le niveau Web (par exemple, modifié les fichiers `.properties` du dossier `custom`), vous devez appliquer manuellement ces personnalisations au système cible.
Rubriques non couvertes par ces instructions	Ce workflow ne décrit pas comment exporter ou importer une base de données. Utilisez les outils du fournisseur de vos bases de données pour copier et restaurer les bases de données.

Les données suivantes sont copiées au cours de la procédure de copie de système :

- Base de données de référentiel du CMS (contient des rapports, des analyses, des dossiers, des droits, des utilisateurs et des groupes d'utilisateurs, des paramètres serveur ainsi que d'autre contenu BI et contenu système)
- Base de données d'audit (contient des événements d'audit déclenchés par les serveurs ou les applications client de la plateforme de BI)
- Base de données de surveillance (contient les données de tendance des métriques, tests et veilles)
- Base de données de gestion des versions (contient différentes versions des rapports, analyses, autre sressources BI ainsi que des informations sur les versions)

> **Remarque**
>
> Pour consulter une description des bases de données et de leur contenu, voir la section Bases de données [page 38] de ce guide.

- Fichiers de configuration de couche sémantique

La configuration du niveau Web, l'index de recherche et toutes les données non mentionnées spécifiquement ci-dessus ne sont pas copiés.

Remarques sur les copies de récupération de fichier

Si vous copiez un système dans l'objectif de récupérer un fichier supprimé par erreur, vous devez prendre en compte les remarques supplémentaires ci-dessous :

A l'aide de votre sauvegarde, suivez les étapes de la procédure Pour importer dans un système cible [page 598] sur le système de production.

- N'installez pas tous les nœuds, installez seulement le premier nœud qui contient le CMS et sa base de données.
- N'installez pas les bases de données d'audit, de gestion des promotions ou de surveillance.
- Ne recréez pas les connexions aux bases de données d'audit ou de reporting.

Utilisez LCM pour promouvoir dans le système source l'objet que vous voulez récupérer dans le système cible.

15.6 Procédure de copie de système

Les procédures suivantes vous guident à travers les deux étapes de la copie de votre déploiement de la plateforme de BI.

15.6.1 Pour exporter depuis un système source

Vous devez noter les informations suivantes concernant le système source. Pour écrire ces informations, il existe une feuille de calcul à l'emplacement Feuille de calcul Copie du système [page 1251]

Propriété	Emplacement
Clé du cluster du CMS (gardez l'enregistrement en lieu sûr)	Créée par l'administrateur système lors de l'installation de la plateforme de BI.
Nom des nœuds.	Accédez à l'onglet *Serveurs* de la CMC et développez *nœuds* dans l'arborescence de gauche.
Nom d'ordinateur et dossier d'installation de la plateforme de BI pour chaque ordinateur du déploiement.	Accédez à l'onglet *Serveurs* de la CMC, cliquez avec le bouton droit sur le CMS et sélectionnez *Espaces réservés*. Recherchez la valeur de l'espace réservé `%INSTALLROOTDIR%`.
Mote de passe administrateur de la plateforme de BI (conservez l'enregistrement en lieu sûr).	Créée par l'administrateur système lors de l'installation de la plateforme de BI.
Toutes les connexions de base de données pouvant être utilisées par le CMS, ainsi que les noms d'utilisateur et les mots de passe associés à ces connexions. La base de données d'audit peut en faire partie si vous voulez copier ces informations. Relevez bien les informations pour tous les ordinateurs du cluster. **Remarque** Si vous copiez la base de données d'audit, vous aurez aussi besoin des noms et des références de connexion la concernant.	Accédez à l'onglet *Serveurs* de la CMC, cliquez avec le bouton droit sur le CMS et sélectionnez *Métriques*. Recherchez les métriques suivantes : • *Nom de la connexion à la base de données système* • *Nom du serveur de la base de données système* • *Nom de l'utilisateur de la base de données système* • *Nom de la source de données* • *Nom de connexion de la base de données d'audit* (facultatif) • *Nom d'utilisateur de la base de données d'audit* (facultatif)
Pour chaque ordinateur du cluster, les détails (types de client, versions) de toutes les autres connexions de base de données (utilisées par les univers et les rapports, par exemple). Vérifiez que vous avez les noms d'utilisateurs et mots de passe.	Pour les rapports Crystal directement issus des bases de données, recherchez les informations de connexion à l'aide des concepteurs SAP Crystal Reports 2020 ou SAP Crystal Reports pour Enterprise. Pour obtenir les informations de connexion d'univers, utilisez l'outil de conception d'information (.unx) ou l'outil de conception d'univers (.unv).
Niveau de version, de Support Package et de correctif du système source.	Sous Windows, vous pouvez le déterminer en consultant l'outil *Modifier ou supprimer des programmes*. Sous Unix, vous pouvez utiliser l'utilitaire `modifyOrRemoveProducts.sh` dans le répertoire d'installation de la plateforme de BI.
Emplacements de stockage de fichiers de chaque Input FRS et Output FRS du déploiement.	Accédez à l'onglet *Serveurs* de la CMC, cliquez avec le bouton droit de la souris sur l'Input FRS ou l'Output FRS et sélectionnez *Propriétés*. Recherchez la propriété *Répertoire de stockage des fichiers*.

Propriété	Emplacement
	Remarque Si la valeur commence par %, c'est un espace réservé, vous devrez cliquer sur *Espaces réservés* et noter le répertoire listé sous cet espace réservé.
Si vous prévoyez de copier Gestion des promotions, l'emplacement du dossier de la base de données Gestion des promotions et des dossiers Sous-version.	Le dossier par défaut de la base de données Gestion des promotions des installations Windows est `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` et sous Unix `<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride`. Les emplacements par défaut des fichiers Sous-version des installations Windows sont : • `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` Sous Unix, il s'agit de : • `<INSTALLDIR>/check_out` (Ce répertoire est créé uniquement lorsque vous avez utilisé la Sous-version pour extraire des fichiers.) • `$HOME/LCM_Repository`
Si vous prévoyez de copier la base de données de surveillance, le dossier de celle-ci.	Cela est défini dans la CMC. Accédez à la zone de gestion *Applications* de la CMC, sélectionnez *Application de surveillance* > *Propriétés* et recherchez le *répertoire de sauvegarde de la base de données des tendances*. Le dossier par défaut des installations Windows est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` et sous Unix, `<REPINSTALL>/sap_bobj/Data/TrendingDB`.
Chemin du dossier de la couche sémantique	Le chemin d'accès au dossier par défaut dans les installations Windows est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connections Server\` par défaut.

Après avoir enregistré les informations ci-dessus :

1. Utilisez les outils de sauvegarde de votre fournisseur de bases de données pour créer une copie de sauvegarde des bases de données suivantes :

- Base de données système du CMS
- Base de données d'audit (facultatif)

2. A l'aide des outils de sauvegarde de fichiers, sauvegardez les ensembles de fichiers suivants :
   - Stockage des fichiers de l'Input FRS et de l'Output FRS.
   - Base de données des tendances de surveillance (facultatif). Cela peut se faire en sauvegardant les fichiers du dossier de surveillance tels qu'ils sont enregistrés dans la feuille de calcul. Par défaut, sous Windows, il s'agit de : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. Sous Unix : `<REPINSTALL>/sap_bobj/Data/TrendingDB`.
   - Base de données des sous-versions de la gestion des promotions (facultatif) Cela peut se faire en sauvegardant les fichiers des dossiers de sous-version tels qu'ils sont enregistrés dans la feuille de calcul. Par défaut, sous Windows, il s'agit de :
     - `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`.

     Sous Unix, il s'agit de :
     - `<INSTALLDIR>/check_out` (Ce répertoire est créé uniquement lorsque vous avez utilisé la Sous-version pour extraire des fichiers.)
     - `$HOME/LCM_Repository`
   - Fichiers de configuration du dossier de la couche sémantique : le fichier `cs.cfg` dans le dossier `connectionServer` et tous les fichiers `.sbo` et `.prm` de tous ses sous-dossiers.

   > **Remarque**
   >
   > Pour consulter les contraintes et une description détaillée de ce workflow, voir la section Sauvegardes à chaud [page 569].

3. Les fichiers suivants sont personnalisables par l'utilisateur. Si vous avez personnalisé l'un d'entre eux, sauvegardez les fichiers du système source et restaurez-les ensuite dans le même dossier du système cible :
   - `BO_trace.ini`, installé sous :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml` installé sur :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` installé sous :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties` installé sous :
     - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
   - Les fichiers de configuration WDeploy installés sous `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf` :
     - `config.apache`
     - `config.jboss7`
     - `config.sapappsvr75`
     - `config.tomcat6`

    - `config.tomcat7`
    - `config.weblogic11`
    - `config.websphere7`
    - `config.websphere8`
    - `wdeploy.conf`
4. Les fichiers de niveau Web suivants sont personnalisables par l'utilisateur. Si vous avez apporté des modifications à l'un de ces fichiers, sauvegardez les fichiers du système source. Par la suite, vous devrez les restaurer ou réappliquer les modifications au système cible.
   - `BO_trace.ini` installé sur :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
   - `clientaccesspolicy.xml` installé sous :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
   - `clientSDKOptions.xml` installé sur :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
   - `crossdomain.xml` installé sous :
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
     - `[INSTALLDIR]tomcat/webapps/ROOT`
   - Tous les fichiers personnalisés du dossier `config/custom` (dans le niveau Web). Sauvegardez ces fichiers pour transférer la personnalisation au système cible.
5. Sauvegardez les extensions personnalisées ajoutées manuellement au système source, par exemple les extensions de publication, les bibliothèques personnalisées, etc.

Conservez les informations enregistrées ci-dessus avec la copie des bases de données et des fichiers. Vous pouvez éventuellement conserver une deuxième copie avec laquelle vous pouvez mettre à jour le cas échéant les futures procédures de copie du système.

15.6.2 Pour importer dans un système cible

Cette procédure part du principe que vous avez créé des copies de sauvegarde des bases de données et des fichiers système du déploiement source à utiliser dans votre système cible. Tous les fichiers de sauvegarde doivent provenir du même jeu de sauvegarde. Vous avez également besoin des détails (clé de cluster et références de connexion à la base de données, par exemple) figurant dans « Pour exporter depuis un système source ».

Si votre système cible est destiné à résider dans un emplacement réseau avec accès aux ressources du système source, vous devez vous assurer que le système cible ne tente pas d'accéder à ces ressources tant qu'il n'a pas été reconfiguré. Cela peut se faire en plaçant un pare-feu entre le système cible et les ressources du système source ou en laissant le système source à l'arrêt pendant que vous démarrez le système cible. Après le premier démarrage du système cible, le pare-feu peut être supprimé ou le système source démarré.

Si la plateforme de BI est déjà installée sur le système cible, assurez-vous qu'elle a le même niveau de version, de Support Package et de correctif que le système source au moment de la création de la copie. Assurez-vous également qu'elle utilise le même chemin d'installation que celui du système source.

1. Sur le système cible, créez les connexions vers la ou les bases de données où vous avez l'intention de placer le référentiel du CMS, la base de données d'audit, et la base de données de reporting.

   > **Remarque**
   >
   > Si les connexions peuvent pointer vers une base de données différente, elles doivent avoir le même nom de connexion ou DSN et utiliser les mêmes références de connexion que le système source.

2. Utilisez les outils de votre base de données pour retaurer la base de données système du CMS et la base de données d'audit (éventuellement) à partir de la sauvegarde du système source dans la base de données cible.

   Si les univers et les rapports du système cible doivent utiliser une base de données de reporting différente, modifiez la connexion pour qu'elle pointe vers cette base de données.

   Pour obtenir d'autres instructions sur cette étape, voir la rubrique Restauration du système [page 576].

3. Si la plateforme de BI est installée sur le système hôte cible, ignorez l'étape 4. Si la plateforme de BI n'est pas installée, installez-la sur le système hôte cible en respectant les étapes suivantes :
   a. Installez le même niveau de version de programme, de Support Package et de correctif que le système source.
   b. Utilisez le même chemin d'installation que celui du système source.
   c. Sélectionnez les mêmes composants que ceux installés sur le système source.
   d. Lorsque le programme d'installation vous demande de créer la base de données du CMS (et la base de données d'audit, le cas échéant), sélectionnez l'option *Utiliser un serveur de base de données existant* et saisissez le nom de connexion et les références de connexion définis à l'étape 1.

      > **Remarque**
      >
      > Ne choisissez pas de réinitialiser la base de données du CMS.

   e. Lorsque vous êtes invité à indiquer le *Nom de nœud*, utilisez les mêmes noms, numéros de port, mot de passe administrateur et clé de cluster que dans le système source.

      Pour consulter des instructions d'installation complètes, voir le *SAP Guide d'installation de la plateforme BusinessObjects Business Intelligence*. Si le système a terminé l'installation, passez à l'étape 6.

      > **Remarque**
      >
      > Si vous ne copiez pas vos données d'audit du système source, vous pouvez créer une nouvelle base de données d'audit en configurant l'audit pendant la procédure d'installation.

   f. Arrêtez tous les nœuds dans le CCM.

4. Si la plateforme de BI est déjà installée sur le système cible, arrêtez tous les nœuds dans le CCM. Démarrez le CCM sur l'ordinateur hébergeant le CMS du système cible.

5. Si la plateforme de BI est déjà installée, ajoutez un nœud à l'aide de l'option *Recréer le nœud*.
   a. Utilisez le *Nom du nœud* et le *Numéro de port SIA* du système source.
   b. Sélectionnez *Démarrer un nouveau CMS temporaire*.
   c. Sélectionnez un nouveau *Numéro de port du CMS* (il peut s'agir de n'importe quel port libre) et *Type de base de données du CMS* (correspondant au type de base de données restauré).

d. Saisissez les détails de la connexion à laquelle a été restaurée la base de données du CMS à l'étape 1.
e. Saisissez la clé de cluster du système source.
f. Saisissez le mot de passe administrateur du système source.

6. Restaurez les stockages de fichiers de l'Input FRS et de l'Output FRS sur le stockage de fichiers système cible. Utilisez le même dossier que celui utilisé sur le système source.
7. Si vous voulez copier les informations de surveillance, restaurez le dossier de la base de données de surveillance dans le même dossier que celui utilisé sur le système source.
8. Restaurez le dossier de la base de données Gestion des promotions (si vous désirez copier les informations Gestion des promotions) dans le même dossier que celui utilisé sur le système source.
9. Restaurez les fichiers Sous-version (si vous désirez copier les informations Gestion des promotions) dans le même dossier que celui utilisé sur le système source.
10. Restaurez les fichiers du serveur de la couche sémantique/de la configuration des connexions dans le même dossier que celui utilisé sur le système source.
11. Redémarrez les ordinateurs hébergeant le système cible.
12. Si vous avez installé la plateforme de BI sur le système cible à l'étape 3, appliquez les Support Packages et correctifs nécessaires conformément au système source.
13. Si le système cible doit être exécuté sur plusieurs ordinateurs hôte, répétez les étapes 1 à 11 pour chaque ordinateur hôte.

    Utilisez l'option Installation étendue lors de l'installation de nœuds de la plateforme de BI supplémentaires et gardez à l'esprit que les mêmes noms de nœud que sur le système source doivent être utilisés pour les nœuds supplémentaires du système cible.
14. Si la base de données du CMS du système cible est destinée à utiliser un type de base de données différent du système source, utilisez le CCM pour effectuer une Copie de données d'une base de données système d'un CMS dans une autre [page 520] en spécifiant comme destination la base de données à utiliser pour la copie.
15. Restaurez les fichiers personnalisables par l'utilisateur sauvegardés lors de l'étape 3 de la procédure « Pour exporter depuis un système source ».
16. Restaurez les fichiers de niveau Web sauvegardés lors de l'étape 4 de la procédure « Pour exporter depuis un système source ».

    « Niveau Web » fait référence à la zone de préparation WDeploy où vous pouvez réaliser les personnalisations et au contenu du niveau Web déployé sur le serveur d'applications.

    Sur le système cible, ne modifiez pas le répertoire du serveur d'applications, appliquez les modifications à la zone de préparation WDeploy, puis redéployez le niveau Web sur le serveur d'applications à l'aide de WDeploy.

    La zone de préparation WDeploy est à cet emplacement sous Windows : `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/warfiles`.
17. Restaurez les extensions sauvegardées lors de l'étape 5 de la procédure « Pour exporter depuis un système source ».

Après exécution de la copie du système de la plateforme de BI :

1. L'installation du premier nœud sur la cible crée un CMS temporaire qui sera arrêté à l'issue de l'installation. A l'aide de la CMC, accédez à la page Serveurs et supprimez ce CMS.

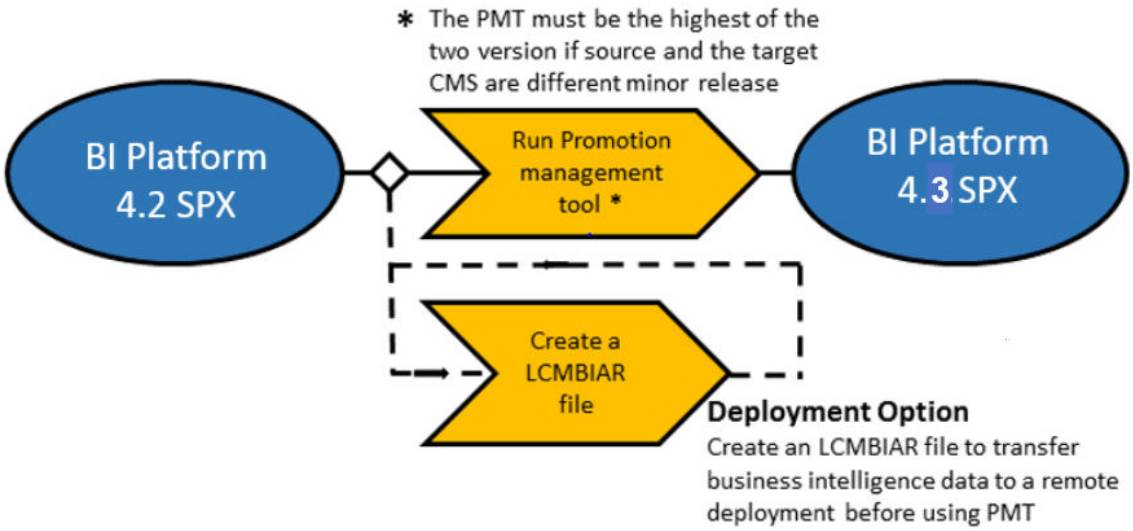
> → N'oubliez pas
>
> Si vous ne supprimez pas le système source (ou si vous l'utilisez en même temps que le système cible), il est recommandé de renommer le cluster sur le système cible.

2. Exécutez le Repository Diagnostic Tool sur la base de données du CMS cible.
3. Le cas échéant, configurez la connexion unique Windows AD sur le système cible. Voir Connexion unique à la plateforme de BI avec l'authentification AD [page 323].
4. Le cas échéant, configurez SLD sur le système cible. Pour en savoir plus, voir la note SAP 1508421 : « SAP SLD Data Supplier for Apache Tomcat » (Fournisseur de données SAP SLD pour Apache Tomcat).
5. Effectuez un test de validité de votre système cible pour vous assurer de son intégrité.
6. Effectuez une réindexation complète de la recherche.

16 Gestion des promotions

16.1 Bienvenue dans la gestion des promotions

16.1.1 Présentation



L'outil de gestion des promotions permet d'effectuer les opérations suivantes :

- Déplacement ou transport des ressources Business Intelligence (BI) d'un référentiel à un autre.
- Gestion des dépendances des ressources.
- Reprise des ressources promues dans le système de destination, le cas échéant.

L'outil de gestion des promotions prend également en charge la gestion de différentes versions de la même ressource BI.

L'outil de gestion des promotions est intégré à la Central Management Console. Vous pouvez promouvoir une ressource de Business Intelligence d'un système vers un autre uniquement si la même version de la plateforme de BI est installée à la fois sur le système source et sur le système de destination.

16.1.2 Fonctionnalités

L'outil de gestion des promotions permet d'effectuer les actions suivantes sur les InfoObjects du déploiement de destination.

- Créer un travail
- Copier un travail existant
- Modifier un travail
- Planifier une promotion de travail
- Afficher l'historique d'un travail
- Exporter sous LCMBIAR
- Importer BIAR et LCMBIAR

Le workflow de promotion comprend aussi les tâches suivantes :

- *Gérer les dépendances* Cette fonctionnalité permet de sélectionner, de filtrer et de gérer les objets dépendants des InfoObjects dans le travail que vous souhaitez promouvoir.
- *Planification* Cette fonctionnalité permet de spécifier un moment pour la promotion d'un travail au lieu de promouvoir ce travail dès sa création. Vous pouvez indiquer si vous souhaitez que la promotion d'un travail soit exécutée à une fois ou périodiquement.
- *Sécurité* Cette fonctionnalité permet de promouvoir des InfoObjects, ainsi que de leurs droits de sécurité associés et, si nécessaire, promeut les InfoObjects associés aux droits d'application.
- *Tester la promotion* Cette fonctionnalité permet de contrôler ou de tester la promotion pour vérifier que toutes les mesures préventives sont prises avant la promotion réelle des InfoObjects.
- *Reprise* Cette fonctionnalité permet de restaurer le système de destination à son statut précédent après la promotion d'un travail. Vous pouvez reprendre l'intégralité d'un travail ou une partie de celui-ci.
- *Audit* Les événements générés par l'outil de gestion des promotions sont stockés dans la base de données d'audit. Cette fonctionnalité permet de surveiller les événements connectés à la base de données d'audit.
- *Paramètres de remplacement Gestion des promotions* Cette fonctionnalité permet d'analyser et de promouvoir les remplacements par le biais d'une promotion de travail.

16.1.3 Droits d'accès à l'application

Cette section décrit les droits d'accès à l'application pour l'outil de gestion des promotions.

- Vous pouvez définir les droits d'accès à l'outil de gestion des promotions dans la CMC.
- Vous pouvez définir les droits d'application granulaires pour différentes fonctionnalités dans l'outil de gestion des promotions.

Pour définir des droits spécifiques dans l'outil de gestion des promotions, procédez comme suit :

1. Connectez-vous à la CMC, puis sélectionnez *Applications*.
2. Cliquez deux fois sur *Gestion des promotions*.
3. Cliquez sur *Sécurité de l'utilisateur* et sélectionnez un utilisateur. Vous pouvez visualiser les droits de sécurité de l'utilisateur ou lui en affecter.
4. Les droits spécifiques à la gestion des promotions disponibles sont les suivants :
   - Autoriser l'accès pour modifier les remplacements
   - Autoriser l'accès pour inclure la sécurité
   - Autoriser l'accès à l'administration
   - Autoriser l'accès pour gérer les dépendances
   - Création de travail

- Supprimer les travaux
- Modifier le travail
- Modifier LCMBIAR
- Exporter sous LCMBIAR
- Importer LCMBIAR
- Promotion de travail
- Reprise
- Vue et sélection des objets BOMM (BusinessObjects Metadata)
- Vue et sélection des vues d'entreprise
- Vue et sélection des calendriers
- Vue et sélection des connexions
- Vue et sélection des profils
- Vue et sélection des QaaWS
- Vue et sélection des objets de rapport
- Vue et sélection des paramètres de sécurité
- Vue et sélection des univers

5. Si vous souhaitez affecter des droits à un utilisateur sélectionné, sélectionnez le droit en question et cliquez sur *Affecter la sécurité*.

Les droits d'accès à l'outil gestion des promotions sont définis dans la CMC (Central Management Console).

16.1.4 Prise en charge de WinAD dans la gestion des promotions

Pour que l'outil de gestion des promotions fonctionne correctement, vous devez ajouter les éléments suivants à tous les arguments `javaargs` pour tous les Adaptive Job Servers :

```
Djava.security.auth.login.config=<chemin>\bsclogin.conf,Djava.security.krb5.conf=
<chemin>\krb5.ini
```

> → N'oubliez pas
>
> Spécifiez le bon chemin d'accès à `bsclogin.conf` et `krb5.ini` sur votre déploiement.

16.2 Introduction à l'outil de gestion des promotions

16.2.1 Accès à l'outil de gestion de la promotion

Pour accéder à l'outil de gestion de la promotion, sélectionnez *Gestion de la promotion* sur la page d'accueil de la CMC.

Un utilisateur possédant des autorisations d'affichage dans le dossier *Travaux de promotion* peut lancer l'outil de gestion de la promotion. Cependant, pour créer, planifier ou promouvoir un travail, l'utilisateur doit obtenir des droits supplémentaires de la part de l'administrateur.

16.2.2 Composants de l'interface utilisateur

Ce chapitre traite des composants de l'interface utilisateur graphique dans l'outil de gestion des promotions.

- Barre d'outils de l'espace de travail de gestion des promotions
- Panneau Espace de travail
- Arborescence
- Panneau Détails
- Page Panier et Visualiseur de travail

Barre d'outils de l'espace de travail de gestion des promotions

Le tableau suivant répertorie les options incluses dans la barre d'outils de l'espace de travail de gestion des promotions et traite des tâches que vous pouvez exécuter à l'aide de ces options :

Option	Description
	Permet de créer un dossier. Le nouveau dossier est créé en tant que sous-dossier dans le dossier *Travaux de promotion*.
	Permet de copier et de supprimer le travail ou le dossier sélectionné à partir de son emplacement actuel.
	Permet de copier le travail ou le dossier à partir de son emplacement actuel.
	Permet de coller le travail ou le dossier dans un nouvel emplacement.
	Permet de supprimer un travail ou un dossier existant.
	Permet d'actualiser la page d'accueil pour obtenir la liste mise à jour des travaux ou dossiers.
Propriétés	Permet de modifier les propriétés du travail sélectionné. Vous pouvez modifier le titre, la description et les mots clés du travail sélectionné.
Historique	Permet de visualiser l'historique du travail sélectionné.
Nouveau travail	Permet de créer un travail.
Importer	Permet d'importer des fichiers BIAR, LCMBIAR ou de remplacer des fichiers.
Modifier	Permet de modifier le travail sélectionné.
Promouvoir	Permet de promouvoir le travail sélectionné.

Option	Description
Reprise	Permet d'annuler le travail promu sur le système de destination. **Remarque** Si le travail promeut des objets vers la destination, la reprise supprime ces objets. Si le travail met à jour des objets sur la destination, la reprise restaure la version précédente de ces objets.
1	Permet de naviguer dans les pages d'une liste de travaux. Vous pouvez utiliser cette option pour naviguer dans une seule page ou vers une page précise en saisissant le numéro de page adéquat.
Rechercher	Permet de rechercher des travaux précis. Vous pouvez rechercher un travail à l'aide de son nom, ses mots clés, sa description ou des trois paramètres.
Travaux de promotion	Permet de visualiser des travaux et des dossiers.
Statut de promotion	Affiche les travaux promus selon leur statut, à savoir Réussite, Echec ou Réussite partielle.

Panneau Espace de travail

Le panneau Espace de travail de la page d'accueil Gestion des promotions affiche la liste des travaux. Vous pouvez utiliser ce panneau pour visualiser le nom, le statut, l'heure de la création, l'heure de la dernière exécution du travail, les systèmes source et de destination ainsi que le créateur du travail.

Arborescence

Le panneau des arborescences de la page d'accueil Gestion de la promotion affiche l'arborescence contenant les dossiers *Travail de promotion* et *Statut de la promotion*. Les travaux sont affichés dans une structure hiérarchique sous le dossier *Travail de promotion*. Le dossier *Statut de la promotion* affiche les travaux promus selon leur statut.

Page Visualiseur de travail

La page « Visualiseur de travail » s'affiche lorsqu'un utilisateur crée un travail ou modifie un travail existant. Elle contient une liste générée dynamiquement d'InfoObjects à promouvoir et un panneau Détails. La liste organise les InfoObjects en groupes d'utilisateurs, univers et connexions. Le panneau Détails affiche le contenu du nœud sélectionné dans la liste.

16.2.3 Utilisation de l'option Paramètres

L'option Paramètres permet de configurer des paramètres avant la promotion d'InfoObjects d'un déploiement de la plateforme de BI vers un autre déploiement de la plateforme de BI et un déploiement SAP. Cette section décrit comment utiliser les options de paramètres.

Cliquez sur la liste déroulante *Paramètres* dans l'écran *Travaux de promotion*. La liste déroulante affiche les options suivantes :

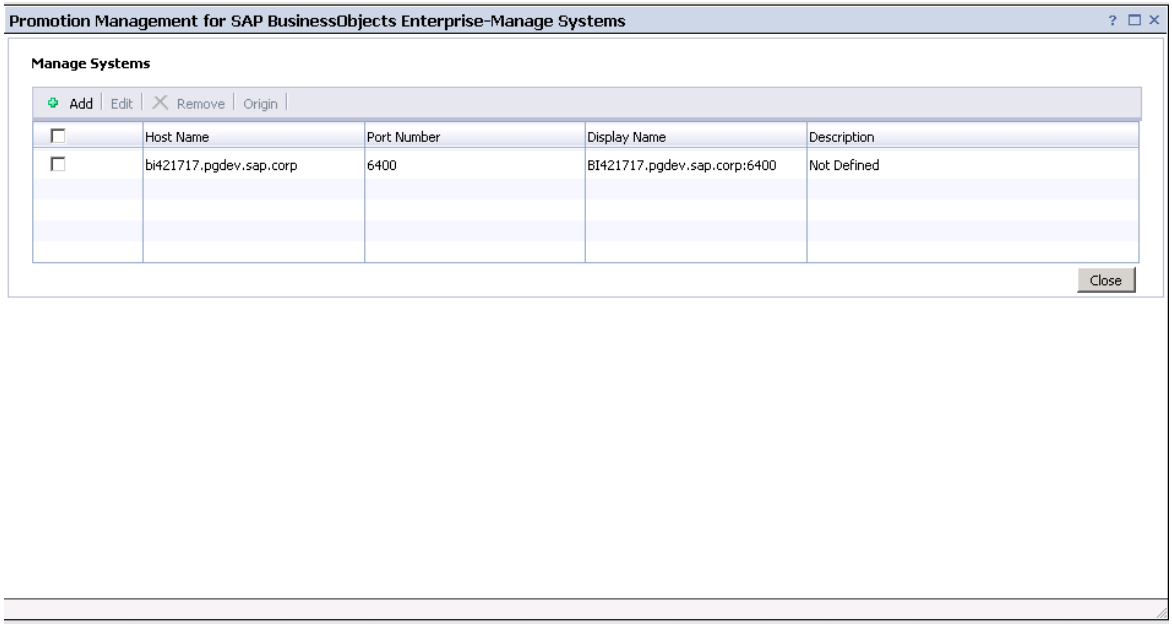
- *Gérer les systèmes* Cette option vous permet d'ajouter tous les systèmes requis pour les activités de gestion des promotions.
- *Paramètres de reprise* Cette option vous permet de sélectionner un système pour lequel la reprise est activée.
- *Paramètres du travail* Cette option vous permet d'afficher les instances finalisées sur la page Dépendances et de gérer les activités de nettoyage des instances de travail. Elle permet aussi le filtrage par date de création.
- *Paramètres CTS* Cette option vous permet d'ajouter le service Web et les informations du système SAP BW pour l'intégration du système Enhanced Change and Transport.

16.2.3.1 Pour utiliser l'option Gérer les systèmes

Cette section décrit comment utiliser l'option Gérer les systèmes. Vous pouvez ajouter ou supprimer des systèmes hôtes à l'aide de cette option.

Pour ajouter un système hôte, procédez comme suit :

1. Dans la barre d'outils de l'espace de travail de gestion des promotions, cliquez sur l'option *Paramètres* puis sur *Gérer les systèmes*.
   La fenêtre *Gérer les systèmes* s'affiche. Cette fenêtre affiche une liste des noms d'hôtes, numéros de ports, noms d'affichage et descriptions.



2. Cliquez sur *Ajouter*.
   La boîte de dialogue *Ajouter un système* apparaît.
3. Ajoutez le nom d'hôte, le numéro de port, le type d'affichage et la description dans les champs appropriés.

   > **Remarque**
   >
   > Sélectionnez l'option *Marquer comme origine* pour identifier le système comme système source, à savoir le système d'où proviennent les informations de connexion. Cette option s'avère utile lorsque vous utilisez des remplacements.

4. Cliquez sur *OK* pour ajouter le système.
   Le système hôte est ajouté à la liste.

> **Remarque**
>
> Pour supprimer ou modifier un système hôte, sélectionnez un système hôte, puis cliquez sur *Supprimer* ou *Modifier*.

Informations associées

Pour utiliser l'option Paramètres de reprise [page 608]
Pour utiliser l'option Paramètres du travail [page 608]

16.2.3.2 Pour utiliser l'option Paramètres de reprise

Par défaut, le processus de reprise est activé au niveau du système. L'option *Paramètres de reprise* permet de désactiver le processus de reprise au niveau du système.

Pour désactiver le processus de reprise au niveau du système, procédez comme suit :

1. Dans la liste des systèmes hôte de la fenêtre *Reprise*, sélectionnez le système hôte pour désactiver le processus de reprise.
2. Cliquez sur *Enregistrer et fermer* pour enregistrer les modifications.

Informations associées

Pour utiliser l'option Paramètres du travail [page 608]

16.2.3.3 Pour utiliser l'option Paramètres du travail

L'option Paramètres du travail permet de spécifier si vous souhaitez ou non afficher les instances finalisées dans la page « Gérer les dépendances » et le nombre d'instances de travail pouvant exister dans le système. Vous pouvez spécifier l'une des options suivantes :

- *Afficher les instances finalisées dans la page Gérer les dépendances* Permet de visualiser les instances finalisées dans la page « Gérer les dépendances » à ajouter au travail.
- *Supprimer les instances en surnombre lorsqu'il existe plus de N instances de l'objet* Permet de limiter le nombre d'instances par objet dans le système.
- *Supprimer les instances après N jours pour le travail* Permet de spécifier les instances de travail créées avant un nombre défini de jours à supprimer.
- Dans la liste déroulante *Afficher les travaux créés*, vous pouvez sélectionner l'intervalle de temps pour visualiser les travaux créés au cours de la période spécifiée.

Pour définir l'option *Paramètres du travail*, procédez comme suit :

1. Sélectionnez l'option et saisissez la valeur souhaitée.
2. Cliquez sur *Enregistrer* pour enregistrer les modifications mises à jour.

Vous pouvez cliquer sur *Paramètres par défaut* pour définir les valeurs par défaut, puis cliquer sur *Fermer* pour fermer la fenêtre.

> ⓘ Remarque
>
> Les anciennes instances de travail ne seront supprimées que lors de la prochaine exécution de travail.

Informations associées

Utilisation de Apache SubVersion comme système de gestion des versions [page 698]

16.2.3.4 Utilisation de l'option Remplacer les options

L'option Remplacer les options permet de promouvoir les remplacements à l'aide d'une promotion de travail ou d'un fichier LCMBIAR. Cette option vous permet d'analyser, de promouvoir et de modifier les informations de connexion à la base de données pour les connexions Crystal Reports et Universe. Vous pouvez également l'utiliser pour modifier les URL QAAWS.

> ⓘ Remarque
>
> Pour utiliser l'option Remplacer les options, vous devez installer Adobe Flash Viewer.

Le terme *système* est utilisé dans les procédures suivantes. Il existe trois types de systèmes :

- *Origine* : Le système d'origine pour toute information de connexion.
- *Système central de la gestion des promotions* : Le système exécutant l'outil de gestion des promotions.
- *Destination* : Le système final dans lequel les ressources Business Intelligence sont promues.

16.2.3.4.1 Pour promouvoir les remplacements

Ajoutez un système hôte avant de promouvoir les remplacements. Pour en savoir plus sur l'ajout des systèmes hôtes, voir Pour utiliser l'option Gérer les systèmes [page 607].

Pour promouvoir les remplacements, procédez comme suit :

1. Dans la barre d'outils de l'espace de travail de gestion des promotions, cliquez sur l'option *Paramètres de remplacement*.
   La fenêtre *Paramètres de remplacement* s'affiche.
2. Dans le volet *Origine*, sélectionnez le système source désiré dans le menu déroulant.

   > ⓘ Remarque
   >
   > Vous pouvez également choisir de vous connecter à un *Nouveau système*. Pour choisir un nouveau système en tant que système source, procédez comme suit :
   > 1. Sélectionnez *Nouveau système* dans le menu déroulant.
   > La boîte de dialogue Identification d'origine s'affiche.
   > 2. Saisissez les références de connexion valides dans les champs *Système*, *Nom d'utilisateur*, *Mot de passe* et *Authentification*.
   > 3. Sélectionnez *Connexion*.

3. Sélectionnez *Connexion*.
4. Sélectionnez *Analyser*.

   Le processus d'analyse démarre. La *liste de connexions uniques* s'affiche.

   > ⓘ Remarque
   >
   > Pour planifier une analyse périodique, sélectionnez l'option *Paramètres de périodicité*.

5. Dans la liste de remplacements, sélectionnez les remplacements que vous souhaitez promouvoir en cochant les cases correspondantes à chaque remplacement.

   > ⓘ Remarque
   >
   > Vous pouvez rechercher des remplacements depuis la liste de remplacements à l'aide de mots-clés tels que le nom du remplacement, la dernière date de mise à jour, etc.
   >
   > Vous pouvez également filtrer les remplacements selon les paramètres suivants : Tous, Connexion, Qwaas, Crystal Report.
   >
   > De plus, vous pouvez trier les remplacements par ordre alphabétique.

6. Dans le volet *Destination*, sélectionnez le système de destination désiré dans le menu déroulant. Vous pouvez spécifier plusieurs systèmes de destination.

   > ⓘ Remarque
   >
   > Vous pouvez également choisir de vous connecter à un *Nouveau système*. Pour choisir un nouveau système en tant que système destination, procédez comme suit :
   > 1. Sélectionnez *Nouveau système* dans le menu déroulant.
   > La boîte de dialogue Identification de destination s'affiche.

2. Saisissez les références de connexion valides dans les champs *Système*, *Nom d'utilisateur*, *Mot de passe* et *Authentification*.
3. Sélectionnez *Connexion*.

Pour exporter les remplacements en tant que fichier LCMBIAR, procédez comme suit :

1. Sélectionnez Exporter en tant que fichier LCMBIAR dans le menu déroulant.
2. Sélectionnez *Exporter*.
   La boîte de dialogue *Paramètres d'exportation* apparaît.
3. Saisissez les références de connexion valides dans les champs correspondants.
4. Sélectionnez *Terminé*.

7. Sélectionnez *Promouvoir*.

   La boîte de dialogue Remplacements de destination s'affiche.

   > **Remarque**
   >
   > Par défaut, les systèmes de destination auxquels vous êtes actuellement connecté sont sélectionnés. Vous pouvez choisir de promouvoir sélectivement des remplacements vers un système de destination particulier en cochant la case correspondant au système de destination désiré.

8. Sélectionnez *Terminé*.

   La promotion des remplacements est terminée.

9. Connectez-vous au système de destination à l'aide de références de connexion valides.

   Une liste de tous les objets promus s'affiche dans une liste de connexions uniques. Le statut de ces objets est Inactif.

10. Sélectionnez *Mettre à jour* pour les objets que vous souhaitez modifier.

    La boîte de dialogue *Modifier les propriétés de connexion commune* s'affiche.

11. Mettez à jour les valeurs souhaitées et cliquez sur *Terminé*.

    Le statut des objets modifiés devient Actif.

    > **Remarque**
    >
    > Vous pouvez également activer une connexion en sélectionnant *Inactif*, sans besoin de modifier la connexion dans le système de destination.

12. Cliquez sur *Enregistrer*.

16.2.3.4.2 Pour promouvoir des remplacements à l'aide de fichiers BIAR

Ajoutez un système hôte avant de promouvoir les remplacements. Pour en savoir plus sur l'ajout des systèmes hôtes, voir Pour utiliser l'option Gérer les systèmes [page 607].

Pour promouvoir les remplacements par le biais de fichiers BIAR, procédez comme suit :

1. Dans la barre d'outils de l'espace de travail de gestion des promotions, cliquez sur l'option *Paramètres de remplacement*.

La fenêtre *Paramètres de remplacement* s'affiche.

2. Si vous êtes connecté au système central de la gestion des promotions, déconnectez-vous du système.
3. Cliquez sur *Connexion* pour vous connecter au système d'origine.
   La fenêtre *Se connecter au système* apparaît.
4. Dans l'écran *Paramètres de remplacement*, sélectionnez le système source signalé comme *Origine* pour analyser les objets et connectez-vous au système à l'aide de références de connexion valides.
5. Dans la liste déroulante *Démarrer* en regard de *Analyse*, sélectionnez l'option *Démarrer*.
   Le processus d'analyse démarre. La Liste de remplacement s'affiche.

   > **Remarque**
   >
   > Pour planifier une analyse périodique, sélectionnez l'option *Paramètres de périodicité* dans la liste déroulante.

6. Dans la liste de remplacement, remplacez le statut des objets par Actif et cliquez sur *Enregistrer*.
7. Cliquez sur *Promouvoir les remplacements*
   L'écran *Promouvoir les remplacements* apparaît où la liste des systèmes de destination s'affiche.
8. Pour crypter le fichier BIAR à l'aide d'un mot de passe, cliquez sur la case *Cryptage de mot de passe*.
   Les champs *Mot de passe* et *Confirmer le mot de passe* sont activés.
9. Saisissez un mot de passe dans le champ *Mot de passe*. Saisissez à nouveau le mot de passe dans le champ*Confirmer le mot de passe*.
10. Cliquez sur *Exporter* et enregistrez le fichier BIAR de remplacement dans un système de fichiers.
11. Connectez-vous au système de destination par le biais de la CMC et dans l'outil de gestion des promotions, cliquez sur *Importer* > *Remplacer le fichier*.
    La fenêtre *Importer le fichier LCMBIAR* apparaît.
12. Cliquez sur *Parcourir* pour rechercher le fichier BIAR.
13. Saisissez le mot de passe du fichier BIAR dans le champ *Mot de passe*.

    > **Remarque**
    >
    > Le champ *Mot de passe* n'apparaît que si le fichier BIAR que vous avez sélectionné est crypté à l'aide d'un mot de passe.

14. Cliquez sur *OK*. La promotion des remplacements est terminée.
15. Déconnectez-vous du système d'origine.
16. Dans l'écran *Paramètres de remplacement*, cliquez sur *Connexion*.
    La fenêtre *Se connecter au système* apparaît.
17. Connectez-vous au système de destination à l'aide de références de connexion valides.
    Une liste des objets importés s'affiche dans la Liste de remplacement. Le statut de ces objets est Inactif.
18. Cliquez sur la case *Sélectionner* des objets que vous souhaitez modifier, puis cliquez sur *Modifier*. Les objets modifiés sont indiqués par une icône.

    > **Remarque**
    >
    > Vous pouvez supprimer les objets de remplacement en cliquant sur l'icône.

19. Mettez à jour les valeurs souhaitées et cliquez sur *Terminé*.
    Le statut des objets modifiés devient Actif.
20. Cliquez sur *Enregistrer*.

16.2.3.4.3 Pour promouvoir des remplacements à l'aide de CTS+

Ajoutez un système hôte avant de promouvoir les remplacements. Pour en savoir plus sur l'ajout des systèmes hôtes, voir Pour utiliser l'option Gérer les systèmes [page 607].

Pour promouvoir les remplacements via CTS+, effectuez les étapes suivantes :

> **Remarque**
>
> Lancez l'outil de gestion des promotions à l'aide de l'authentification SAP pour que cette option soit disponible.

1. Dans la barre d'outils de l'espace de travail de gestion des promotions, cliquez sur l'option *Paramètres de remplacement*.
   La fenêtre *Paramètres de remplacement* s'affiche.
2. Si vous êtes connecté au système central de la gestion des promotions, déconnectez-vous du système.
3. Cliquez sur *Connexion* pour vous connecter au système d'origine.
   La fenêtre *Se connecter au système* apparaît.
4. Sélectionnez le système source signalé comme *Origine* pour analyser les objets et connectez-vous au système à l'aide de références de connexion valides.
5. Dans la liste déroulante *Démarrer* en regard de *Analyse*, sélectionnez l'option *Démarrer*.
   Le processus d'analyse démarre. La *Liste de remplacement* s'affiche.

   > **Remarque**
   >
   > Pour planifier une analyse périodique, sélectionnez l'option *Paramètres de périodicité* dans la liste déroulante.

6. Dans la liste de remplacement, modifiez le statut par Actif pour les objets que vous souhaitez promouvoir et cliquez sur *Enregistrer*.
7. Cliquez sur *Promouvoir les remplacements*
   L'écran *Promouvoir les remplacements* apparaît où la liste des systèmes de destination s'affiche.
8. Dans la liste déroulante *Options de promotion*, sélectionnez l'option *Promouvoir avec CTS+*.
9. Cliquez sur *Promouvoir*.
10. Libérez les remplacements vers le système de destination en procédant comme suit :
    a. Connectez-vous au contrôleur du domaine de CTS+ et ouvrez l'interface utilisateur Web de *Transport Organizer*. Pour en savoir plus sur l'utilisation de l'interface utilisateur Web de Transport Organizer, voir Transport Organizer Web UI.
    b. Si le statut de la demande est*Modifiable*, cliquez sur *Libérer* pour libérer la demande de transport des remplacements. Pour en savoir plus sur la libération de demandes de transport avec des objets non ABAP, voir Releasing Transport Requests with Non-ABAP Objects.
    c. Fermez l'interface utilisateur Web de *Transport Organizer*.
11. Importez les remplacements vers le système de destination en procédant comme suit :
    a. Connectez-vous au contrôleur de domaine de CTS+.
    b. Appelez la transaction STMS pour saisir le système de gestion du transport.
    c. Cliquez sur l'icône *Présentation de l'importation*.

L'écran *Présentation de l'importation* apparaît et vous pouvez voir ici les éléments de la file d'attente d'importation en provenance de tous les systèmes.

d. Cliquez sur l'ID système du système Gestion des promotions de destination.
Vous pouvez voir la liste des demandes de transport pouvant être importées dans le système.

e. Cliquez sur *Actualiser*.

f. Importez les demandes de transport appropriées. Pour en savoir plus, voir la documentation relative à Importing Requests.

12. La promotion des remplacements est terminée.
13. Connectez-vous au système de destination à l'aide de références de connexion valides.
Une liste de tous les objets promus s'affiche dans "Liste de remplacements". Le statut de ces objets est Inactif.
14. Cliquez sur la case *Sélectionner* des objets que vous souhaitez modifier, puis cliquez sur *Modifier*.
15. Mettez à jour les valeurs souhaitées et cliquez sur *Terminé*.
Le statut des objets modifiés devient Actif.
16. Cliquez sur *Enregistrer*.

16.2.3.5 Utilisation de l'option Paramètres CTS

Vous pouvez utiliser cette option pour ajouter des services Web et gérer les systèmes de BW dans votre infrastructure. Reportez-vous à la section Pour configurer les paramètres CTS+ dans l'outil de gestion des promotions [page 670] pour en savoir plus sur l'utilisation de l'option Paramètres CTS et sur la configuration de CTS pour être utilisé avec l'outil de gestion des promotions.

16.3 Utilisation de l'outil de gestion des promotions

Lorsque vous lancez l'outil de gestion des promotions, par défaut, vous êtes dirigé vers la page *Travaux de promotion*.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

L'écran de page d'accueil *Travaux de promotion* comprend divers onglets permettant d'effectuer les tâches suivantes :

- Cliquez sur *Nouveau travail* pour créer un travail. Vous pouvez également cliquer avec le bouton droit sur l'écran de page d'accueil et sélectionner *Nouveau travail* dans la liste.
- Cliquez sur *Importer* > *Importer le fichier* pour importer un fichier BIAR ou LCMBIAR directement depuis le système de fichiers au lieu d'effectuer la procédure complète de création d'un travail.
- Cliquez sur *Importer* > *Remplacer le fichier* pour importer des fichiers de remplacement.
- Sélectionnez un travail existant dans la liste, puis cliquez sur *Modifier* pour modifier le travail sélectionné.

- Sélectionnez un travail existant dans la liste, puis cliquez sur *Promouvoir* pour promouvoir le travail du système source vers le système de destination ou exporter le travail vers un fichier LCMBIAR.
- Sélectionnez un travail existant préalablement exécuté dans la liste, puis cliquez sur *Reprendre* pour reprendre les objets promus du système de destination.
- Sélectionnez un travail existant préalablement exécuté dans la liste, puis cliquez sur *Historique* pour visualiser les précédentes instances de promotion du travail.
- Sélectionnez un travail existant dans la liste, puis cliquez sur *Propriétés* pour visualiser les propriétés du travail sélectionné, telles que titre, ID, nom de fichier et description.

La zone d'application *Travaux de promotion* affiche la liste de travaux et dossiers existant dans le système ainsi que les informations suivantes pour chaque travail ou dossier :

- *Nom :* affiche le nom du travail ou dossier créé.
- *Statut :* affiche le statut du travail tel que Créé, Réussite, Réussite partielle, En cours d'exécution ou Échec.
- *Créé :* affiche la date et l'heure de la création du travail ou dossier.
- *Dernière exécution :* affiche la date et l'heure de la dernière promotion du travail.
- *Système source :* affiche le nom du système depuis lequel le travail est promu.
- *Système de destination :* affiche le nom du système vers lequel le travail est promu.
- *Auteur de la création :* affiche le nom de l'utilisateur qui a créé le travail ou le dossier en question.

> **Remarque**
>
> L'outil de gestion des promotions utilise le SDK de la plateforme de BI pour toutes ses activités.

16.3.1 Création et suppression de dossiers

Cette section décrit comment créer et supprimer un dossier dans la page d'accueil des travaux de promotion.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

16.3.1.1 Création d'un dossier

Cette section décrit comment créer un dossier.

Pour créer un dossier, procédez comme suit :

1. Dans la barre d'outils de la gestion des promotions, cliquez sur .
2. Dans la boîte de dialogue *Créer un dossier*, saisissez le nom du dossier.
3. Cliquez sur *OK*.

Un dossier est créé.

Informations associées

Permet de créer un travail [page 616]
Suppression d'un dossier [page 616]

16.3.1.2 Suppression d'un dossier

Cette section décrit comment supprimer un dossier.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour supprimer un dossier, procédez comme suit :

1. Sélectionnez un dossier dans la page d'accueil *Travaux de promotion*.
2. Cliquez sur .
   La boîte de dialogue de confirmation s'affiche.
3. Cliquez sur *OK*.

Le dossier sélectionné est supprimé.

Informations associées

Permet de créer un travail [page 616]

16.3.2 Permet de créer un travail

Cette section décrit le mode de création d'un travail à l'aide de l'outil degestion des promotions.

Le tableau suivant traite des éléments et champs de l'interface utilisateur que vous pouvez utiliser pour créer un travail :

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Champ	Description
Nom	Nom du travail que vous souhaitez créer.
Description	Description du travail que vous souhaitez créer.
Mots clés	Mots clés pour les contenus du travail que vous souhaitez créer.
Enregistrer le travail dans	Le dossier sélectionné par défaut s'affiche.
Système source	Nom du système de la plateforme de BI à partir duquel vous souhaitez promouvoir un travail.
Système de destination	Nom du système de la plateforme de BI vers lequel vous souhaitez promouvoir un travail.
Nom d'utilisateur	ID de connexion que vous devez utiliser pour vous connecter au système source ou destination.
Mot de passe	Mot de passe que vous devez utiliser pour vous connecter au système source ou destination.
Authentification	Type d'authentification utilisé pour se connecter au système source ou destination. L'outil de gestion des promotions prend en charge les types d'authentification suivants : • Enterprise • Windows AD • LDAP • SAP

> **Remarque**
>
> Avant de procéder à la création d'un travail, assurez-vous que les remplacements, le cas échéant, ont été modifiés et mis à jour dans le système de destination, afin que le contenu de la plateforme de BI soit automatiquement mis à jour. Pour plus d'informations, voir Utilisation de l'option Remplacer les options.

Pour créer un travail à l'aide de l'outil de gestion de la promotion, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
2. Dans la page d'accueil *Travaux de promotion*, cliquez sur *Nouveau travail*.
3. Saisissez le nom, la description et les mots clés du travail dans les champs appropriés.

   > **Remarque**
   >
   > Il n'est pas obligatoire de fournir des informations pour les champs Description, Mots clés et Système de destination.

4. Dans le champ *Enregistrer le travail dans*, recherchez le dossier dans lequel vous voulez enregistrer le travail et sélectionnez-le.

   > **Remarque**
   >
   > Le champ *Enregistrer le travail dans* contient par défaut le nom du dossier mis en surbrillance dans le volet des dossiers avant de cliquer sur *Nouveau travail*.

5. Sélectionnez les systèmes source et destination dans les listes déroulantes respectives.

Si le nom du système ne se trouve pas dans la liste déroulante, cliquez sur l'option *Se connecter à un nouveau CMS*. Une nouvelle fenêtre apparaît. Saisissez le nom du système ainsi que le nom d'utilisateur et le mot de passe.

6. Cliquez sur *Créer*.
   La fenêtre « Ajouter des objets » s'affiche.
7. Sélectionnez les objets du système source à ajouter au travail, puis cliquez sur *Ajouter et fermer*.
8. Cliquez sur *Enregistrer*.

Le travail récemment créé est stocké dans le référentiel du CMS du système source.

> ⓘ Remarque
>
> Si vous créez un travail en tant qu'objet principal et qu'il s'agit d'un travail périodique, celui-ci comprendra tout contenu ajouté au dossier lors de la prochaine exécution.

Informations associées

Utilisation de l'option Remplacer les options [page 609]

16.3.2.1 Pour se connecter à un nouveau CMS

Cette section décrit comment se connecter à un nouveau CMS.

> ⓘ Remarque
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour vous connecter à un nouveau CMS, procédez comme suit

1. Lancez l'application de gestion des promotions.
2. Créez un travail.
   Pour en savoir plus sur la création d'un travail, voir Permet de créer un travail [page 616].
3. Dans la liste déroulante *Système source*, sélectionnez *Connexion à un nouveau CMS*.
   La boîte de dialogue *Se connecter au système* apparaît.
4. Sélectionnez le système dans la liste déroulante ou saisissez un nouveau nom.
5. Saisissez les références de connexion de l'utilisateur, sélectionnez le type d'authentification approprié et cliquez sur *Connexion*.
6. Dans la liste déroulante *Système de destination*, sélectionnez *Connexion à un nouveau CMS*.
7. Sélectionnez le système dans la liste déroulante ou saisissez un nouveau nom.
8. Saisissez les références de connexion de l'utilisateur, sélectionnez le type d'authentification approprié et cliquez sur *Connexion*.

Informations associées

Pour modifier un travail [page 620]
Pour ajouter un InfoObject à un travail [page 621]
Promotion d'un travail quand les référentiels sont connectés [page 624]
Pour planifier une promotion de travail [page 630]

16.3.3 Pour créer un travail en copiant un travail existant

Cette section décrit comment créer un travail en copiant un travail existant.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour créer un travail en copiant un travail existant, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
2. Dans la page d'accueil *Travaux de promotion*, cliquez sur *Nouveau travail*.
3. Cliquez sur l'option *Copier un travail existant*.
   La fenêtre *Copier un travail existant* apparaît et affiche la liste des travaux dans le dossier *Travaux de promotion*.
4. Sélectionnez le travail souhaité dans la liste et cliquez sur *Créer*.
   Le nom, la description et les mots clés du travail ainsi que les champs *Enregistrer le travail dans* et *Destination* s'affichent. Vous pouvez modifier ces champs si nécessaire.
5. Dans le champ *Enregistrer le travail dans*, parcourez et sélectionnez le dossier dans lequel vous souhaitez enregistrer le travail, puis cliquez sur *Créer*.

Un travail est créé et la page *Ajouter des objets* apparaît.

Informations associées

Pour ajouter un InfoObject à un travail [page 621]
Pour modifier un travail [page 620]
Promotion d'un travail quand les référentiels sont connectés [page 624]

16.3.4 Pour rechercher un travail

La fonctionnalité de recherche de l'outil de gestion de la promotion permet de localiser un travail dans le référentiel.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour rechercher un travail, procédez comme suit :

1. Dans le champ *Rechercher* de la page d'accueil, saisissez le texte que vous souhaitez localiser.
2. Cliquez sur la liste qui apparaît à côté du champ *Rechercher* pour préciser les paramètres de recherche. Vous pouvez préciser les paramètres de recherche suivants :
   - *Rechercher par titre* Cette option permet de rechercher un travail par son nom.
   - *Rechercher par mot clé* Cette option permet de rechercher un travail par ses mots clés.
   - *Rechercher par description* Cette option permet de rechercher un travail par sa description.
   - *Rechercher dans tous les champs* Cette option permet de rechercher un travail par son titre, ses mots clés et sa description.
3. Cliquez sur l'icône Rechercher.

Informations associées

Pour ajouter un InfoObject à un travail [page 621]
Pour modifier un travail [page 620]

16.3.5 Pour modifier un travail

Cette section décrit comment modifier un travail.

> **Remarque**
>
> - Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.
> - Modifier un travail ne revient pas à créer un travail.

Pour modifier un travail, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
2. Dans la page d'accueil *Travaux de promotion*, sélectionnez le travail que vous souhaitez modifier.
3. Cliquez sur *Modifier*.
   Les détails relatifs au travail sélectionné s'affichent. En fonction de vos besoins, vous pouvez ajouter ou supprimer des InfoObjects, gérer les dépendances ou promouvoir le travail.

Vous ne pouvez pas changer le nom du système source lors de la modification d'un travail.

Informations associées

Pour ajouter un InfoObject à un travail [page 621]
Promotion d'un travail quand les référentiels sont connectés [page 624]
Pour planifier une promotion de travail [page 630]

16.3.6 Pour ajouter un InfoObject à un travail

Chaque travail doit contenir un jeu d'InfoObjects. Vous devez donc ajouter des InfoObjects à un travail avant de le promouvoir vers le système de destination.

> **Remarque**
>
> - Lorsque vous promouvez un rapport Crystal basé sur des InfoObjects Vue d'entreprise (connexion de données, fondation de données, éléments d'entreprise et vue d'entreprise), vous pouvez inclure des informations de sécurité (droit DataAccess sur la connexion de données et droit ViewDataField sur la fondation de données et les éléments d'entreprise) afin de voir les données d'un rapport sur le système de destination.
> - Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour ajouter un InfoObject à un travail, procédez comme suit :

1. Lancez l'outil de gestion des promotions.
2. Créez un travail ou modifiez un travail existant.
   Pour en savoir plus sur la création d'un travail, voir Permet de créer un travail [page 616] et Pour modifier un travail [page 620].
3. Cliquez sur *Ajouter des objets* en cas de modification d'un travail.

   > **Remarque**
   >
   > La boîte de dialogue *Ajouter des objets* s'affiche lors de la création d'un travail.

4. Accédez au dossier dans lequel vous voulez sélectionner l'objet.
   La liste des InfoObjects du dossier sélectionné s'affiche.
5. Sélectionnez l'InfoObject que vous voulez ajouter au travail et cliquez sur *Ajouter*.

   Si vous souhaitez ajouter un InfoObject et fermer la boîte de dialogue « Ajouter des objets à partir du système : `<NOM>` », cliquez sur *Ajouter et fermer*. L'InfoObject est ajouté au travail et la boîte de dialogue se ferme.

Après avoir ajouté un InfoObject à un travail, vous pouvez cliquer avec le bouton droit sur la page *Visualiseur de travail* et sélectionner les processus de promotion pour effectuer la tâche de promotion. Il est possible de gérer les objets dépendants des InfoObjects que vous avez sélectionnés à l'aide de l'option *Gérer les dépendances* de la page *Visualiseur de travail*.

> **Remarque**
>
> - Le Panier, qui apparaît sur le panneau de gauche de la page *Visualiseur de travail*, affiche le travail ainsi que ses objets dépendants sous forme d'arborescence.
> - Après avoir ajouté les InfoObjects, cliquez sur l'option *Enregistrer* pour enregistrer les modifications. Dans le cas contraire, l'utilisateur a la possibilité d'enregistrer le travail lorsqu'il ferme l'onglet.

Meilleures pratiques : SAP BusinessObjects recommande de sélectionner un petit nombre d'InfoObjects n'excédant pas 100 à la fois afin d'obtenir un rendement maximal de l'outil de gestion des promotions.

Informations associées

Pour gérer les dépendances d'un travail [page 622]
Promotion d'un travail quand les référentiels sont connectés [page 624]
Pour planifier une promotion de travail [page 630]

16.3.7 Pour gérer les dépendances d'un travail

Cette section décrit comment gérer les objets dépendants d'un InfoObject.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour gérer les objets dépendants d'un InfoObject, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
2. Créez un travail ou modifiez un travail existant.
   Pour en savoir plus sur la création d'un travail, voir Permet de créer un travail [page 616] et Pour modifier un travail [page 620].
3. Ajoutez les InfoObjects requis au travail, puis fermez la boîte de dialogue *Ajouter des objets* pour revenir à la fenêtre *Visualiseur de travail*.
4. Cliquez sur *Gérer les dépendances*.
   La fenêtre *Gérer les dépendances* s'affiche. Cette fenêtre affiche la liste des InfoObjects et de leurs objets dépendants. Pour afficher uniquement les objets dépendants qui n'ont pas été sélectionnés, cochez la case *Afficher les objets dépendants non sélectionnés*.
5. Dans la liste déroulante *Sélectionner les objets dépendants*, sélectionnez les options pour ajouter les objets dépendants au travail. Les objets dépendants ne sont pas sélectionnés par défaut ; vous devez sélectionner expressément les objets dépendants que vous souhaitez promouvoir.

   Par exemple, si vous sélectionnez *Tous les univers* dans la liste déroulante *Sélectionner les objets dépendants*, tous les univers inclus dans la liste des objets dépendants seront alors sélectionnés. Vous pouvez également sélectionner les objets dépendants individuellement.

Vous pouvez cliquer sur le *Type* pour visualiser les options de filtrage prises en charge pour les InfoObjects. Une liste déroulante s'affiche. Cette liste affiche les options de filtrage prises en charge. Sélectionnez l'option de filtrage et cliquez sur *OK*. Les InfoObjects filtrés sont affichés.

Lorsque vous sélectionnez les objets dépendants dans la colonne *Objets dépendants* puis cliquez sur *Appliquer les modifications*, ceux-ci sont automatiquement déplacés vers la colonne *Objets dans le travail*.

Vous pouvez également saisir le nom de l'objet dépendant dans le champ *Rechercher les objets dépendants* pour rechercher un objet dépendant.

Pour en savoir plus sur la recherche d'objets dépendants, voir Pour rechercher des objets dépendants [page 623].

6. Cliquez sur *Appliquer les modifications* pour mettre à jour la liste des objets dépendants et cliquez sur *Appliquer les modifications et fermer* pour enregistrer les modifications.

Les objets dépendants sont automatiquement calculés par l'outil. Ces objets dépendants sont générés en fonction des relations d'InfoObject ou des propriétés d'InfoObject. Les autres objets dépendants ne sont pas générés dans cette version de l'outil.

> **Remarque**
>
> Si vous sélectionnez un dossier pour promotion, les contenus du dossier sélectionné sont alors considérés comme ressources principales.

Informations associées

Promotion d'un travail quand les référentiels sont connectés [page 624]

16.3.8 Pour rechercher des objets dépendants

La fonctionnalité de recherche avancée de l'outil de gestion de la promotion permet de localiser les objets dépendants d'InfoObjects dans le référentiel.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour rechercher les objets dépendants d'un InfoObject, procédez comme suit :

1. Lancez la gestion de la promotion.
2. Créez un travail ou modifiez un travail existant.
   Si vous avez créé un travail, ajoutez-y les InfoObjects. Si vous modifiez un travail existant, vous pouvez ajouter des objets si nécessaire.
3. Cliquez sur *Gérer les dépendances*.
4. Dans le champ *Rechercher les objets dépendants*, saisissez le nom de l'objet dépendant que vous souhaitez localiser.

5. Cliquez sur l'icône Rechercher.

Informations associées

Pour gérer les dépendances d'un travail [page 622]

16.3.9 Promotion d'un travail quand les référentiels sont connectés

Cette section décrit comment promouvoir un travail à partir du système source vers le système de destination si les deux systèmes sont connectés.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Le tableau suivant répertorie les types d'InfoObjects pouvant être promus au moyen de l'outil de gestion des promotions :

Catégorie	Types d'objets que vous pouvez promouvoir
Rapports	Rapports Crystal, Web Intelligence, QaaWS, Lumira
Objets tiers	Texte enrichi, document texte, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Flash, Adobe Acrobat
Utilisateurs	Utilisateurs et groupes d'utilisateurs
Serveur	Groupes de serveurs
Plateforme de Business Intelligence	Dossier, Programme, Evénements, Profils, Lot d'objets, Lien hypertexte, Catégories, Boîte de réception, dossiers Personnel et Favoris
Univers, Espace de travail, Ensembles	Univers UNV, Connexions, Ensembles
Tableau de bord EPM	Univers, Connexions, Rapports et Analyses
Vue d'entreprise	Fondation de données
Fédération • Liste de réplication • Travaux de réplication	La liste de réplication promeut les objets suivants : Flash, .txt, Discussions, .pdf, Lien hypertexte, .xls, Lot d'objets, rapports Crystal Reports, Documents Web Intelligence, Univers, Programme, Connexions, Fondation de données, Vues d'entreprise, .rtf, Profil, Événement, Utilisateurs et Groupes d'utilisateurs. Les connexions de réplication promeuvent les Travaux de réplication, la Connexion distante, les Publications, la Discussion, la Connexion Pioneer
Services BI	Documents Web Intelligence, Univers et Connexions

Catégorie	Types d'objets que vous pouvez promouvoir
Nouveaux InfoObjects	Rapports Crystal (rpt/rptr), Pioneer, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Foundation (DFX), WebI, Data Federator, Data Steward, Espace de travail BI, etc.
Clients	L'outil de gestion des promotions prend en charge la promotion des clients (avec leurs dépendances) du système source au système de destination en fournissant des options pour sélectionner et ajouter des clients et en faisant correspondre les objets client à un travail. Une relation entre les clients et les objets client correspondant en tant que dépendance est ainsi établie. Cette fonction est disponible dans les modes GUI et CLI de la gestion des promotions.

Commentaires BI est pris en charge par l'outil de gestion des promotions. Lors de la promotion d'un document avec des commentaires, les commentaires du document sont également migrés du système source au système de destination (Live vers Live, Live vers BIAR, BIAR vers Live). Pour promouvoir un document avec des commentaires, sélectionnez *Promouvoir* > *Paramètres de commentaires* et cochez la case *Inclure commentaires*.

> **Remarque**
>
> Par défaut, la case *Inclure commentaires* n'est pas cochée.

Lorsque vous promouvez des objets répliqués, les informations spécifiques de la réplication associées aux objets sont elles aussi promues du système source au système de destination (Live vers Live, Live vers BIAR, BIAR vers Live). Pour promouvoir un document sans les informations spécifiques de la réplication, sélectionnez *Promouvoir* > *Paramètres des travaux de fédération* et désélectionnez la case à cocher *Inclure la relation des travaux de fédération*.

> **Remarque**
>
> Par défaut, la case à cocher *Inclure la relation des travaux de fédération* est sélectionnée.

Pour promouvoir un travail, procédez comme suit :

1. Lancez la gestion de la promotion.
2. Dans la page d'accueil *Travaux de promotion*, sélectionnez le travail que vous souhaitez promouvoir. Vous pouvez également cliquer avec le bouton droit de la souris sur l'écran de page d'accueil, puis cliquer sur *Promouvoir*.
3. Dans la liste du système de *Destination*, sélectionnez un autre système de destination selon vos besoins.

   > **Remarque**
   >
   > Assurez-vous de vous être connecté aux systèmes source et de destination avant d'entamer le processus de promotion.

4. Dans le champ *ID de gestion des modifications*, saisissez la valeur appropriée et cliquez sur *Enregistrer*.

   > **Remarque**
   >
   > L'ID de gestion des modifications est utilisé pour obtenir des informations relatives à la connexion, l'audit, l'historique de travail. L'outil de gestion de la promotion permet de mapper chaque instance de création de travail à un ID de gestion des modifications. Ce dernier est un attribut défini par l'utilisateur

> dans la définition de travail lors de la création d'un travail. L'outil génère automatiquement un ID pour chaque travail.

5. Sélectionnez *Paramètres de sécurité*, si nécessaire. Les options suivantes s'affichent :
   - *Ne pas promouvoir la sécurité* : il s'agit de l'option par défaut.
   - *Promouvoir la sécurité* : utilisez cette option pour promouvoir des travaux et les droits de sécurité associés.
   - *Promouvoir la sécurité des objets* : utilisez cette option pour promouvoir la sécurité des objets et des dossiers.
   - *Promouvoir la sécurité des utilisateurs* : utilisez cette option pour promouvoir les droits des utilisateurs faisant partie du travail.
   - *Inclure les droits d'application* : vous ne pouvez sélectionnez cette option que lorsque vous avez sélectionné *Promouvoir la sécurité*. Si les objets du travail héritent de droits d'application, le travail est promu avec ces droits.
   - *Promouvoir la sécurité de niveau supérieur* : cette option permet de promouvoir les droits de sécurité de niveau supérieur.

     > ⚠ Attention
     >
     > L'option *Promouvoir la sécurité de niveau supérieur* écrase les droits de sécurité de niveau supérieur sur le système cible.

   Vous pouvez aussi cliquer sur *Afficher la sécurité* pour visualiser les dépendances de sécurité d'InfoObjects dans le travail.

   > ⓘ Remarque
   >
   > Le bouton *Afficher les droits* est désactivé jusqu'à ce que vous enregistriez le nouveau travail.

6. Cliquez sur *Enregistrer*.

   Le bouton *Afficher les droits* est activé. Vous pouvez désormais voir les dépendances de sécurité.

7. Cliquez sur *Tester la promotion* pour vérifier qu'il n'y a pas de conflit entre les CUID d'InfoObjects des systèmes source et destination. Les détails de la promotion sont affichés sous les onglets *Réussite*, *Echec* et *Avertissement*. La première colonne affiche les objets à promouvoir et la seconde le statut de promotion de chaque InfoObject. L'outil de gestion de la promotion classe les objets sélectionnés en utilisateurs, groupes, univers.

   > ⓘ Remarque
   >
   > Cette fonctionnalité n'implique la promotion d'aucun InfoObject.

   Le résultat d'un test de promotion peut être l'un des suivants :
   - `Remplacé` : l'InfoObject du système de destination est remplacé par l'InfoObject du système source.
   - `Copié` : l'InfoObject du système source est copié vers le système de destination.
   - `Abandonné` : l'InfoObject n'est pas promu du système source vers le système de destination.
   - `Avertissement` : l'InfoObject du système de destination est la nouvelle version et vous pouvez supprimer l'InfoObject du travail. Cependant, si vous le souhaitez, l'InfoObject sera promu.
   - `Mappé` : l'InfoObject est mappé à un InfoObject sur le système de destination.

8. Cliquez sur *Planifier* si vous souhaitez que la promotion soit exécutée à un moment donné ou périodiquement.

9. Cliquez sur *Promouvoir*.
   Le travail sélectionné est promu.

Si vous ne voulez pas promouvoir le travail, vous pouvez utiliser l'option *Enregistrer* pour enregistrer les modifications telles que les paramètres de Sécurité, ID de gestion des modifications et Planification.

16.3.10 Promotion d'un travail à l'aide d'un fichier LCMBIAR

La promotion est l'activité de transfert d'une ressource de Business Intelligence d'un référentiel vers un autre. Si le système source et le système de destination sont sur le même réseau, l'outil de gestion des promotions utilise le WAN ou le LAN pour promouvoir l'InfoObject. Cependant, l'outil de gestion des promotions permet aussi la promotion d'InfoObjects même si les systèmes source et de destination ne sont pas sur le même réseau.

Dans des scénarios où les systèmes source et de destination ne sont pas sur le même réseau, l'outil de gestion des promotions prend en charge la promotion de travaux dans le système de destination en permettant d'exporter le travail du système source vers un fichier LCMBIAR et d'importer le travail du fichier BIAR vers le système de destination.

Cette section décrit comment exporter un travail vers un fichier LCMBIAR et importer ensuite le travail du fichier BIAR vers le système de destination.

> ⓘ Remarque
>
> - Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.
> - Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, voir 3350454.

Informations associées

Exportation d'un travail vers un fichier LCMBIAR [page 627]
Importation d'un travail depuis un fichier LCMBIAR [page 628]

16.3.10.1 Exportation d'un travail vers un fichier LCMBIAR

Cette section explique comment exporter un travail vers un fichier LCMBIAR.

Pour exporter un travail vers un fichier LCMBIAR, procédez comme suit :

1. Lancez l'outil de gestion des promotions et créez un travail.
   Pour en savoir plus sur la création d'un travail, voir Permet de créer un travail [page 616]

2. Dans la liste déroulante *Destination*, sélectionnez l'option *Sortie vers le fichier LCMBIAR* et cliquez sur *Créer*.
3. Cliquez sur *Ajouter des objets* pour ajouter des InfoObjects au travail.

   Vous pouvez utiliser l'option *Gérer les dépendances* pour gérer les dépendances du travail sélectionné.
4. Pour crypter le fichier LCMBIAR à l'aide d'un mot de passe, cliquez sur la case *Cryptage de mot de passe*.
5. Saisissez un mot de passe dans le champ *Mot de passe*.
6. Confirmez le mot de passe dans le champ *Vérifier le mot de passe*.
7. Cliquez sur *Promouvoir*.
   La fenêtre *Promouvoir* s'affiche.
8. Modifiez les options de sécurité selon vos besoins, puis cliquez sur *Exporter*.
   Le fichier LCMBIAR est créé. Vous pouvez enregistrer un fichier LCMBIAR dans le système de fichiers.
9. (Facultatif) Cliquez sur *Destination fichier LCMBiar*, puis sélectionnez *FTP* ou *SFTP* pour exporter le fichier LCMBIAR respectivement vers un serveur FTP ou SFTP. Saisissez les valeurs des champs Nom d'hôte, Port, Nom d'utilisateur, Mot de passe, Répertoire et Nom de fichier, puis cliquez sur *Exporter*.

   > **Remarque**
   >
   > Si vous choisissez comme *Destination de fichier LCMBiar* le *SFTP*, vous devez saisir par ailleurs l'empreinte SFTP.
10. Dans la liste déroulante *Destination*, sélectionnez *Sortie vers le fichier LCMBIAR* et cliquez sur *Destination fichier LCMBiar*.

Vous pouvez planifier l'exportation d'un travail vers un fichier LCMBIAR. Pour en savoir plus, voir la section Pour planifier une promotion de travail [page 630].

Informations associées

Pour ajouter un InfoObject à un travail [page 621]
Pour gérer les dépendances d'un travail [page 622]

16.3.10.2 Importation d'un travail depuis un fichier LCMBIAR

Il est possible d'importer un travail depuis un fichier LCMBIAR. Le fichier LCMBIAR est copié du périphérique de stockage vers le système de destination.

Pour importer un fichier LCMBIAR, procédez comme suit :

1. Lancez l'outil de gestion des promotions.
2. Sur la page d'accueil *Travaux de promotion*, cliquez sur *Importer* > *Fichier d'importation*.
   La fenêtre *Importer à partir du fichier* apparaît.
3. Vous pouvez importer un fichier BIAR à partir d'un système de fichiers ou d'un serveur FTP ou SFTP.
   - Pour importer un fichier BIAR à partir d'un système de fichiers, procédez comme suit :
     1. Sélectionnez *Système de fichiers*.

2. Cliquez sur *Parcourir* et sélectionnez un fichier LCMBIAR dans le système de fichiers.
3. Dans le champ *Mot de passe*, saisissez le mot de passe du fichier LCMBIAR.

> **Remarque**
>
> Le champ Mot de passe n'apparaît que si le fichier LCMBIAR est crypté à l'aide d'un mot de passe.

4. Cliquez sur *Créer*. Le travail est créé.

> **Remarque**
>
> Si un travail portant le même nom existe, le menu contextuel Confirmer l'enregistrement apparaît. Cliquez sur "Oui" pour écraser le travail existant ou sur "Non" pour créer un travail avec un nouveau nom : `jobname_copy<DATE_ET_HEURE_ACTUELLES>`.

- Pour importer un fichier LCMBIAR à partir d'un serveur FTP, procédez comme suit :
  1. Sélectionnez *FTP*.
  2. Saisissez les détails appropriés dans les champs Hôte, Port, Nom d'utilisateur, Mot de passe, Répertoire et Nom de fichier, puis cliquez sur *OK*
- Pour importer un fichier LCMBIAR à partir d'un serveur SFTP, procédez comme suit :
  1. Sélectionnez *SFTP*.
  2. Saisissez les détails appropriés dans les champs Hôte, Port, Nom d'utilisateur, Mot de passe, Répertoire, Empreinte et Nom de fichier, puis cliquez sur *OK*.

4. Cliquez sur *Promouvoir*.
   La fenêtre *Promouvoir - Nom du travail* apparaît.
5. Dans la liste déroulante *Destination*, sélectionnez le système de destination. Si vous sélectionnez *Connexion à un nouveau CMS*, vos références de connexion vous seront demandées. Confirmez les références de connexion du système de destination.
6. Cliquez sur *Promouvoir* pour promouvoir les contenus vers le système de destination.

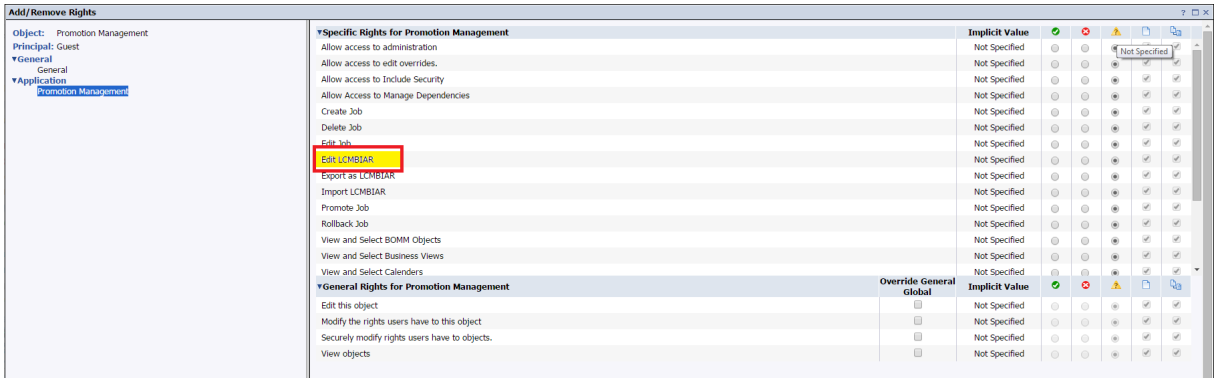
   Vous pouvez également cliquer sur l'option *Tester la promotion* pour visualiser les objets à promouvoir et le statut de promotion.
7. **Facultatif :** Si vous importez un document Web Intelligence qui utilise la personnalisation, dans l'onglet *Préférences BI des groupes d'utilisateurs*, assurez-vous de cocher la case *Écraser les préférences BI des groupes d'utilisateurs* pour importer la personnalisation.

Informations associées

Pour gérer les dépendances d'un travail [page 622]

16.3.10.2.1 Extraction sélective d'objet d'un fichier LCMBIAR

Pour extraire de façon sélective des objets d'un fichier LCMBIAR, il est nécessaire que l'utilisateur dispose du droit de *modification LCMBIAR*.



Pour extraire de façon sélective des objets d'un fichier LCMBIAR, procédez comme suit :

1. Sélectionnez les objets à promouvoir.
2. Cliquez sur *Promouvoir*.

> **Remarque**
>
> - Un nouveau travail avec les objets sélectionnés est créé.
> - Vous pouvez effectuer la même opération en utilisant l'outil de ligne de commande. Pour en savoir plus, voir Paramètres de l'outil de commande [page 643]
> - La promotion sélective n'est pas prise en charge pour le scénario Live vers Live.

16.3.11 Pour planifier une promotion de travail

Cette section décrit comment planifier la promotion d'un travail. Elle décrit également comment spécifier les paramètres et options de périodicité.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour planifier la promotion d'une instance de travail, procédez comme suit :

1. Dans la boîte de dialogue *Promouvoir*, cliquez sur l'option *Planifier*.
2. Définissez l'option de planification requise et cliquez sur *Planifier*.

Si vous ajoutez des InfoObjects à un dossier contenu dans un travail après la planification du travail pour la promotion, ils seront également promus vers la destination à l'heure planifiée. Cependant, ce n'est pas le cas lorsque vous essayez de planifier une promotion de travail à l'aide d'un fichier LCMBIAR, puisque LCMBIAR n'est pas considéré comme une destination réelle.

> **→ Conseil**
>
> Une fois la promotion du travail terminée, vous pouvez visualiser toutes les instances du travail en sélectionnant le travail dans la page *Travaux de promotion* et en cliquant sur *Historique* dans la barre d'outils.

La promotion d'un travail peut également s'effectuer en fonction de déclenchements d'événements.

Vous pouvez sélectionner des notifications par courrier électronique en fonction du statut de la promotion du travail (tel que réussite/réussite partielle/échec). Pour obtenir des informations détaillées sur les différentes options de planification et la configuration des notifications, voir la section Planification.

Informations associées

Exportation d'un travail vers un fichier LCMBIAR [page 627]

16.3.11.1 Pour mettre à jour les instances de promotion de travail périodiques et en suspens

L'outil de gestion des promotions permet de suivre le statut des instances de promotion de travail et de les replanifier à l'aide de l'option *Instances périodiques et en suspens*.

Pour ce faire, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
2. Dans la page d'accueil *Travaux de promotion*, sélectionnez un travail.
3. Cliquez sur *Historique*.
   La fenêtre *Historique de travail* s'affiche.
4. Cliquez sur *Instances périodiques et en suspens*.
   La fenêtre *Historique de travail pour instances périodiques et en suspens* apparaît. Cette fenêtre affiche la liste des instances de promotion de travail périodiques et en suspens.

   Vous pouvez utiliser les options suivantes selon vos besoins :
   - Cliquez sur *Instances promues* pour afficher la liste des instances de promotion de travail.
   - Cliquez sur *Suspendre* pour suspendre l'instance périodique ou en suspens sélectionné.
   - Cliquez sur l'option *Reprendre* pour reprendre l'instance planifiée de promotion de travail suspendue.
   - Cliquez sur l'option *Replanifier* pour replanifier l'instance de promotion de travail sélectionnée.
   - Cliquez sur pour supprimer une instance planifiée de promotion de travail.
   - Cliquez sur pour actualiser le statut d'une instance planifiée de promotion de travail.
   - Vous pouvez utiliser l'option

     pour naviguer dans une seule page ou vers une page précise en saisissant le numéro de page.

> **Remarque**
>
> La colonne de statut de la fenêtre *Historique de travail pour instances périodiques et en suspens* affiche le statut de l'instance de promotion de travail, à savoir périodique, en suspens, etc.

Informations associées

Pour reprendre un travail [page 632]

16.3.12 Pour afficher l'historique d'un travail

Cette section décrit comment visualiser l'historique d'un travail.

> **Remarque**
>
> Pour visualiser l'historique d'un travail, assurez-vous que le statut du travail est l'un des suivants :
>
> - Réussite
> - Echec
> - Réussite partielle

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour visualiser l'historique d'un travail, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
   La page d'accueil *Travaux de promotion* s'affiche.
2. Sélectionnez le travail dont vous voulez afficher l'historique puis cliquez sur l'onglet *Historique*.

   L'heure de l'instance de travail, le nom du travail, le nom des systèmes source et destination, l'ID de l'utilisateur qui a promu le travail et le statut (Réussite, Echec ou Réussite partielle) du travail s'affichent.

   Vous pouvez visualiser le statut détaillé du travail en utilisant le lien affiché dans la colonne *Statut*.

16.3.13 Pour reprendre un travail

L'option Reprise permet de restaurer le système de destination à son statut précédent après la promotion d'un travail.

> **Remarque**
>
> Des améliorations de sécurité ont été implémentées dans l'outil de gestion des promotions, entraînant des modifications de certains comportements lors de l'exécution d'actions. Pour en savoir plus, reportez-vous à 3350454.

Pour reprendre un travail, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
   La page d'accueil *Travaux de promotion* s'affiche.

2. Exécutez une des opérations suivantes :
   - Cliquez avec le bouton droit sur le travail que vous souhaitez reprendre et sélectionnez *Reprise*.
   - Sélectionnez le travail que vous souhaitez reprendre et cliquez sur l'onglet *Reprise*.

   La fenêtre *Reprise* s'affiche.
3. Sélectionnez l'instance que vous souhaitez reprendre et cliquez sur *Exécuter la reprise*.
   L'instance est reprise.

Vous ne pouvez reprendre que l'instance la plus récente d'une promotion de travail. Il est impossible de reprendre simultanément plusieurs instances de travail.

16.3.13.1 Pour utiliser l'option Reprise partielle

L'outil de gestion des promotions permet de reprendre des InfoObjects d'un travail complètement ou partiellement depuis le système de destination.

Pour reprendre partiellement des InfoObjects, procédez comme suit :

1. Lancez l'outil de gestion de la promotion.
   La page d'accueil *Travaux de promotion* s'affiche.
2. Exécutez une des opérations suivantes :
   - Cliquez avec le bouton droit sur le travail que vous souhaitez reprendre et sélectionnez *Reprise*.
   - Sélectionnez le travail que vous souhaitez reprendre et cliquez sur l'onglet *Reprise*.

   La fenêtre *Reprise* s'affiche.
3. Sélectionnez l'instance dans la liste et cliquez sur *Reprise partielle*.

   La liste d'InfoObjects du travail sélectionné s'affiche dans la page *Visualiseur de travail*.
4. Sélectionnez les InfoObjects que vous souhaitez reprendre et cliquez sur *Reprise*.

> **Remarque**
>
> Assurez-vous d'avoir repris tous les InfoObjects d'une instance avant de reprendre les InfoObjects de l'instance suivante.

> **Attention**
>
> Si un travail est promu avec sécurité, la sécurité des InfoObjects dépendants sélectionnés pourrait alors ne pas être restaurée à son statut précédent lors de la reprise partielle des InfoObjects.

Informations associées

Gestion de différentes versions de ressources BI [page 696]

16.3.13.2 Pour reprendre un travail après expiration du mot de passe

Cette section décrit comment reprendre un travail après expiration du mot de passe utilisé pour sa promotion.

Pour reprendre un travail après expiration du mot de passe, procédez comme suit :

1. Sélectionnez le travail que vous souhaitez reprendre et cliquez sur *Reprise*.
2. Dans la fenêtre *Reprise*, sélectionnez *Reprise complète*.
   Un message d'erreur s'affiche. Ce message indique que le travail ne peut pas être repris. Vous êtes également invité à vous connecter au système source ou de destination.
3. Saisissez vos nouvelles références de connexion et cliquez sur *Connexion*.

Une boîte de dialogue s'affiche et indique que le processus de reprise est terminé.

> ⓘ Remarque
>
> Les travaux qui étaient promus au moyen des références de connexion du système source ou destination sont automatiquement mis à jour.

Informations associées

Pour reprendre partiellement des InfoObjects après expiration du mot de passe [page 634]
Pour utiliser l'option Reprise partielle [page 633]

16.3.13.2.1 Pour reprendre partiellement des InfoObjects après expiration du mot de passe

Cette section décrit comment reprendre partiellement des InfoObjects après expiration du mot de passe du système source ou destination.

Pour reprendre partiellement des InfoObjects après expiration du mot de passe, procédez comme suit :

1. Sélectionnez le travail que vous souhaitez reprendre et cliquez sur *Reprise*.
   La fenêtre *Reprise* s'affiche.
2. Sélectionnez l'option *Reprise partielle*.
   Un message d'erreur s'affiche. Ce message indique que les InfoObjects ne peuvent pas être repris. Vous êtes également invité à vous connecter au système source ou de destination.
3. Saisissez vos nouvelles références de connexion et cliquez sur *Connexion*.
   La page *Visualiseur de travail* s'affiche. Cette page affiche la liste des InfoObjects.
4. Sélectionnez les InfoObjects requis et cliquez sur *Reprendre*.

> ⓘ Remarque
>
> Les travaux qui étaient promus au moyen des références de connexion du système source ou destination sont automatiquement mis à jour.

Informations associées

Pour reprendre un travail [page 632]
Pour utiliser l'option Reprise partielle [page 633]
Pour reprendre un travail après expiration du mot de passe [page 634]

16.4 Promotion du contenu d'un référentiel entier à l'aide de l'outil de gestion des promotions

La promotion du contenu d'un référentiel exige une planification une préparation et de disposer de suffisamment de temps. Cette section décrit les actions requises pour une promotion réussie du contenu d'un déploiement à un autre.

16.4.1 Préparation des systèmes source et cible

Vous devez vous assurer que les systèmes source et cible sont configurés de façon optimale avant de promouvoir du contenu.

1. Sur le système source :
   a. Utilisez le Repository Diagnostic Tool (RDT) pour analyser et réparer le système source, ainsi que pour corriger les incohérences du référentiel ou du FRS. Pour en savoir plus sur le RDT, voir le *Guide de l'utilisateur de l'outil de diagnostic de référentiel de la plateforme de Business Intelligence*.
   b. Réduisez l'utilisation du système sur le système source afin d'assurer le moins de changements lors de la promotion. Un système actif peut entraîner un échec de l'objet.

   > ⓘ Remarque
   >
   > En cas d'échec, examinez le statut du travail afin de corriger les erreurs.

2. Sur le système cible :
   a. Utilisez le code clé de licence pour vous assurer que la licence sur le système cible est correcte et suffisante.

   > ⓘ Remarque
   >
   > Pour éviter que la promotion de contenu échoue en raison de droits de licence insuffisants, utilisez des licences identiques sur les deux systèmes.

   b. Si vous utilisez une authentification tierce, vous devez la configurer et l'activer sur le système cible avant de promouvoir du contenu.

   > ⓘ Remarque
   >
   > Ne mappez pas les utilisateurs ou les groupes d'utilisateurs. Cette action entraînera la création d'utilisateurs ou de groupes d'utilisateurs comportant des CUID différents sur le système cible. Le processus de promotion utilise des CUID pour identifier et mapper des objets entre le système

> source et le système cible. Le mappage d'utilisateurs et de groupes d'utilisateurs créera des incohérences de contenu et entraînera l'échec de la promotion.

c. Assurez-vous que les modules complémentaires requis sur le système source sont également installés sur le système cible.

> **Remarque**
>
> Pour assurer une migration réussie, vous devez installer des modules complémentaires tels que Analysis ou Design Studio sur le système source.

d. Si vous avez du contenu qui utilise des connexions QaaWS, vous devez activer les remplacements pour garantir que ces connexions sont dirigées vers les bons services Web. Pour en savoir plus sur la configuration de remplacements, consultez la section « Remplacements ».

e. Si vous avez besoin de migrer l'ensemble des instances planifiées terminées, vous devez cliquer sur *Afficher les instances finalisées dans la page Gérer les dépendances* dans la partie *Paramètres du travail* de la Gestion des promotions.

3. Sur le système central :

a. Vous pouvez désigner le système source, le système cible ou un système distinct comme système central sur lequel les travaux de Gestion des promotions sont exécutés. Lors de la promotion d'un référentiel entier, vous allez gérer un grand volume de contenu qui nécessitera des ressources système supplémentaires sur le système central. Utilisez les références de dimensionnement suivantes pour configurer le système central pour 10 000 objets :

	Allocation d'espace temporaire	Allocation de mémoire	Configuration supplémentaire
`LCM_CLI`	2 Go	2 Go	Mettez à jour `LCM_CLI.bat` et modifiez le paramètre `-Xmx`.
Job Server de la Gestion des promotions	3 Go	3 Go	Dans la CMC, mettez à jour la propriété de démarrage du Job Server de la Gestion des promotions en ajoutant le paramètre `-javaargs Xmx3g`. Pour en savoir plus, voir la note SAP 2286419.

Par exemple, si vous évaluez que le travail contient 50 000 objets :

- Allouez 10 Go de mémoire à `LCM_CLI` (50,000 ÷ 10,000 × 2)
- Allouez 15 Go de mémoire au Job Server (50,000 ÷ 10,000 × 3)

> **Remarque**
>
> Ces instructions de dimensionnement s'appliquent à la plupart des environnements. Toutefois, la taille des documents peut avoir une incidence sur les spécifications de la ressource.

16.4.2 Stratégies de migration

- Utilisez l'interface de ligne de commande (CLI) plutôt que l'outil CMC pour toutes les promotions de travail.
  - La CLI contourne la limite de session Web définie à 20 minutes qui a lieu durant un travail de promotion qui comprend plus de 1 000 objets.

    > ⓘ Remarque
    >
    > La limite d'objets dépend des ressources système.

  - La CLI offre un contrôle granulaire sur la promotion de contenu à l'aide d'un langage de requête pour sélectionner le contenu à migrer. Vous pouvez sélectionner du contenu du même type ou du contenu situé dans le même répertoire.
  - La CLI peut être exécutée par lots et les travaux de promotion peuvent être lancés par d'autres outils de script.
- Définissez la sécurité en promouvant les objets principaux (utilisateurs et groupes d'utilisateurs) en premier.
  - Le fait de promouvoir les utilisateurs et les groupes d'utilisateurs en premier permet de conserver le modèle de sécurité sur le système cible et garantit la réussite d'une migration ultérieure du contenu personnel des utilisateurs (tels que les boîtes de réception, les favoris, les catégories personnelles, etc.).

    > ⓘ Remarque
    >
    > Il est important d'effectuer cette tâche en premier lieu pour que les CUID des utilisateurs et des groupes d'utilisateurs sur le système cible soient identiques à ceux du système source.

- Désactivez le calcul de dépendances.
  - Le calcul de dépendances est l'une des tâches du processus de création d'un travail demandant le plus d'efforts. Lors de la migration du référentiel complet, tous les objets sont migrés : le calcul n'est donc pas nécessaire.

    > ⓘ Remarque
    >
    > Cette fonctionnalité n'est utile que lorsque vous ne savez pas exactement quels objets dépendants sont requis.

- Évitez d'inclure le calcul de sécurité lorsque c'est possible.
  - Le calcul de sécurité est la deuxième tâche du processus de création d'un travail demandant le plus d'efforts. Divisez la promotion en deux travaux si vous avez de nombreux documents dans plusieurs répertoires et que la sécurité est définie uniquement sur les répertoires. Le premier travail devra contenir uniquement les objets pour lesquels la sécurité est activée, et le deuxième travail contiendra uniquement les documents pour lesquels la sécurité est désactivée. Ainsi, vous pouvez effectuer des calculs de sécurité uniquement sur les répertoires, évitant de calculer la sécurité sur tous les documents.

    > ⓘ Remarque
    >
    > La sécurité des objets est conservée puisqu'elle est héritée de la sécurité des dossiers.

16.5 Étapes de promotion d'un système entier

La promotion d'un système entier exige l'exécution de trois travaux de promotion distincts dans un ordre spécifique. Chaque travail promeut un type de contenu spécifique. Pour plus d'informations sur la manière de promouvoir plusieurs objets, consultez l'article de la base de connaissances 1969259.

Le tableau suivant répertorie les types de contenu et les paramétrages des paramètres pour chaque travail de promotion.

Travail de promotion	Type de contenu	`exportDependencies`	`includeSecurity`
1	Tous les utilisateurs et groupes d'utilisateurs	false	true
2	Tous les objets dépendants	false	true
3	Tous les objets principaux	false	true

Utilisez l'interface de ligne de commande (CLI) pour créer et exécuter chaque travail. Pour en savoir plus sur la CLI, voir la section Utilisation de l'option Ligne de commande [page 641].

Paramètres communs

Utilisez les paramètres suivants pour les trois travaux de promotion :

> → N'oubliez pas
>
> Assurez-vous que chaque paramètre soit sur une nouvelle ligne.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

16.5.1 Pour promouvoir les utilisateurs et les groupes d'utilisateurs (Travail 1)

Pour établir des modèles de sécurité identiques entre les systèmes source et cible et afin de garantir que les CUIDs des objets des utilisateurs ou groupe d'utilisateurs sont identiques, promouvez les utilisateurs et les groupes d'utilisateurs en premier.

1. Créez un fichier `usersandgroups.properties` avec les paramètres communs et ajoutez les paramètres suivants afin de sélectionner tous les utilisateurs et groupes d'utilisateurs :

```
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
(SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2,
3))
```

2. Pour exécuter le travail, accédez au répertoire `<REPINSTALL>\win64x64\scripts` et exécutez la commande suivante :

```
Lcm_cli.bat –lcmproperties=usersandgroups.properties
```

16.5.2 Pour promouvoir des objets dépendants (Travail 2)

Les objets dépendants dépendent des objets principaux dans le dossier Public ou dans le dossier Favoris de l'utilisateur. Pour ne pas avoir à définir `includeDependencies` sur `true` pour tous les autres travaux, promouvez les objets dépendants en deuxième. Les objets dépendants sont les suivants :

- Niveaux d'accès
- Applications
- Vues d'entreprise
- Calendriers
- Catégories
- Connexions
- Evénements
- Connexions OLAP
- Profils
- Projets
- QaaWS
- Connexions à distance
- Listes de réplication
- Groupes de serveurs
- Univers

1. Créez le fichier dependencies.properties avec les paramètres communs et ajoutez les paramètres suivants au fichier afin de sélectionner tous les objets dépendants :

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
```

```
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. Pour exécuter le travail, accédez au répertoire `<REPINSTALL>\win64x64\scripts` et exécutez la commande suivante :

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

16.5.3 Pour promouvoir des objets principaux (Travail 3)

Les objets principaux sont des documents BI essentiels qui se trouvent dans le dossier Public et dans le dossier Favoris de l'utilisateur. En partant du principe que le deuxième travail de promotion a déjà été exécuté, la migration de tous les objets dépendants en promouvant les objets principaux en dernier rétablit leurs relations avec les objets dépendants.

1. Créez un fichier `primaryobjects.properties` avec les paramètres communs et ajoutez les paramètres suivants afin de sélectionner tous les utilisateurs et groupes d'utilisateurs :

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
```

```
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

Si vous réexécutez le même travail, excluez le travail LCM à l'aide de la requête suivante :

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. Pour exécuter le travail, accédez au répertoire `<REPINSTALL>\win64x64\scripts` et exécutez la commande suivante :

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> **ⓘ Remarque**
>
> Si le dossier Public ou les dossiers Favoris de l'utilisateur contiennent plus de 50 000 objets, il est recommandé de diviser ce travail final en plusieurs petits travaux.

> **ⓘ Remarque**
>
> Assurez-vous que les ordinateurs exécutant la commande d'interface de ligne de commande et le Job server de Gestion des promotions respectent les exigences de dimensionnement. Pour en savoir plus, voir la section « Dimensionnement ».

16.5.4 Post-promotion

La Gestion des promotions promeut uniquement les groupes de serveurs, mais pas leurs serveurs. Pour garantir que les rapports avec les serveurs désignés continuent à fonctionner, vous devez recréer et affecter les serveurs aux groupes de serveurs correspondants.

16.6 Utilisation de l'option Ligne de commande

L'option Ligne de commande de l'outil de gestion des promotions permet de promouvoir des objets d'un déploiement de la plateforme de BI vers un autre. Vous pouvez créer un script pour plusieurs travaux.

> **→ Conseil**
>
> Utilisez l'option Ligne de commande pour les travaux contenant un grand nombre d'objets.

L'outil de gestion des promotions prend en charge les types de promotion de travail suivants à partir de ligne de commande :

- Exporter un modèle de promotion de travail existant vers LCMBIAR avec un cryptage protégé par mot de passe
- Exporter un modèle de promotion de travail existant vers LCMBIAR sans cryptage protégé par mot de passe
- Exporter une seule ou plusieurs requêtes de plateforme
- Promouvoir plusieurs requêtes de plateforme
- Promouvoir avec un modèle de travail existant
- Importer et promouvoir un fichier LCMBIAR existant
- Réalisation d'une promotion Live-to-Live

16.6.1 Pour exécuter l'outil de ligne de commande sous Windows

Pour exécuter l'outil de ligne de commande, procédez comme suit :

1. Démarrez une fenêtre ou un shell de ligne de commande.
2. Accédez au répertoire approprié.

   Par exemple, le chemin du répertoire pour Windows est `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Effectuez l'une des actions suivantes :
   - Exécutez l'interface de ligne de commande de gestion du cycle de vie, vérifiez que le répertoire java est défini avant l'exécution du programme.
     Commande : `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <fichier de propriétés>`
   - Exécutez le fichier BAT depuis `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`.
     Commande : `lcm_cli.bat -lcmproperty <fichier de propriétés>`

     > **Remarque**
     >
     > Saisissez les mots de passe valides demandés.

L'outil de ligne de commande de la gestion des promotions utilise un fichier de `<propriétés>` comme paramètre. Le fichier de `<propriétés>` contient les paramètres nécessaires pour communiquer à l'outil de gestion des promotions les actions à effectuer, la connexion au déploiement de la plateforme de BI, les méthodes de connexion, les objets à promouvoir.

Le nom du fichier doit suivre le modèle suivant : `<NOMFICHIER>.properties`

Par exemple : `<Mespropriétés.properties>`

16.6.2 Pour exécuter l'outil de ligne de commande sous Unix

Pour exécuter l'outil de ligne de commande, procédez comme suit :

1. Lancez le shell.
2. Accédez au répertoire approprié.

   Par exemple, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. Effectuez l'une des actions suivantes :
   - Exécutez l'interface de ligne de commande de gestion du cycle de vie, vérifiez que le répertoire java est défini avant l'exécution du programme.
     Commande : `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <fichier de propriétés>`
   - Exécutez le fichier BAT à partir de `<chemin_rep_install>\sap_bobj\lcm_cli.sh`
     Commande : `lcm_cli.sh -lcmproperty <fichier de propriétés>`

> ⓘ Remarque
>
> Saisissez les mots de passe valides demandés.

16.6.3 Paramètres d'outil de ligne de commande

Les paramètres de ligne de commande pour l'option de ligne de commande de l'outil de gestion des promotions sont organisés en fonction de trois principaux types de promotions :

- Promotion d'objets d'un fichier LCMBIAR vers un CMS (Live)
- Promotion d'objets d'un CMS source (Live) vers un CMS cible (Live)
- Exportation d'objets d'un CMS (Live) vers un fichier LCMBIAR

Outre les paramètres concernés par ces trois types de promotion, il existe également des paramètres pour les commandes générales qui peuvent être utilisés dans tous les scénarios de promotion.

> → N'oubliez pas
>
> Ne placez pas de paramètres de ligne de commande entre guillemets.

> ⓘ Remarque
>
> - Semblable à la création d'un travail avant l'exportation, l'option Ligne de commande crée un travail temporaire à la volée. Ce nom de travail peut être une combinaison de `Query_<UTILISATEUR>_<horodatage>` Cela est spécifique uniquement à `<exportQuery>`.
> - Vous pouvez reprendre le travail uniquement par le biais de l'outil de gestion des promotions. Il n'existe pas de prise en charge de ligne de commande pour la reprise des travaux.
> - Lors de l'utilisation d'un grand nombre d'objets, il est préférable d'augmenter la taille du segment Java maximale en définissant le paramètre `-Xmx=8g` dans le script `LCMCLI`.

Informations associées

Fichier LCMBIAR vers un CMS (Live) [page 647]
Promotion d'un CMS source (Live) vers un CMS cible (Live) [page 654]
Promotion d'un CMS (Live) vers un fichier LCMBIAR [page 650]
Liste de tous les paramètres de ligne de commande [page 657]

16.6.3.1 Paramètres de ligne de commande par scénario de promotion

Les paramètres de ligne de commande sont présentés dans l'ordre recommandé pour chaque scénario de promotion. Le tableau indique tous les paramètres disponibles et leur statut (obligatoire ou facultatif) pour chaque scénario de promotion. Chaque paramètre obligatoire est décrit pour son scénario de promotion correspondant. Les paramètres facultatifs sont décrits dans la section Liste de tous les paramètres de ligne de commande. Reportez-vous aux liens associés pour toutes les informations relatives aux paramètres par scénario et les paramètres additionnels disponibles.

Groupe de paramètres	Paramètre	LCMBIAR vers Live	Live vers LCMBIAR	Live vers Live	Reprise
Fichier de propriétés	`lcmproperty`	Facultatif	Recommandé	Recommandé	Recommandé
Type d'action	`action`	Obligatoire action=promote	Obligatoire action=export	Obligatoire action=promote	Obligatoire action=rollback
Nœud LCM	`LCM_CMS`	Obligatoire			
	`LCM_userName`	Obligatoire			
	`LCM_Password`	Obligatoire Si le paramètre est vide, il sera requis dans la console			
	`LCM_authentication`	Facultatif : Par défaut : `secEnterprise`			
	`LCM_SystemID`	Obligatoire seulement pour l'authentification SAP.			
	`LCM_ClientID`	Obligatoire seulement pour l'authentification SAP.			
Source (Live ou LCMBIAR)	`importLocation`	Obligatoire	Non applicable	Non applicable	Non applicable

Groupe de paramètres	Paramètre	LCMBIAR vers Live	Live vers LCMBIAR	Live vers Live	Reprise
	`lcmbiarpassword`	Obligatoire (peut être vide)	Non applicable	Non applicable	Non applicable
	`Source_CMS`	Non applicable	Obligatoire	Obligatoire	Non applicable
	`Source_UserName`	Non applicable	Obligatoire	Obligatoire	Non applicable
	`Source_password`	Non applicable	Obligatoire Si le paramètre est vide, il sera requis dans la console	Obligatoire Si le paramètre est vide, il sera requis dans la console	Non applicable
	`Source_authentication`	Non applicable	Facultatif Par défaut : `secEnterprise`	Facultatif Par défaut : `secEnterprise`	Non applicable
	`Source_systemID`	Non applicable	Obligatoire seulement pour l'authentification SAP.	Obligatoire seulement pour l'authentification SAP.	Non applicable
	`Source_clientID`	Non applicable	Obligatoire seulement pour l'authentification SAP.	Obligatoire seulement pour l'authentification SAP.	Non applicable
Destination (Live ou LCMBIAR)	`Destination_CMS`	Obligatoire	Non applicable	Obligatoire	Non applicable
	`Destination_username`	Obligatoire	Non applicable	Obligatoire	Non applicable
	`Destination_password`	Obligatoire	Non applicable	Obligatoire	Non applicable
	`Destination_authentication`	Facultatif Par défaut : `secEnterprise`	Non applicable	Facultatif Par défaut : `secEnterprise`	Non applicable
	`Destination_systemID`	Obligatoire seulement pour l'authentification SAP.	Non applicable	Obligatoire seulement pour l'authentification SAP.	Non applicable
	`Destination_clientID`	Obligatoire seulement pour l'authentification SAP.	Non applicable	Obligatoire seulement pour l'authentification SAP.	Non applicable

Groupe de paramètres	Paramètre	LCMBIAR vers Live	Live vers LCMBIAR	Live vers Live	Reprise
	`ExportLocation`	Non applicable	Obligatoire	Non applicable	Non applicable
	`lcmbiarpassword`	Non applicable	Obligatoire (peut être vide)	Non applicable	Non applicable
Associé au travail	`JOB_CUID`	Non applicable	Facultatif	Facultatif	Obligatoire
	`Override`	Facultatif	Non applicable	Non applicable	Non applicable
	`forceOverride` Disponible dans la version SP4	Facultatif	Non applicable	Non applicable	Non applicable
	`Timeout` Disponible dans la version SP4	Facultatif	Non applicable	Facultatif	Non applicable
Associé à l'exportation	`ExportDependencies`	Non applicable	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
	`ExportQuery`	Non applicable	Obligatoire	Obligatoire	Non applicable
	`ExportQueriesTotal`	Non applicable	Facultatif : utiliser si vous avez plusieurs requêtes d'exportation	Facultatif : utiliser si vous avez plusieurs requêtes d'exportation	Non applicable
	`BatchJobQuery`	Non applicable	Facultatif : utiliser avec Exportquery	Facultatif : utiliser avec Exportquery	Non applicable
	`LimitQueryBatchSize`	Non applicable	Facultatif	Facultatif	Non applicable
Associé au journal	`Consolelog`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
	`ResultFileName`	Facultatif	Facultatif	Facultatif	Non applicable
	`LogFileName` Disponible dans la version SP4	Facultatif	Facultatif	Facultatif	Non applicable

Groupe de paramètres	Paramètre	LCMBIAR vers Live	Live vers LCMBIAR	Live vers Live	Reprise
Sélection de l'objet	`Selected_CUIDS`	Facultatif	Non applicable	Non applicable	Non applicable
	`selectUser` Disponible dans la version SP4	Non applicable	Facultatif Par défaut : `All`	Facultatif Par défaut : `All`	Non applicable
	`selectGroup` Disponible dans la version SP4	Non applicable	Facultatif Par défaut : `All`	Facultatif Par défaut : `All`	Non applicable
Sécurité	`IncludeApplicationSecurity`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
	`IncludeSecurity`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
	`IncludeTopLevelSecurity`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
Commentaires	`IncludeComments`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Facultatif Par défaut : `False`	Non applicable
Travaux de fédération	`IncludeFederationJobsRelationship`	Facultatif Par défaut : `True`	Non applicable	Facultatif Par défaut : `True`	Non applicable

Informations associées

Fichier LCMBIAR vers un CMS (Live) [page 647]
Promotion d'un CMS (Live) vers un fichier LCMBIAR [page 650]
Promotion d'un CMS source (Live) vers un CMS cible (Live) [page 654]
Liste de tous les paramètres de ligne de commande [page 657]

16.6.3.2 Fichier LCMBIAR vers un CMS (Live)

Lors de la promotion d'objets d'un fichier LCMBIAR vers un CMS (Live), vous référencez un fichier de propriétés dans la ligne de commande qui spécifie l'ordre de promotion comme suit :

- Emplacement de l'importation et type d'action de promotion
- Informations de connexion du CMS qui héberge l'outil de gestion de la promotion (précédemment appelé l'outil de gestion du cycle de vie LCM).

- Informations de connexion du CMS de destination.
- Autres paramètres requis pour promouvoir le CMS, par exemple le mot de passe LCMBIAR, ou remplacer des paramètres pour écraser des objets existants si nécessaire.

Vous pouvez inclure d'autres paramètres facultatifs pour spécifier les besoins de promotion particuliers. Ces paramètres facultatifs sont décrits dans la section Liste de tous les paramètres de ligne de commande [page 657].

L'exemple suivant illustre une promotion d'un fichier LCMBIAR vers un CMS (Live) sans utiliser de fichier de propriétés dans la ligne de commande :

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
lcmbiarpassword
```

L'exemple suivant illustre une promotion d'un fichier LCMBIAR vers un CMS (Live) en utilisant un fichier de propriétés dans la ligne de commande :

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

Le tableau suivant répertorie les paramètres obligatoires requis pour un fichier de propriétés réussi pour la promotion d'un fichier LCMBIAR vers un CMS (Live).

Groupe de paramètres	Paramètre	Description
Type d'action	`action`	Opération que la CLI doit réaliser. Valeur : export Exemple : `action=export`

Groupe de paramètres	Paramètre	Description
Nœud LCM	`LCM_CMS`	CMS pour l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Nom d'utilisateur du compte que l'outil doit utiliser pour se connecter au CMS de l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_userName=adminLCM`
	`LCM_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `LCM_password=my_adminpassword1`
Source :Fichier LCMBIAR	`importLocation`	Emplacement du fichier LCMBIAR qui contient les objets à promouvoir. Valeur : Texte au format libre. Extension `<.lcmbiar>` obligatoire Exemple : `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Permet le cryptage et le décryptage de fichiers BIAR à l'aide d'un mot de passe. Valeur : Texte au format libre Exemple : `lcmbiar=validlcmbiarpassword`
Destination :CMS (Live)	`Destination_CMS`	Le CMS auquel l'outil doit se connecter. Valeur : Nom du CMS valide Exemple : `Destination_CMS=myCMS.mydomain.sap:6400`

Groupe de paramètres	Paramètre	Description
	`Destination_username`	Le compte utilisateur que l'outil doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Nom d'utilisateur valide Exemple : `Destination_username=admin LCM`
	`Destination_password`	Mot de passe associé du compte utilisateur. Valeur : Mot de passe valide Exemple : `Destination_password=my_adminpassword1`

Informations associées

Promotion d'un CMS (Live) vers un fichier LCMBIAR [page 650]
Promotion d'un CMS source (Live) vers un CMS cible (Live) [page 654]
Liste de tous les paramètres de ligne de commande [page 657]

16.6.3.3 Promotion d'un CMS (Live) vers un fichier LCMBIAR

Lors de la promotion d'objets d'un CMS (Live) vers un fichier LCMBIAR, vous référencez un fichier de propriétés à partir de la ligne de commande qui spécifie l'ordre de promotion comme suit :

- Type d'action de promotion : export
- Informations de connexion du CMS qui héberge l'outil de gestion de la promotion (précédemment appelé l'outil de gestion du cycle de vie LCM).
- Informations de connexion du CMS source.
- Répertoire de destination du fichier LCMBIAR.
- Les autres paramètres nécessaires à la promotion du CMS, par exemple le mot de passe du fichier LCMBIAR ou les paramètres de sécurité.

Vous pouvez inclure d'autres paramètres facultatifs pour spécifier les besoins de promotion particuliers. Ces paramètres facultatifs sont décrits dans la section Liste de tous les paramètres de ligne de commande [page 657].

L'exemple suivant montre un fichier de propriétés habituel pour la promotion d'un CMS (Live) vers un fichier LCMBIAR :

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

Le tableau suivant répertorie les paramètres obligatoires requis pour un fichier de propriétés réussi pour la promotion d'un fichier LCMBIAR vers un CMS (Live).

Groupe de paramètres	Paramètre	Description
Type d'action	`action`	Opération que la CLI doit réaliser. Valeur : export Exemple : `action=export`
Nœud LCM	`LCM_CMS`	CMS pour l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_CMS=myCMS.mydomain.sap:6400`

Groupe de paramètres	Paramètre	Description
	`LCM_userName`	Nom d'utilisateur du compte que l'outil doit utiliser pour se connecter au CMS de l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_userName=adminLCM`
	`LCM_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `LCM_password=my_adminpassword1`
Source :CMS (Live)	`Source_CMS`	Le CMS auquel l'outil de gestion de la promotion doit se connecter. Valeur : Texte au format libre Exemple : `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_userName`	Le compte utilisateur que l'outil de gestion de la promotion doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Texte au format libre Exemple : `Source_username=adminLCM`
	`Source_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `Source_password=my_adminpassword1`

Groupe de paramètres	Paramètre	Description
Destination :Fichier LCMBIAR	`exportLocation`	Spécifie l'emplacement du fichier LCMBIAR après l'exportation et le re-groupement en lot des objets. Valeur : Texte au format libre. Extension `<.lcmbiar>` obligatoire Exemple : `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Permet le cryptage et le décryptage de fichiers BIAR à l'aide d'un mot de passe. Valeur : Texte au format libre Exemple : `lcmbiarpassword=validlcmbiarpassword`
Associé à l'exportation	`exportQuery`	Envoie une requête au CMS source pour obtenir les objets nécessaires à l'exportation vers le fichier LCMBIAR. Valeur : Texte au format libre. Utilisez le format de langage de requête du CMS. Exemple : `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Remarque** Vous pouvez avoir le nombre de requêtes que vous souhaitez dans un seul fichier de propriétés mais elles doivent être nommées exportQuery1, exportQuery2.

Informations associées

Fichier LCMBIAR vers un CMS (Live) [page 647]

Promotion d'un CMS source (Live) vers un CMS cible (Live) [page 654]
Liste de tous les paramètres de ligne de commande [page 657]

16.6.3.4 Promotion d'un CMS source (Live) vers un CMS cible (Live)

Lors de la promotion d'objets d'un CMS source (Live) vers un CMS cible (Live), vous référencez un fichier de propriétés à partir de la ligne de commande qui spécifie l'ordre de promotion comme suit :

- Type d'action de promotion : promotion
- Informations de connexion du CMS qui héberge l'outil de gestion de la promotion (précédemment appelé l'outil de gestion du cycle de vie LCM).
- Informations de connexion du CMS source.
- Informations de connexion du CMS de destination.
- Les autres paramètres nécessaires à la promotion du CMS, par exemple les paramètres de sécurité ou de dépendances.

Vous pouvez inclure d'autres paramètres facultatifs pour spécifier les besoins de promotion particuliers. Ces paramètres facultatifs sont décrits dans la section Liste de tous les paramètres de ligne de commande [page 657].

L'exemple suivant montre un fichier de propriétés habituel pour la promotion d'un CMS source vers un CMS cible.

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

Le tableau suivant répertorie les paramètres obligatoires requis pour un fichier de propriétés réussi pour la promotion d'un CMS source vers un CMS cible :

Groupe de paramètres	Paramètre	Description
Type d'action	`action`	Opération que la ligne de commande doit réaliser. Valeur : promouvoir Exemple : `action=promote`
Nœud LCM	`LCM_CMS`	CMS pour l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Nom d'utilisateur du compte que l'outil doit utiliser pour se connecter au CMS de l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_userName=adminLCM`
	`LCM_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `LCM_password=my_adminpassword1`
Source : CMS (Live)	`source_CMS`	Le CMS auquel l'outil de gestion de la promotion doit se connecter. Valeur : Texte au format libre Exemple : `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_username`	Le compte utilisateur que l'outil de gestion de la promotion doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Texte au format libre Exemple : `Source_username=adminLCM`

Groupe de paramètres	Paramètre	Description
	`Source_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `Source_password=my_adminpassword1`
Destination : CMS (Live)	`Destination_CMS`	Le CMS auquel l'outil doit se connecter. Valeur : Texte au format libre Exemple : `Destination_CMS=myCMS1:myCMS2`
	`Destination_username`	Le compte utilisateur que l'outil doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Texte au format libre Exemple : `Destination_username=adminLCM`
	`Destination_password`	Mot de passe associé du compte utilisateur. Valeur : Texte au format libre Exemple : `Destination_password=my_adminpassword1`

Groupe de paramètres	Paramètre	Description
Associé à l'exportation	`exportQuery`	Requêtes que l'outil LCM exécute pour obtenir les objets nécessaires à l'exportation vers le CMS cible. Valeur : Texte au format libre. Utilisez le format de langage de requête du CMS. Exemple : `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Remarque** Vous pouvez avoir le nombre de requêtes que vous souhaitez dans un seul fichier de propriétés mais elles doivent être nommées exportQuery1, exportQuery2.

Informations associées

Fichier LCMBIAR vers un CMS (Live) [page 647]
Promotion d'un CMS (Live) vers un fichier LCMBIAR [page 650]
Liste de tous les paramètres de ligne de commande [page 657]

16.6.3.5 Liste de tous les paramètres de ligne de commande

Le tableau suivant décrit tous les paramètres de ligne de commande.

> **Remarque**
> Lorsqu'ils sont exécutés dans une ligne de commande, la syntaxe des paramètres est la suivante : `-<parameterName><space><parameterValue>`. Dans un fichier de propriétés, la syntaxe des paramètres est la suivantes : `-<parameterName><space><parameterValue>`.

Groupe de paramètres	Paramètre	Description
Fichier de propriétés	`lcmproperty`	Fait référence aux valeurs, enregistrées dans un fichier, requises pour l'exécution d'une commande. Valeur : Chemin complet de l'emplacement où le fichier de propriété a été enregistré Exemple : `-lcmproperty C:\MyPropertyFile.properties`
Type d'action	`action`	Opération que la CLI doit réaliser. Valeur : promote ou export Exemple : `action=promote`
Nœud LCM	`LCM_CMS`	CMS pour l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Nom d'utilisateur du compte que l'outil doit utiliser pour se connecter au CMS de l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_userName=adminLCM`
	`LCM_Password`	Mot de passe du compte utilisateur. Si le paramètre est vide, il sera requis dans la console. Valeur : Texte au format libre Exemple : `LCM_password=my_adminpassword1`
	`LCM_authentication`	Indique le type d'authentification à utiliser. Valeur : secEnterprise, secWinAD, secLDAP,secSAPR3. Si le paramètre n'est pas spécifié, la valeur par défaut `secEnterprise`. Exemple : `LCM_authentication=secEnterprise`
	`LCM_systemID` **Remarque** Obligatoire pour l'authentification SAP.	Requis pour l'authentification SAP uniquement. Valeur : ID système Exemple : `LCM_systemID=systemID`

Groupe de paramètres	Paramètre	Description
	`LCM_clientID` **Remarque** Obligatoire pour l'authentification SAP.	Requis pour l'authentification SAP uniquement. Valeur : ID client Exemple : `LCM_clientID=clientID`
Source :Fichier LCMBIAR	`importLocation`	Emplacement du fichier LCMBIAR qui contient les objets à promouvoir. Valeur : Texte au format libre. Extension `<.lcmbiar>` obligatoire Exemple : `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Permet le cryptage et le décryptage de fichiers BIAR à l'aide d'un mot de passe. Valeur : Texte au format libre Exemple : `lcmbiar=validlcmbiarpassword`
Source :CMS (Live)	`Source_CMS`	Le CMS auquel l'outil de gestion de la promotion doit se connecter. Valeur : Texte au format libre Exemple : `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_UserName`	Le compte utilisateur que l'outil de gestion de la promotion doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Texte au format libre Exemple : `Source_username=adminLCM`
	`Source_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `Source_password=my_adminpassword1`
	`Source_authentication`	Indique le type d'authentification à utiliser. Valeur : secEnterprise, secWinAD, secLDAP,secSAPR3. Si le paramètre n'est pas spécifié, la valeur par défaut `secEnterprise`. Exemple : `Source_authentication=secEnterprise`

Groupe de paramètres	Paramètre	Description
	`Source_systemID`	Requis pour l'authentification SAP uniquement. Valeur : ID système Exemple : `Source_systemID=systemID`
	`Source_clientID`	Requis pour l'authentification SAP uniquement. Valeur : ID système Exemple : `Source_clientID=clientID`
Destination :Fichier LCMBIAR	`exportLocation`	Spécifie l'emplacement du fichier LCMBIAR après l'exportation et le regroupement en lot des objets. Valeur : Texte au format libre. Extension `<.lcmbiar>` obligatoire Exemple : `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Permet le cryptage et le décryptage de fichiers BIAR à l'aide d'un mot de passe. Valeur : Texte au format libre Exemple : `lcmbiarpassword=validlcmbiarpassword`
Destination :CMS (Live)	`Destination_CMS`	Le CMS auquel l'outil doit se connecter. Valeur : Nom du CMS valide Exemple : `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Le compte utilisateur que l'outil doit utiliser pour se connecter au CMS de la plateforme de BI. Valeur : Nom d'utilisateur valide Exemple : `Destination_username=adminLCM`
	`Destination_password`	Mot de passe associé du compte utilisateur. Valeur : Mot de passe valide Exemple : `Destination_password=my_adminpassword1`

> **Remarque**
> Obligatoire pour l'authentification SAP.

> **Remarque**
> Obligatoire pour l'authentification SAP.

Groupe de paramètres	Paramètre	Description
	`Destination_authentication`	Indique le type d'authentification à utiliser. Valeur : secEnterprise, secWinAD, secLDAP, secSAPR3. Si le paramètre n'est pas spécifié, la valeur par défaut `secEnterprise`. Exemple : `Destination_authentication=secEnterprise`
	`Destination_systemID` **Remarque** Obligatoire pour l'authentification SAP.	Requis pour l'authentification SAP uniquement. Valeur : ID système Exemple : `Destination_systemID=systemID`
	`Destination_clientID` **Remarque** Obligatoire pour l'authentification SAP.	Requis pour l'authentification SAP uniquement. Valeur : ID client Exemple : `Destination_clientID=clientID`
Associé au travail	`JOB_CUID`	Donne à l'outil l'instruction d'exporter tous les objets du travail vers le fichier LCMBIAR. Valeur : Le CUID du travail de gestion enregistré.
	`Override`	Utilisé pour promouvoir sélectivement les objets à partir d'un fichier LCMBIAR. Si défini sur `true` : permet à l'utilisateur de remplacer un travail existant. Si défini sur `false` : permet à l'utilisateur de créer un nouveau travail avec le nom `<JOB_NAME>_<TIME_STAMP>` . Valeur : true ou false Exemple : `Override=true`
	`forceOverride` Disponible dans la version SP4	Utilisé pour remplacer un travail qui porte le même nom mais pas le même CUID. Valeur : true ou false Exemple : `forceOverride=true`

Groupe de paramètres	Paramètre	Description
	`Timeout` Disponible dans la version SP4	Définit un délai d'expiration pour la promotion d'action. Valeur : Durée en secondes Exemple : `timeout=30`
Associé à l'exportation	`ExportDependencies`	Spécifie les dépendances d'objet que l'outil rassemble pour l'exportation. Applicable uniquement lorsqu'il est utilisé conjointement avec l'indicateur `Source_CMS`. Valeur : true ou false. La valeur est `false` s'il n'est pas spécifié. Exemple : `ExportDependencies=false`
	`ExportQuery`	Requêtes que l'outil LCM exécute pour obtenir les objets nécessaires à l'exportation vers le CMS cible. Valeur : Texte au format libre. Utilisez le format de langage de requête du CMS. Exemple : `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **Remarque** Vous pouvez avoir le nombre de requêtes que vous souhaitez dans un seul fichier de propriétés mais elles doivent être nommées exportQuery1, exportQuery2.
	`ExportQueriesTotal`	Utilisé pour spécifier le nombre de requêtes d'exportation à exécuter. Si vous avez x requêtes d'exportation et souhaitez toutes les exécuter, vous devez attribuer à ce paramètre la valeur x. Valeur : nombre entier positif. La valeur par défaut est 1 s'il n'est pas spécifié. Exemple : `ExportQuery1=<your sql statement> ExportQuery2=<your sql statement> ExportQueriesTotal=2`

Groupe de paramètres	Paramètre	Description
	`BatchJobQuery`	Utilisé conjointement avec `ExportQuery`. Crée et lance un travail pour chaque ligne renvoyée par la requête de travail. Les requêtes d'exportation de travail peuvent utiliser des "espaces réservés" qui référencent les propriétés signalées dans la requête de travail. Le format des espaces réservés est $b:PPTY$, lorsque le nom de la propriété n'est pas sensible à la casse. Les propriétés <PPTY> valides sont : "cuid" - "name" - "id" Une erreur survient si un espace réservé n'est pas reconnu ou signalé par la requête de travail. Valeur : Texte au format libre Exemple : `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")`
	`LimitQueryBatchSize`	Limite le nombre d'objets renvoyés à 1 000 par défaut. Lorsque ce paramètre est défini sur faux, tous les objets demandés sont renvoyés. **Remarque** Vous pouvez aussi définir explicitement la nouvelle limite pour le nombre d'objets renvoyés par la requête à l'aide de `select TOP <number>` Valeur : true ou false. La valeur par défaut est true s'il n'est pas spécifié. Exemple : `LimitQueryBatchSize=true`

Groupe de paramètres	Paramètre	Description
Associé au journal	`consolelog`	Utilisé pour afficher l'intégralité du journal de la commande exécutée par l'utilisateur dans le journal de commande. Valeur : true ou false. La valeur est `false` s'il n'est pas spécifié. Exemple : `consolelog=true`
	`ResultFileName`	Le nom du fichier sur le système de fichiers local lorsque le paramètre `consolelog` est utilisé. Valeur : Chemin d'accès au fichier de résultats du travail Exemple : `ResultFileName=C:\Logs\ResultFile.txt`
	`LogFileName` Disponible dans la version SP4	Permet à l'utilisateur de spécifier un chemin fixe à utiliser pour le fichier journal. Valeur : Chemin d'accès du fichier journal Exemple : `LogFileName=C:\Logs\LogFile.log`
Sélection de l'objet	`Selected_CUIDS`	Permet à l'utilisateur de promouvoir sélectivement les objets (rapports, utilisateurs, univers, etc.) avec leurs dépendances d'un fichier LCMBIAR au lieu de promouvoir l'ensemble du fichier. Valeur : Les CUID d'objets dans le fichier LCMBIAR doivent être promus sélectivement
	`selectUser` Disponible dans la version SP4	Filtre les utilisateurs en fonction de l'authentification tierce (LDAP, SAPR3, WindowsAD...). Valeur : all, none, excludeTP ou onlyTP. La valeur est `all` s'il n'est pas spécifié. Exemple : `selectUser=excludeTP`
	`selectGroup` Disponible dans la version SP4	Filtre les groupes d'utilisateurs en fonction de l'authentification tierce (LDAP, SAPR3, WindowsAD...). Valeur : all, none, excludeTP ou onlyTP. La valeur est `all` s'il n'est pas spécifié. Exemple : `selectGroup=onlyTP`
Sécurité	`IncludeApplicationSecurity`	Donne à l'outil l'instruction d'exporter ou d'importer la sécurité associée aux applications sélectionnées. Valeur : true ou false. La valeur est `false` s'il n'est pas spécifié. Exemple : `IncludeApplicationSecurity=true`

Groupe de paramètres	Paramètre	Description
	`IncludeSecurity`	Donne à l'outil l'instruction d'exporter ou d'importer la sécurité associée aux objets sélectionnés et aux utilisateurs sélectionnés. Si les niveaux d'accès sont utilisés, cela les exportera ou les importera également. Valeur : true ou false. La valeur est `false` s'il n'est pas spécifié. Exemple : `IncludeSecurity=true`
Commentaires	`IncludeComments`	Donne à l'outil l'instruction d'exporter ou d'importer les commentaires associée aux objets sélectionnés. Valeur : true ou false. La valeur est `false` s'il n'est pas spécifié. Exemple : `IncludeComments=true`
Travaux de fédération	`IncludeFederationJobsRelationship`	Indique à l'outil de conserver les relations des travaux de fédération (Listes de réplication et Connexions distantes). Lorsque cette option est définie sur false, les objets répliqués deviennent des objets standard et l'indicateur de fédération est supprimé. Cette option peut être utile lorsque l'objet répliqué est le seul objet disponible et que l'objet source ne l'est plus. Valeur : true ou false. La valeur est `true` s'il n'est pas spécifié. Exemple : `IncludeFederationJobsRelationship=false`

16.6.3.6 Reprise

Vous pouvez annuler le travail promu dans le système de destination via l'outil *Gestion des promotions*.

Si vous avez promu un travail via l'outil *Gestion des promotions*, par exemple, pour mettre à jour BI 4.2 SP07 vers BI 4.3 et si vous voulez annuler cette modification ultérieurement, vous pouvez utiliser les paramètres de ligne de commande, définis dans Paramètres de ligne de commande par scénario de promotion [page 644] et exécuter l'opération de reprise.

Lorsque vous exécutez l'opération de reprise, vous devez fournir un fichier de propriétés qui spécifie l'ordre de promotion comme suit :

- Type d'action de promotion : reprise
- Informations de connexion du CMS qui héberge l'outil de gestion de la promotion (précédemment appelé l'outil de gestion du cycle de vie LCM).
- Informations de connexion du CMS source.

- Informations de connexion du CMS de destination.
- Les autres paramètres nécessaires à la promotion du CMS, par exemple les paramètres de sécurité ou de dépendances.

Vous pouvez inclure d'autres paramètres facultatifs pour spécifier les besoins de promotion particuliers. Ces paramètres facultatifs sont décrits dans Liste de tous les paramètres de ligne de commande [page 657].

Vous pouvez vous référer à l'exemple de fichier de propriétés pour effectuer une opération de reprise :

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **Remarque**
>
> Vous pouvez trouver le `job_cuid` pour un travail promu sous *Accueil de la CMC* > *Gestion des promotions* > *Propriétés*.

Le tableau suivant répertorie les paramètres obligatoires requis pour un fichier de propriétés réussi pour la promotion d'un fichier LCMBIAR vers un CMS (Live).

Groupe de paramètres	Paramètre	Description
Type d'action	`action`	Opération que la CLI doit réaliser. Valeur : reprise Exemple : `action=rollback`
Associé au travail	`job_cuid`	Donne à l'outil l'instruction d'exporter tous les objets du travail vers le fichier LCMBIAR. Valeur : Le CUID du travail de gestion enregistré. Exemple : `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`
Nœud LCM	`LCM_CMS`	CMS pour l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_CMS=myCMS.mydomain.sap:6400`

Groupe de paramètres	Paramètre	Description
	`LCM_userName`	Nom d'utilisateur du compte que l'outil doit utiliser pour se connecter au CMS de l'outil de gestion de la promotion. Valeur : Texte au format libre Exemple : `LCM_userName=adminLCM`
	`LCM_password`	Mot de passe du compte utilisateur. Valeur : Texte au format libre Exemple : `LCM_password=my_adminpassword1`
	`LCM_authentication`	Type d'authentification pour le compte utilisateur Valeur : Type d'authentification Exemple : `secEnterprise`

16.6.4 Exemple de fichier de propriétés

Ceci est un exemple de fichier de `propriétés` :

Exemple

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<nom du CMS:numéro du port>
LCM_userName=<nom utilisateur>
LCM_password=<mot de passe>
LCM_authentication=<authentification>
LCM_systemID=<ID>
LCM_clientID=<ID client>
Destination_CMS=<nom du CMS:numéro du port>
Destination_userName=<nom utilisateur>
Destination_password=<mot de passe>
```

```
Destination_authentication=<authentification>

Destination_systemID=<ID>

Destination_clientID=<ID client>

lcmbiarpassword=<mot de passe>
```

> **Remarque**
>
> Si le fichier de `propriétés` ne possède aucune information personnelle, l'interface de ligne de commande LCM les demande dans la console.

16.7 Utilisation du CTS (Change and Transport System) amélioré

Le CTS (Change and Transport System) organise et personnalise des projets de développement dans ABAP Workbench, puis transporte ces modifications entre les Systèmes SAP dans votre paysage système. Le CTS+ (Enhanced Change and Transport System) est un module complémentaire au CTS qui promeut les contenus non ABAP à travers les référentiels non ABAP sur lesquels le CTS+ est activé.

Les InfoObjects de la plateforme de BI peuvent utiliser le contenu SAP Business Warehouse comme source de données. L'intégration de CTS+ dans l'outil de gestion des promotions permet d'utiliser le référentiel de la plateforme de BI de la même manière que le référentiel de SAP Business Warehouse (BW), via l'utilisation de requêtes de transport CTS pour promouvoir les travaux. CTS+ fournit une option de transport des objets non SAP au sein d'un paysage système. Par exemple, des objets créés dans le système de développement peuvent être joints à une demande de transport et transférés vers d'autres systèmes au sein du paysage.

Pour en savoir plus sur le CTS (Change and Transport System), voir Change and Transport System - Overview (BC-CTS)

Pour en savoir plus sur le CTS+ (Enhanced Change and Transport System), voir Transporting Non-ABAP Objects in Change and Transport System

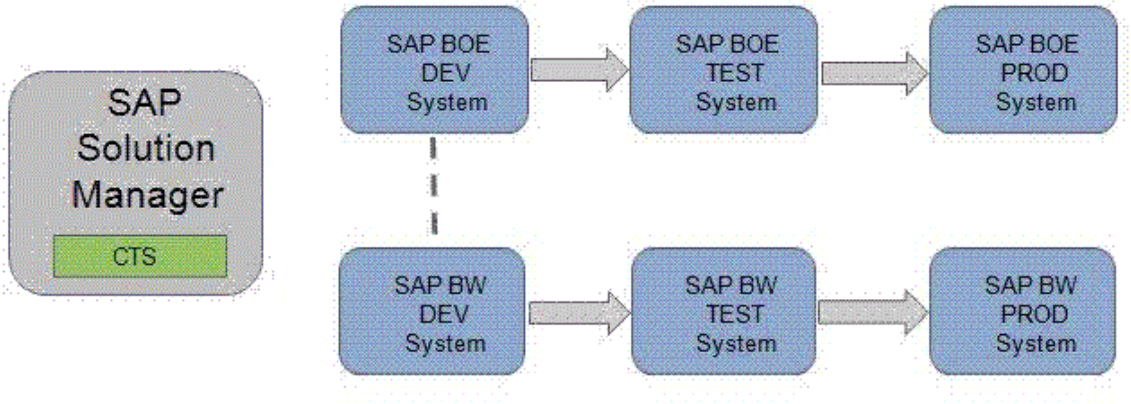
16.7.1 Prérequis

Le transport de contenu BI d'un système à un autre via CTS+ suppose les conditions préalables suivantes :

1. La plateforme de BI 4.0 (ou une version plus récente) est installée.
2. SAP Solution Manager 7.1 ou SAP Solution Manager 7.0 EHP1 (minimum SP25) est installé et utilisé comme contrôleur de domaine pour le CTS+, au moins pour la configuration des systèmes SAP BusinessObjects.
   Pour en savoir plus sur la configuration du domaine de transport, voir Configuration du domaine de transport.
3. Le plug-in CTS est installé sur SAP Solution Manager (le plug-in CTS est issu de SL Toolset 1.0 SP02. Il est recommandé d'utiliser le plug-in CTS disponible le plus récent.)
   Pour en savoir plus sur l'installation du plug-in CTS requis, consultez la note SAP 1533059.

4. Les systèmes *SAP Business Warehouse 7.0* (SPS 24 ou version supérieure) sont installés. Pour en savoir plus, consultez la note SAP 1369301.
5. Le paysage de transport de SAP Business Warehouse (SAP BW) est configuré dans le CTS (Change and Transport System).
6. Les notes 1692417 et 1860594 ont été implémentées sur l'ordinateur qui héberge le service Web de déploiement CTS.

16.7.2 Pour configurer la plateforme de BI et l'intégration CTS+



Le système de gestion de transport (TMS) qui fait partie du système de transport des modifications (CTS) permet de transporter les modifications entre les systèmes SAP au sein d'un paysage. Il gère les systèmes connectés, leurs routes et les importations dans ses systèmes. Pour en savoir plus sur le système de gestion de transport, voir Transport Management System (BC-CTS-TMS)

Le CTS+ permet de collecter des fichiers de l'extérieur et de les distribuer au sein d'un paysage de transport. L'interface utilisateur Web de Transport Organizer, qui fait partie du CTS+, gère les requêtes de transport et les objets qu'elle contient. Pour en savoir plus, voir Transport Management System (BC-CTS-TMS)

Vous pouvez intégrer la gestion des promotions de la plateforme de BI au CTS+ et à SAP BW à l'aide de requêtes de transport CTS.

> **Remarque**
>
> Pour activer l'intégration de la plateforme de BI avec SAP Solution Manager, vous devez définir le type d'application "BOLM" dans le paysage SAP Solution Manager.

Procédez comme suit pour intégrer la plateforme de BI et CTS+ :

1. Activez le service Web d'exportation CTS.
2. Configurez les paramètres CTS dans l'outil de gestion des promotions.
3. Configurez le système d'importation de la plateforme de BI dans SAP Solution Manager.

Informations associées

Pour activer le service Web d'export CTS [page 670]
Pour configurer les paramètres CTS+ dans l'outil de gestion des promotions [page 670]
Pour configurer la plateforme de BI et l'intégration CTS+ [page 669]

16.7.2.1 Pour activer le service Web d'export CTS

Pour configurer le système de la plateforme de BI, vous devez activer le service Web d'exportation CTS dans l'outil Web SOA Management.

1. Pour démarrer l'application, saisissez le code de transaction SOAMANAGER dans SAP Solution Manager. Une fois l'authentification requise effectuée, la console SOA Management s'ouvre dans un navigateur Web.

   Pour en savoir plus sur SOA Management et la configuration d'une extrémité de service à l'aide de SAP Solution Manager 7.0, consultez la page Configuring a Service Provider. Pour SAP Solution Manager 7.1, consultez la page Configuring a Service Provider.
2. Dans l'onglet *Application and Scenario Communication (Application et communication de scénario)*, cliquez sur *Single Service Configuration (Configuration de service unique)*.

   Le service Web d'exportation CTS est nommé `EXPORT_CTS_WS`
3. Dans l'onglet *Configuration*, créez ou modifiez la terminaison de service.
4. Dans l'onglet *Security* (Sécurité), configurez le protocole de transport et la méthode d'authentification.
5. Dans l'onglet *Transport Settings* (Paramètres de transport), définissez une autre URL d'accès pour l'accès approprié à la terminaison de service.

16.7.2.2 Pour configurer les paramètres CTS+ dans l'outil de gestion des promotions

La section suivante décrit les étapes de configuration à suivre dans l'application de la CMC pour configurer le CTS+ en vue de l'utiliser avec l'outil de gestion des promotions.

1. Sur la page *Travaux de promotion*, cliquez sur *Paramètres CTS*, puis sur *Paramètres BW*.
2. Sur la page *Systèmes BW*, cliquez sur *Ajouter* pour ajouter un système BW au paysage.
3. Sur la page *Ajouter système*, saisissez les informations suivantes :
   - *SID du système BW hôte* : spécifiez l'ID de système (SID) de l'ordinateur hôte SAP BW/ABAP.
   - *Nom d'hôte* : spécifiez l'adresse IP de l'ordinateur hôte.
   - *Numéro du système* : saisissez le numéro du système hôte.
   - *Client* : fait référence aux informations système de l'ordinateur client.
   - *Utilisateur* et *Mot de passe* : spécifiez le nom d'utilisateur et le mot de passe pour l'ordinateur client dans ces champs.
   - *Langue* : spécifiez votre choix de langue dans ce champ.

4. Cliquez sur *OK* pour ajouter le système à votre paysage.

> **Remarque**
>
> Après avoir ajouté un système BW à votre paysage, vous pouvez utiliser *Modifier* ou *Supprimer* sur les pages *Systèmes BW* pour modifier les systèmes de votre paysage.

5. Sur la page *Travaux de promotion*, cliquez sur *Paramètres CTS* puis sur *Paramètres du service Web*.
6. Sur la page *Paramètres du service Web*, saisissez l'URL du service Web et les informations d'utilisateur.

> **Remarque**
>
> Si vous ne connaissez pas ces informations, vous pouvez les obtenir auprès de l'administrateur Solution Manager.

7. Cliquez sur *Enregistrer* et *Fermer* pour terminer l'ajout des paramètres de service Web.
8. Créez un fichier de mappage pour le système CMS de gestion des promotions de la plateforme de BI.

   Procédez comme suit dans le système de développement de la plateforme de BI pour créer un fichier texte avec les détails de connectivité pour activer le mappage :

   a. Sur le CMS de gestion des promotions de la plateforme de BI, accédez au répertoire racine et créez un dossier nommé **`LCM`** à l'emplacement `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/`.
   b. Créez un fichier texte nommé `LCM_SOURCE_CMS_SID_MAPPING.properties`, et saisissez l'un des éléments suivants dans le fichier :
      - `<Nom complet du système source de la plateforme SAP BI avec domaine>@<numéro de port du CMS> = <nom logique du système source utilisé dans la configuration du CTS >`
      - `<Adresse IP du système source de la plateforme SAP BI>@<numéro de port du CMS> = <nom logique du système source utilisé dans la configuration du CTS >`

   Par exemple :

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **Remarque**
>
> Dans le cas d'un environnement en cluster, copiez le fichier `LCM_SOURCE_CMS_SID_MAPPING.properties` sur le système où est exécuté le serveur de traitement adaptatif.

Pour en savoir plus sur les étapes de configuration à suivre pour les systèmes non ABAP, voir Making Transport Settings in the Application.

16.7.2.3 Pour configurer le système d'importation de la plateforme de BI dans SAP Solution Manager

1. Connectez-vous au système SAP Solution Manager.
2. Saisissez la transaction `stms` et appuyez sur `Entrée`.
3. Configurez BOLM comme type d'application.
   a. Accédez à *Overview (Synthèse)* > *Systems (Systèmes)*.
   b. Accédez à *Extras (Autres fonctions)* > *Application Type (Type d'application)* > *Configure (Configurer)*.
   c. Sélectionnez *New Entries (Nouvelles entrées)*.
   d. Dans le champ *Application Type (Type d'application)*, saisissez **`BOLM`**.
   e. Saisissez la description.
   f. Dans le champ *Support Details (Détails de prise en charge)*, saisissez **`http://service.sap.com (ACH: BOJ-BIP-DEP)`**
   g. Choisissez *Table View (Vue Tableau)* > *Save (Sauvegarder)*.
   h. Confirmez l'invite en choisissant *Yes (Oui)*.
4. Pour travailler avec des langues différentes, vous pouvez conserver un texte traduit en procédant comme suit :
   a. Choisissez *Goto (Saut)* > *Translation (Traduction)*.
   b. Sélectionnez les langues dans lesquelles vous souhaitez traduire le texte.
   c. Saisissez les valeurs traduites dans les champs *Description* et *Support Details (Détails de la prise en charge)*.
   d. Confirmez votre choix dans la boîte de dialogue.
   e. Choisissez *Continue (Continuer)*.
   f. Choisissez *Table View (Vue Tableau)* > *Save (Sauvegarder)*.
   g. Confirmez l'invite.

   Le domaine TMS est à présent prêt à prendre en charge l'utilisation du contenu Business Intelligence dans CTS.
5. Dans le CTS+, définissez le système source de la plateforme de BI comme système d'exportation.

   > **Remarque**
   >
   > Pour en savoir plus sur la création d'un système non ABAP comme système source, consultez la page Defining and Configuring Non-ABAP Systems.

6. Dans le CTS+, configurez le système d'importation de la plateforme de BI en procédant comme suit :

   > **Remarque**
   >
   > Vous pouvez définir un SID comme référence au système d'importation de la plateforme de BI.

   a. Créez un système non ABAP comme système d'importation.

      Pour en savoir plus, consultez la page Defining and Configuring Non-ABAP Systems.
   b. Spécifiez la méthode de déploiement *Other (Autre)* et désélectionnez toutes les autres options.
   c. Sélectionnez *Save (Sauvegarder)*.

d. Confirmez votre choix dans la boîte de dialogue de distribution.
La vue Tableau permettant de configurer les paramètres du système d'importation s'affiche.

e. Choisissez *Edit (Traiter)* > *New Entries (Nouvelles entrées)*.

f. Dans l'écran "Change View CTS:System details for handling of application types" (Modifier la vue CTS : Détails du système pour le traitement des types d'application), procédez comme suit :

   1. Dans le champ *Deploy Method (Méthode de déploiement)*, sélectionnez *application-specific Deployer (EJB) (Déployeur spécifique à l'application)*.
   2. Dans le champ *Deploy URI (Déployer l'URI)*, saisissez l'URI suivante : **`http://<nom serveur Web BOE>:<port du serveur Web>/BOE/LCM/CTSServlet?&cmsName=<nom destination BOE>:<portCMS>&authType=<type d'authentification BOE>`**
      où
      - "nom serveur Web BOE" est le nom ou l'adresse IP de l'ordinateur où est exécuté le serveur Web de la plateforme de Business Intelligence.
      - "port du serveur Web" est le numéro de port du serveur Web de la plateforme de Business Intelligence.
      - "nom destination BOE" est le nom de l'ordinateur sur lequel est exécuté le CMS (Central Management Server) de la plateforme de Business Intelligence cible.
      - "port CMS" est le numéro de port du CMS cible.
      - "type d'authentification BOE" est le type d'authentification utilisateur pour l'importation de contenu Business Intelligence. Les types d'authentification pris en charge sont secEnterprise, secLDAP, secWinAD et secSAPR3.
   3. Dans le champ *User (Utilisateur)*, saisissez le nom d'utilisateur de la plateforme de Business Intelligence.
   4. Dans le champ *Password (Mot de passe)*, saisissez le mot de passe de la plateforme de Business Intelligence.
   5. Sélectionnez *Save (Sauvegarder)* pour enregistrer les paramètres.

Si vous avez besoin de plusieurs systèmes d'importation, répétez les étapes ci-dessus pour créer autant de systèmes de destination que nécessaire. Pour configurer des itinéraires de transport entre le système source et le système cible après la création des systèmes de destination, consultez la page Configuring Transport Routes.

16.7.2.4 Pour exporter depuis la plateforme de BI vers CTS+ avec SSL

16.7.2.4.1 Pour configurer SSL pour CTS+

Pour configurer SSL pour CTS+, vous devez configurer SSL sur le serveur d'applications ABAP. Pour en savoir plus, voir Configuring the SAP Web AS for Supporting SSL.

16.7.2.4.2 Pour configurer le certificat SSL côté client

Pour configurer le certificat SSL côté client, vous devez importer le certificat de serveur ou le certificat CA approuvé dans le stockage de clés de la JVM.

1. Sauvegardez les fichiers `cacerts` depuis le répertoire `<REPINSTALL>\win64_x64\sapjvm\jre\lib\security`.
2. Importez le certificat dans la JVM Tomcat qui héberge le fichier `BOE.war` à l'aide des paramètres suivants :

```
<REPINSTALL>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer
-keystore cacerts
```

3. Redémarrez Tomcat.

16.7.2.4.3 Pour configurer le service Web d'export CTS+

Pour configurer le service Web d'export CTS+ prenant en charge HTTPS (`EXPORT_CTS_WS`), vous pouvez créer une extrémité HTTPS.

> **Remarque**
>
> Vous pouvez également faire basculer votre extrémité HTTP existante vers HTTPS.

1. Utilisez le code de transaction **`soamanager`**. Dans l'onglet *Provider Security (Sécurité du fournisseur)*, sous *Communication Security (Sécurité de communication)*, sélectionnez *SSL over HTTP (Transport Channel Security) (SSL sur HTTP (Canal de communication sécurisé))* et sous *Transport Channel Authentication (Authentification du canal de communication)*, sélectionnez *User ID/Password (ID utilisateur/Mot de passe)*.
2. Dans l'onglet *Transport settings (Paramètres de communication)*, sous *Transport Binding (Liaison de communication)*, sélectionnez *HTTPS* pour *Calculated Protocol (Protocole calculé)*.

16.7.2.4.4 Pour configurer la gestion des promotions pour SSL

> **→ N'oubliez pas**
>
> Importez le certificat de serveur ou la certification CA approuvée dans le stockage de clés de la JVM.

1. Dans l'onglet *Gestion des promotions* de la CMC, cliquez sur *Paramètres* > *Paramètres CTS* > *Paramètres du service Web* >.
2. Assurez-vous que le paramètre *URL du service Web* inclut `https://` et le numéro de port configuré ci-dessus.

> **Remarque**
>
> *Promouvoir par CTS* ne sera pas affiché dans la liste *Destination du travail* ou dans la boîte de dialogue *Remplacements* si l'URL spécifiée n'est pas accessible. Si la connexion SSL entre la gestion des promotions et CTS+ échoue, une erreur sera consignée dans le fichier journal de la CMC.

16.7.2.5 Pour importer depuis CTS+ vers la plateforme de BI avec SSL

16.7.2.5.1 Pour configurer Tomcat sur la plateforme de BI pour l'utilisation de HTTPS

Pour configurer Tomcat sur la plateforme de BI pour utiliser HTTPS, vous devez effectuer les étapes suivantes sur l'ordinateur sur lequel la plateforme de BI est installée.

1. Créez une paire de clés de serveur, un certificat et un stockage de clés.
   a. Exécutez `<REPINSTALL>\win64_x64\sapjvm\jre\bin\keytool.exe` à l'aide des paramètres suivants :

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. Lorsque vous y êtes invité, saisissez les informations suivantes :
      - Vos nom et prénom
      - Le nom de votre unité d'entreprise
      - Le nom de votre entreprise
      - Le nom de votre ville ou localité
      - Le nom de votre Etat ou province
      - Le code-pays à deux lettres correspondant à cette unité

      Une chaîne mise en forme s'affichera (par exemple `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Saisissez **`yes`** et appuyez sur `Entrée` pour confirmer.
2. Envoyez la demande de certificat de serveur à une autorité de certification (CA).
3. Importez le certificat de serveur signé dans le stockage de clés du serveur à l'aide des paramètres suivants :

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. Configurez le fichier de configuration Tomcat `server.xml` pour activer HTTPS et utiliser le stockage de clés du serveur que vous avez créé.
5. Redémarrez Tomcat et testez la connexion en accédant à l'URL suivante dans un navigateur : `https://<NOMSERVEUR>:<NUMEROPORTSSL>`

Informations associées

Pour configurer SSL pour CTS+ [page 673]

16.7.2.5.2 Pour configurer CTS+ pour SSL

Pour configurer CTS+ pour SSL, vous devez créer un PSE de client SSL et y importer un certificat.

Informations associées

Pour configurer SSL pour CTS+ [page 673]

16.7.2.5.3 Mise à jour des systèmes de test et de production dans CTS+ pour utiliser HTTPS

Pour activer HTTPS sur les systèmes de test et de production, procédez comme suit :

1. Utilisez le code de transaction STMS.
2. Cliquez sur *Présentation du système*.
3. Sélectionnez le système de test ou de production, puis cliquez sur *Atteindre* > *Types d'application* > *Méthode de déploiement*.
4. Assurez-vous que le paramètre *Deploy URI (Déployer l'URI)* inclut `https://` et un numéro de port HTTPS configuré.

16.7.3 Pour promouvoir un travail à l'aide de CTS

Cette section décrit le workflow pris en charge par l'outil de gestion des promotions pour promouvoir les objets du CMS (Central Management Server) de la plateforme de Business Intelligence depuis le système source jusqu'au système de destination à l'aide du CTS (Change Transport System). Pour utiliser le CTS afin de promouvoir un travail, effectuez les étapes suivantes :

1. Lancez l'outil de gestion des promotions à l'aide de l'authentification SAP, puis créez un travail.

   Pour en savoir plus sur la création d'un travail, voir la section "Création d'un travail" dans le lien associé ci-dessous.

   > **Remarque**
   >
   > Veillez à sélectionner "SAP" comme type d'authentification dans l'écran de connexion du système source.

2. Dans la liste déroulante *Destination*, sélectionnez l'option *Promouvoir par CTS*.

3. Cliquez sur *Créer*.
   L'écran *Ajouter des objets à partir du système* s'affiche. Les dossiers et les sous-dossiers s'affichent ici sous forme d'arborescence.
4. Accédez au dossier dans lequel vous voulez sélectionner l'objet.
5. Sélectionnez l'InfoObject que vous voulez ajouter au travail et cliquez sur *Ajouter*. Si vous souhaitez ajouter un InfoObject et fermer l'écran *Ajouter des objets*, cliquez sur *Ajouter et fermer*.
   L'InfoObject est ajouté au travail et l'écran *Travaux de promotion* apparaît.

   > **Remarque**
   >
   > L'écran Travaux de promotion permet d'effectuer les opérations suivantes :
   > - Utiliser l'option *Ajouter des objets* pour ajouter d'autres InfoObjects au travail. Pour en savoir plus, voir Ajout d'un InfoObject à un travail.
   > - Utiliser l'option *Gérer les dépendances* pour gérer les dépendances de l'InfoObject sélectionné. Les dépendances SAP BW de l'objet sont affichées dans l'interface utilisateur, où l'utilisateur peut les sélectionner.
   > Pour en savoir plus, voir Gestion des dépendances de travaux.

6. Cliquez sur *Promouvoir*.
   L'écran *Promouvoir* apparaît et affiche l'ID, le propriétaire et une brève description de la demande de transport actuellement configurée par défaut.
7. Le lien hypertexte *Demandes de transport* permet d'effectuer les opérations suivantes :
   - Afficher les détails de la demande de transport.
   - Changer les paramètres de la demande de transport par défaut.
   - Choisir une autre demande de transport.
   - Créer une demande de transport.

   1. Cliquez sur le lien hypertexte *Demandes de transport* pour ouvrir l'interface utilisateur Web de *Transport Organizer*.
   2. Si vous êtes invité à fournir des références de connexion, connectez-vous en utilisant des références utilisateur valides pour le système du contrôleur de domaine du CTS.
   3. Actualisez l'écran *Promouvoir* pour afficher vos mises à jour.

   Pour en savoir plus sur l'utilisation de l'interface utilisateur Web de *Transport Organizer*, consultez la page Transport Organizer Web UI.
8. Pour afficher les détails des dépendances des objets SAP BW, cliquez sur le lien hypertexte *Dépendances de second niveau*.

> **Remarque**
>
> Seuls les objets verrouillés dans une demande s'affichent lorsque vous cliquez sur le lien hypertexte *Dépendances de second niveau*. Si la demande a été émise, vous ne pouvez afficher aucune dépendance. De plus, ce lien hypertexte est grisé en l'absence de dépendance de second niveau active.

9. Cliquez sur *Promouvoir*.
10. Fermez le travail.
    L'écran principal de la gestion des promotions s'affiche. Le statut du travail que vous avez créé est à présent *Exporté au format CTS*.
11. Libérez l'objet de la plateforme de BI dans le système de destination en effectuant les étapes suivantes :
    a. Cliquez sur le lien affiché dans la colonne de statut du travail à promouvoir.
       La fenêtre *Statut de la promotion* s'affiche.
    b. Cliquez sur *Etat de la requête*.
       L'interface utilisateur Web de *Transport Organizer* s'affiche.
    c. Si le statut de la demande est *Modifiable*, cliquez sur *Release (Libérer)* pour libérer la demande de transport de l'objet de la plateforme de BI. Pour en savoir plus sur la libération des demandes de transport contenant des objets non ABAP, consultez la page Releasing Transport Requests with Non-ABAP Objects.
    d. Fermez l'interface utilisateur Web de *Transport Organizer*.
12. Pour afficher les dépendances des objets SAP BW, cliquez sur le lien hypertexte *Liste des dépendances BW*.

> **Remarque**
>
> Nous recommandons de prendre contact avec l'équipe SAP BW pour obtenir des mises à jour relatives aux dépendances SAP BW et à leur libération, l'équipe travaillant actuellement sur ces objets.

13. Fermez la fenêtre *Statut de la promotion*.
14. Importez l'objet de la plateforme de BI dans le système de destination en effectuant les étapes suivantes :
    a. Connectez-vous au contrôleur de domaine de CTS+.
    b. Appelez la transaction **STMS** pour saisir le système de gestion du transport.
    c. Cliquez sur l'icône *Présentation de l'importation*.
       L'écran *Présentation de l'importation* apparaît et vous pouvez voir ici les éléments de la file d'attente d'importation en provenance de tous les systèmes.
    d. Choisissez l'ID système du système Gestion des promotions de destination.
       Vous pouvez voir la liste des demandes de transport pouvant être importées dans le système.
    e. Cliquez sur *Actualiser*.
    f. Importez les demandes de transport appropriées. Pour en savoir plus, consultez la page Importing Requests.

       Pour obtenir des informations générales sur l'importation de demandes de transport avec du contenu BOLM, consultez la page Importing Transport Requests with Non-ABAP Objects.
15. Si l'objet sélectionné présente des dépendances SAP BW, procédez comme suit :
    a. Libérez les dépendances SAP BW vers le système de destination en procédant comme suit :
       1. Connectez-vous au système SAP BW source.
       2. Appelez la transaction SE09. L'écran *Transport Organizer* apparaît.
       3. Cliquez sur *Affichage*. La demande SAP BW s'affiche.
       4. Cliquez sur la demande SAP BW et développez-la pour afficher les travaux créés pour les dépendances.

5. Cliquez avec le bouton droit de la souris sur la demande associée à l'objet SAP BW principal et sélectionnez *Libérer directement*. Répétez cette étape pour libérer séparément tous les travaux associés à chaque dépendance.
6. Cliquez avec le bouton droit sur la requête associée à l'objet BW principal et sélectionnez *Libérer directement*.
7. Actualisez l'écran jusqu'à ce que les demandes soient libérées.

> **Remarque**
>
> Vous pouvez afficher les journaux associés à une demande en cliquant deux fois dessus.

b. Importez les dépendances SAP BW vers le système de destination en procédant comme suit :
   1. Connectez-vous au système SAP BW de destination.
   2. Appelez la transaction STMS pour saisir le système de gestion du transport.
   3. Cliquez sur l'icône *Présentation de l'importation*. L'écran *Présentation de l'importation* s'affiche.
   4. Cliquez deux fois sur l'ID système de la destination SAP BW. Vous pouvez voir la liste des demandes de transport pouvant être importées dans le système.
   5. Importez les demandes de transport appropriées. Pour en savoir plus, consultez la page Importing Requests.
      Pour en savoir plus sur le transport avec file d'attente d'importation, consultez la page Transports with Import Queues.

16. Connectez-vous au système de destination pour afficher le statut du travail promu.

Pour en savoir sur le CTS générique, consultez la page Configuring Target Systems for Further Applications

Informations associées

Permet de créer un travail [page 616]
Pour gérer les dépendances d'un travail [page 622]

16.8 Utilisation de l'assistant de gestion des promotions

L'assistant de gestion des promotions permet de copier des ressources Business Intelligence (BI) d'un référentiel à un autre, facilement et en quelques clics seulement.

Il prend en charge les scénarios de promotion suivants :

- Exportation d'une ressource BI d'un système source vers un fichier LCMBIAR.
- Réplication d'une ressource BI d'un système source vers un système de destination.
- Importation d'un fichier LCMBIAR vers un système de destination.

Avec l'assistant de gestion des promotions, vous pouvez maintenant promouvoir la totalité du contenu d'un référentiel ou le contenu sélectif d'un référentiel, sans devoir utiliser la ligne de commande. En effet, son interface graphique conviviale simplifie la réalisation des tâches d'administration.

Pour plus d'informations concernant les meilleures pratiques applicables à l'Assistant de gestion des promotions, reportez-vous à la note SAP 2531264.

> ⚠ Attention
>
> L'assistant de gestion des promotions ne prend pas en charge la reprise. Après avoir promu des ressources BI, vous ne pouvez donc pas restaurer le système de destination vers son état précédent.

> ⓘ Remarque
>
> Assurez-vous d'examiner la valeur de mémoire avant de lancer la promotion d'objets. La valeur Xms doit être inférieure ou égale à la valeur Xmx.

> ⓘ Remarque
>
> Si vous disposez d'objets QaaWs, vous devez configurer correctement le système de destination.

> → Conseil
>
> Afin d'augmenter les performances, désactivez l'audit et la surveillance dans le CMC du système de destination. Pour en savoir plus, voir le Guide d'administration de la plateforme Business Intelligence > Audit.

16.8.1 Exclusion d'objets de la promotion

Vous pouvez sélectionner les objets dans la liste fournie ci-dessous et les exclure d'un travail de promotion pour enregistrer l'espace disque et réduire le temps de migration.

Un travail de promotion migre chaque actif de BI de la source au système cible. Par conséquent, les actifs, qui sont spécifiques au système source et qui ne sont pas utiles dans le système de destination, sont également migrés. Pour exclure les actifs de BI de la promotion, suivez les étapes ci-dessous.

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Ouvrez le fichier *PromotionManagementWizard.ini* dans un éditeur de texte.
3. Recherchez et localisez la chaîne *# Liste des types à exclure automatiquement de l'exportation complète/sélective.*
   Vous trouverez le code `-Dcom.sap.businessobjects.pmw.exclude.kind={}` sous la chaîne.
4. Référez-vous à la liste d'objets ci-dessous et ajoutez les objets à exclure entre les `{}`.
5. Enregistrez le fichier.

Les objets mentionnés dans le code seront exclus lors de l'exécution d'un travail de promotion.

Reportez-vous à la table ci-dessous pour la liste des objets pouvant être exclus d'un travail de promotion.

CustomMappedAttributes	DFS.Parameter	Discussions	GDPRObject
LCMJOBS	LCMOverrides	LCMScanHistory	LCMSettings
LANDSCAPE	LANDSCAPEConnection	LIVEOffice	MoN.MBEANConfig
MON.ManagedEntityStatus	MON.MonAppDataStore	Mon.Probe	Mon.Subscription

NotificationScheduleObject	OverrideEntry	PlatformSearchApplicationStatus	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator
XL.XcelsiusApplication	busobjectreporter	Explorer	LumiraExtensions

16.8.2 Quand utiliser l'assistant de gestion des promotions

Plusieurs options sont disponibles pour la gestion des promotions. Le tableau ci-dessous vous permet d'identifier les circonstances dans lesquelles l'assistant de gestion des promotions est la solution la mieux adaptée à vos besoins.

Options disponibles pour la gestion des promotions

	Assistant de gestion des promotions	**Gestion des promotions à l'aide de l'option de ligne de commande**	**Gestion des promotions dans la Central Management Console**
Objectif	Promotion en une seule opération	Automatisation	Projet
Étendue de la promotion	Nombre élevé de ressources BI	Nombre élevé de ressources BI	Peu de ressources BI
Travail	Aucune possibilité de créer un travail pouvant être réexécuté par le Job Server	Possibilité de créer un travail pouvant être réexécuté par le Job Server	Possibilité de créer un travail pouvant être réexécuté par le Job Server

> **Remarque**
>
> Les fichiers LCMBIAR sont compatibles avec chaque option de gestion des promotions, indépendamment de celle sélectionnée.

16.8.2.1 Définition des paramètres de gestion des promotions

1. Spécifiez les paramètres de gestion des promotions de votre choix. Voici quelques informations destinées à vous aider :

Paramètre	Description
Dossier temporaire	ⓘ Remarque Assurez-vous d'allouer suffisamment d'espace pour le Dossier temporaire. La quantité d'espace libre doit être au moins deux fois plus élevée que la quantité d'espace requise.
Emplacement du journal	L'emplacement du journal est défini par défaut. Vous pouvez le modifier ultérieurement. Les modifications sont immédiatement appliquées dans les paramètres de gestion des promotions.
Niveau de journalisation	Vous pouvez définir le niveau de journalisation sur les valeurs suivantes : • Par défaut • Faible • Moyen • Elevé Le niveau de journalisation est défini sur "Par défaut" si vous ne le modifiez pas.
Langue	Vous pouvez définir l'assistant de gestion des promotions sur votre langue préférée.

2. Cliquez sur *Suivant*.

16.8.3 Scénario

L'assistant de gestion des promotions prend en charge trois types de scénario de promotion :

- Du système Live vers le fichier LCMBIAR : Vous copiez des objets d'un CMS Live vers un fichier LCMBIAR.
- D'un système CMS Live vers un autre : Vous copiez des objets d'un système source CMS Live vers un système de destination CMS Live.
- D'un fichier LCMBIAR vers un système Live : Vous importez des objets d'un fichier LCMBIAR vers un système de destination CMS Live

16.8.3.1 Promotion d'objets d'un système source CMS Live vers un fichier LCMBIAR

Pour promouvoir des objets d'un CMS Live vers un fichier LCMBIAR, procédez comme suit :

1. Sélectionnez *Exporter*.
2. Pour définir le CMS source, effectuez l'une des opérations suivantes :
   - Pour utiliser le CMS central comme CMS source, cochez la case *Transformer le CMS central en CMS source*.

- Dans la section Source, entrez les informations suivantes :
  - Nom du CMS
  - Utilisateur
  - Mot de passe
  - Authentification
3. Dans la zone *Destination*, cliquez sur *Choisir* pour sélectionner l'emplacement du fichier LCMBIAR.
4. (Facultatif) Saisissez un mot de passe pour le chiffrement du fichier LCMBIAR.

> **Remarque**
>
> Le processus de promotion prend plus de temps si vous chiffrez le fichier LCMBIAR.

5. Cliquez sur *Suivant* pour sélectionner les objets à exporter.

16.8.3.2 Promotion d'objets d'un système source CMS Live vers un système de destination CMS Live

Pour promouvoir des objets d'un système source CMS Live vers un système de destination CMS Live, procédez comme suit :

1. Sélectionnez *Promouvoir*.
2. Pour définir le CMS source, effectuez l'une des opérations suivantes :
   - Pour utiliser le CMS central comme CMS source, cochez la case *Transformer le CMS central en CMS source*.
   - Dans la section Source, entrez les informations suivantes :
     - Nom du CMS
     - Utilisateur
     - Mot de passe
     - Authentification
3. Pour définir le CMS de destination, effectuez l'une des opérations suivantes :
   - Pour utiliser le CMS central comme CMS de destination, cochez la case *Transformer le CMS central en CMS de destination*.
   - Dans la section *Destination*, entrez les informations suivantes :
     - Nom du CMS
     - Utilisateur
     - Mot de passe
     - Authentification
4. Cliquez sur *Suivant* pour sélectionner les objets à copier du système source vers le système de destination.

16.8.3.3 Promotion d'objets d'un fichier LCMBIAR vers un système de destination CMS Live

Pour promouvoir des objets d'un fichier LCMBIAR vers un CMS Live, procédez comme suit :

1. Sélectionnez *Importer*.
2. Pour définir le CMS de destination, effectuez l'une des opérations suivantes :
   - Dans la section *Destination*, cochez la case *Transformer le CMS central en CMS de destination*.
   - Dans la section *Destination*, entrez les informations suivantes :
     - Nom du CMS
     - Utilisateur
     - Mot de passe
     - Authentification
3. Dans la section *Source*, cliquez sur *Choisir* pour sélectionner le fichier LCMBIAR à importer.
4. (Facultatif) Saisissez un mot de passe pour le chiffrement du fichier LCMBIAR.

   > **Remarque**
   >
   > Le processus de promotion prend plus de temps si vous chiffrez le fichier LCMBIAR.

5. Cliquez sur *Suivant* pour sélectionner les objets à importer.

16.8.4 Objets

L'assistant de gestion des promotions prend en charge deux types de promotion de contenu :

- Promotion de contenu complet
- Promotion de contenu sélectif

Le table ci-après explique les caractéristiques de chaque type :

Types de promotion de contenu	Contenu promu	Dépendances de contenu
Promotion de contenu complet	Vous promouvez la totalité du contenu ci-dessous du système source vers le système de destination : • Objets (utilisateurs, documents, univers, connexions, etc.) • Instances • Relations entre les objets • Sécurité d'objet	Il n'est pas nécessaire d'évaluer les dépendances, puisque les relations sont conservées. Vous passez directement de l'étape Objets actuelle à l'étape Résumé.

Types de promotion de contenu	Contenu promu	Dépendances de contenu
Promotion de contenu sélectif	Vous promouvez, vers le système de destination, le contenu que vous avez sélectionné dans le système source. Le contenu peut prendre la forme de ce qui suit : • Objets (utilisateurs, documents, univers, connexions, etc.) • Instances • Relations entre les objets • Sécurité d'objet	Étant donné que vous ne promouvez pas la totalité du contenu du système source vers le système de destination, les dépendances doivent être évaluées.

16.8.4.1 Promotion de la totalité du contenu

Pour promouvoir la totalité du contenu du système source vers le système de destination, procédez comme suit :

1. Sélectionnez *Promotion de contenu complet*.

   Tous les objets sont sélectionnés pour promotion.
2. Cliquez sur *Suivant* pour examiner le contenu que vous avez sélectionné.

16.8.4.2 À propos de la promotion du content sélectif

Avant de promouvoir le contenu sélectif du système source vers le système de destination, vous devez définir les options d'exportation. Cette opération permet de récupérer les paramètres que vous avez sélectionnés sur le système source comme devant être promus vers le système de destination.

16.8.4.2.1 À propos des options d'exportation

Si vous souhaitez récupérer les paramètres spécifiés sur le système source et les promouvoir sur le système de destination, vous devez définir les paramètres suivants dans la section Options d'exportation :

- Instances d'objet
- Dépendances entre les objets
- Sécurité
- Commentaire
- Travaux de fédération

- Résolution des conflits de noms

Instances d'objet

Instances d'objet	Description
Exporter toutes les instances d'un objet lorsque l'objet est sélectionné	Vous exportez les objets sélectionnés avec toutes leurs instances.
Exporter uniquement les instances récurrentes d'un objet lorsque l'objet est sélectionné	Vous exportez les objets sélectionnés uniquement avec leurs instances récurrentes. Par exemple, si vous avez planifié l'actualisation hebdomadaire et l'actualisation mensuelle d'un document, ce document et ses deux instances récurrentes seront exportés pendant l'exportation.
Ne pas exporter les instances d'objet	Vous pouvez exporter uniquement les objets sélectionnés. Leurs instances ne sont pas exportées.

Dépendances entre les objets

Dépendances entre les objets	Description
Inclure les dépendances lors de la sélection d'objets	Vous exportez les objets sélectionnés avec toutes leurs dépendances. **Remarque** L'option est activée par défaut.
Exclure les dépendances lors de la sélection d'objets	Vous exportez uniquement les objets sélectionnés sans toutes leurs dépendances.

Sécurité

Sécurité	Description
Inclure la sécurité des objets	Vous exportez les objets sélectionnés avec leurs paramètres de sécurité d'objet.
Inclure la sécurité des utilisateurs	Vous exportez les objets sélectionnés avec leurs paramètres de sécurité d'utilisateur.
Inclure la sécurité des applications	Vous exportez les objets sélectionnés avec leurs paramètres de sécurité d'application.

Sécurité	Description
Inclure la sécurité de niveau supérieur	Vous exportez les paramètres de sécurité définis dans le dossier racine. **⚠ Attention** Cette option remplace les paramètres de sécurité définis dans le système de destination. Il est conseillé d'utiliser cette option avec modération.

Commentaire

Commentaire	Description
Inclure les commentaires	Vous exportez les objets sélectionnés avec tous leurs commentaires.
Préférences de la zone de lancement BI pour les groupes d'utilisateurs	Si vous cochez la case, les préférences du groupe d'utilisateurs de la zone de lancement BI du système source sont activées et les préférences par défaut sont définies dans le système de destination.

Préférences BI du groupe d'utilisateurs

Préférences BI du groupe d'utilisateurs	Description
Écraser les préférences BI des groupes d'utilisateurs	Si vous cochez la case, les préférences du groupe d'utilisateurs de la zone de lancement BI du système source sont activées et les préférences par défaut sont définies dans le système de destination. **ⓘ Remarque** Si vous faites la promotion d'un document Web Intelligence qui utilise la personnalisation à l'aide d'un fichier BIAR, assurez-vous d'activer cette option pour importer la personnalisation.

Travaux de fédération

Travaux de fédération	Description
Inclure la relation des travaux de fédération	Vous importez les objets sélectionnés sans modifier les relations entre les travaux de fédération.

Résolution des conflits de noms

Résolution des conflits de noms	Description
Résolution des conflits de noms	Si un objet sélectionné porte le même nom qu'un objet dans le système de destination, mais possède un CUID différent, une copie de l'objet sélectionné sera créée dans le système de destination. Si vous n'activez pas cette option, l'objet sélectionné portant le même nom qu'un objet dans le système de destination, mais avec un CUID différent ne sera pas copié dans le système de destination.

16.8.4.2.2 Promotion du contenu sélectif

Pour promouvoir le contenu sélectif du système source vers le système de destination, procédez comme suit :

1. Sélectionnez *Promotion de contenu sélectif*.
2. Pour définir *Options d'exportation*, cliquez sur *Options*.
3. (Facultatif) Cochez la case *Appliquer le filtre chronologique* pour filtrer les objets en fonction d'une plage de dates et d'heures.
4. Sélectionnez les objets que vous souhaitez exporter.
5. Pour évaluer les dépendances d'un objet, cochez la case associée sous l'icône des dépendances.

   > **Remarque**
   >
   > Par défaut, toutes les cases correspondant aux dépendances sont cochées. Si vous ne souhaitez pas évaluer les dépendances d'un objet, décochez la case.

6. Cliquez sur *Suivant* pour évaluer les dépendances.

16.8.5 Dépendances

Si vous optez pour promouvoir le contenu sélectif du système source vers le système de destination, les dépendances du contenu sélectif peuvent être évaluées. L'étape *Dépendances* fournit une vue d'ensemble des objets sélectionnés identifiés comme dépendances.

Vous pouvez visualiser les informations suivantes concernant les dépendances des objets sélectionnés :

- Titre
- CUID
- Date

Vous pouvez sélectionner les objets identifiés comme des dépendances :

1. En fonction du niveau de détails à visualiser, effectuez l'une des opérations suivantes :

- Cliquez sur *Tout développer* pour afficher les détails de chaque dépendance.
- Cliquez sur *Tout réduire* pour afficher uniquement les objets dépendants.

2. Sélectionnez les dépendances à promouvoir.

> **Remarque**
>
> Par défaut, toutes les cases correspondant aux dépendances sont cochées. Si vous ne souhaitez pas promouvoir les dépendances d'un objet, décochez la case.

3. Cliquez sur *Suivant* pour examiner les objets que vous avez sélectionnés pour la promotion.

16.8.6 Résumé

Avant de procéder à la promotion, vous devez examiner les objets que vous avez sélectionnés pour la promotion.

Vous pouvez afficher les informations suivantes concernant chaque objet :

- Titre
- CUID
- Date

> **Attention**
>
> Assurez-vous que les objets que vous souhaitez copier sont inclus, car une fois la promotion commencée, vous ne pouvez pas l'annuler. L'assistant de gestion des promotions ne prend pas en charge la reprise.

Vous pouvez examiner les objets :

1. En fonction du niveau de détail à examiner, effectuez l'une des opérations suivantes :
   - Cliquez sur *Développer* pour afficher les détails de chaque objet.
   - Cliquez sur *Réduire* pour afficher le parent de chaque objet.

   > **Remarque**
   >
   > Dans le fichier CSV des résultats de la promotion, le niveau de détail varie selon que vous sélectionnez l'option *Développer* ou *Réduire*.

2. Afin de vous assurer que votre disque dur dispose de l'espace suffisant pour la promotion, consultez l'*Espace temporaire minimum requis*.
3. Cliquez sur *Démarrer* pour promouvoir les objets.

   Une fois que vous avez démarré la promotion, vous ne pouvez pas l'annuler.

16.8.7 (Facultatif) Fichier des propriétés

Vous pouvez configurer les paramètres suivants dans le fichier des propriétés de l'assistant de gestion des promotions :

- Paramètres SSL
- Paramètres

Le fichier des propriétés de l'assistant de gestion des promotions se trouve à l'emplacement suivant :`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

16.8.7.1 Configuration des paramètres SSL

Si vous utilisez SSL, vous devez configurer les paramètres SSL de l'assistant de gestion des promotions sous

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Ouvrez le fichier `PromotionManagementWizard.ini` dans un éditeur de texte.
2. Pour activer le mode SSL, retirez les commentaires des lignes qui commencent par "-D".
3. Saisissez la valeur de chaque paramètre.

Paramètre	Valeur
`-Dbusinessobjects.orb.oci.protocol`	Valeur : ssl **Remarque** Cette valeur active la communication SSL.
`-DcertDir`	Emplacement des clés et des certificats
`-DtrustedCert`	Nom du fichier de certificat approuvé **Remarque** Si vous spécifiez plusieurs fichiers, séparez les entrées par un point-virgule (par exemple, fichierA; fichierB).
`-DsslCert`	Certificat SDK
`-DsslKey`	Clé privée du certificat SDK
`-Dpassphrase`	Emplacement du fichier contenant la phrase de passe de la clé privée

Paramètre	Valeur
`-Dpsecert`	Fichier de certificat PSE

> ⚠ Attention
>
> N'ajoutez et ne modifiez aucune autre valeur ni aucun autre paramètre.

4. Enregistrez le fichier `PromotionManagementWizard.ini`.

Exemple : Paramètres SSL du fichier `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

16.8.7.2 Configuration des paramètres

En fonction de vos besoins, vous pouvez configurer plusieurs options dans le fichier des propriétés de l'assistant de gestion des promotions situé à l'emplacement suivant :

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Ouvrez le fichier `PromotionManagementWizard.ini` dans un éditeur de texte.
2. Pour activer les options, retirez les commentaires des lignes qui commencent par "-D".
3. Saisissez les valeurs de chaque paramètre.

Paramètre	Valeur
`-Dbusinessobjects.connectivity.directory`	Emplacement du référentiel du serveur de connexion.
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` ⓘ Remarque Ne modifiez pas cette valeur.
`-Xms8g`	Par défaut, la valeur de mémoire est définie sur 8 Go. La valeur Xms doit être inférieure ou égale à la valeur Xmx.

Paramètre	Valeur
`-Xmx10g`	Par défaut, la valeur de mémoire est définie sur 10 Go. Une mémoire de 10 Go est suffisante pour un référentiel contenant 65 000 objets.
`-Dbobj.biar.suggestSplit=512`	Valeur par défaut (recommandée) Il est conseillé d'utiliser le paramètre `-Dbobj.biar.suggestSplit`. Lorsque vous promouvez des objets d'un CMS Live vers un fichier LCMBIAR, ce paramètre permet de fractionner le fichier LCMBIAR en plusieurs fichiers LCMBIAR.
`-Dbobj.biar.forceSplit=768`	Valeur par défaut (recommandée) Si le paramètre `-Dbobj.biar.suggestSplit` ne peut pas être appliqué, le paramètre `-Dbobj.biar.forceSplit` s'applique comme solution de secours.
`-Dcom.businessobjects.lcm.commit`	• `KEEP_TS` : Valeur par défaut. Cette valeur permet de conserver les dates de modification de la source. • `LEGACY` : Les dates de modification correspondent à la date d'exécution dans le système de destination. Ce comportement est antérieur à la version 4.2 SP5.
`-Dcom.sap.businessobjects.pmw.exclude.list`	Ce paramètre permet d'exclure des objets lorsque vous promouvez des objets d'un système source vers un système de destination ou lorsque vous exportez un système source vers un fichier LCMBIAR. La valeur (CUID) peut être un objet (document, dossier, etc.). En cas de spécification d'un dossier, tous les enfants qu'il contient seront exclus.

4. Enregistrez le fichier `PromotionManagementWizard.ini`.

Exemple : Options de l'assistant de gestion des promotions dans le fichier `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

16.8.8 Assistant de gestion des promotions sous Linux

Vous pouvez exécuter l'assistant de gestion des promotions sur un système Linux.

Avant de lancer l'assistant de gestion des promotions sous Linux, assurez-vous que le Java Runtime Environment (JRE) est défini dans la variable de système `PATH`.

Pour démarrer l'assistant de gestion des promotions sous Linux, procédez comme suit :

1. Ouvrez un shell et accédez au répertoire d'installation tel que :

   ```
   /usr/sap_bobj/enterprise_xi40
   ```

2. Exécutez la commande suivante :

   ```
   ./PromotionManagementWizard
   ```

   L'assistant de gestion des promotions démarre.

   Pour de plus amples informations sur l'utilisation de la redirection SSH et X11, veuillez vous reporter à la documentation relative à votre système d'exploitation.

17 Gestion des versions

17.1 Pour gérer différentes versions d'un InfoObject

L'application de gestion des versions permet de gérer les versions de ressources BI qui se trouvent dans le référentiel de la plateforme de BI. Elle prend en charge les systèmes de gestion des versions SubVersion et GIT. Cette section décrit comment utiliser la fonctionnalité Gestion des versions de l'outil de gestion des promotions.

Pour créer et gérer différentes versions d'un InfoObject, procédez comme suit :

1. Lancez l'outil de gestion des promotions.
2. Cliquez avec le bouton droit de la souris sur un travail, sélectionnez *Actions VMS*, puis cliquez sur *Ajouter à la gestion de versions*. (Vous pouvez également cliquez sur l'onglet *Actions VMS* , puis sur *Ajouter à la gestion de versions*.)

   > **Remarque**
   >
   > En cliquant sur *Ajouter à la gestion des versions*, vous créez une version de base de l'objet dans le référentiel du VMS. Une version de base est requise pour la vérification consécutive.

3. Cliquez sur *Vérification* pour mettre à jour le document du référentiel du VMS.
   La boîte de dialogue *Commentaires de vérification* apparaît.
4. Saisissez vos commentaires et cliquez sur *OK*.
   La modification de numéro de version de l'InfoObject sélectionné est affichée dans les colonnes VMS et Système de gestion des contenus.
5. Pour obtenir la version la plus récente du document depuis le VMS, sélectionnez l'InfoObject requis et cliquez sur *Obtenir la version la plus récente*.
6. Pour créer une copie de la version la plus récente, cliquez sur *Créer une copie*.
   Une copie de la version sélectionnée est créée.
7. Sélectionnez *Historique* pour visualiser toutes les versions disponibles de la ressource sélectionnée.
   La fenêtre *Historique* s'affiche. Les options suivantes s'affichent :
   - *Obtenir la version* : En présence de plusieurs versions, et si vous avez besoin d'une version précise de la ressource de Business Intelligence, sélectionnez la ressource requise et cliquez sur *Obtenir la version*.
   - *Obtenir une copie de la version* : permet d'obtenir une copie de la version sélectionnée.
   - *Exporter une copie de la version* : permet d'obtenir une copie de la version sélectionnée et de l'enregistrer sur votre système local.

17.1.1 Droits d'accès à l'application de la gestion des versions

Cette section décrit les droits d'accès à l'application pour l'application de gestion des versions.

- Vous pouvez définir les droits d'accès d'application de gestion des versions dans la CMC.

- Vous pouvez définir les droits d'application granulaires pour différentes fonctionnalités dans l'application de gestion des versions.

Pour définir des droits spécifiques dans l'application de gestion des versions, procédez comme suit :

1. Connectez-vous à la CMC et sélectionnez *Applications*.
2. Cliquez deux fois sur *Gestion des versions*.
3. Cliquez sur *Sécurité de l'utilisateur* et sélectionnez un utilisateur. Vous pouvez visualiser les droits de sécurité de l'utilisateur sélectionné ou lui en affecter.
4. Les droits spécifiques à la gestion des versions désormais disponibles sont les suivants :
   - Autoriser la vérification
   - Autoriser la création de la copie
   - Autoriser la suppression de la révision
   - Autoriser l'obtention de la révision
   - Autoriser le verrouillage et le déverrouillage
   - Vue et version des objets BOMM
   - Vue et version des vues d'entreprise
   - Vue et version des calendriers
   - Vue et version des connexions
   - Vue et version des profils
   - Vue et version des QaaWS
   - Vue et version des objets du rapport
   - Vue et version des objets de sécurité
   - Vue et version des univers
   - Afficher les ressources supprimées
5. Si vous souhaitez affecter des droits à un utilisateur sélectionné, sélectionnez le droit en question et cliquez sur *Affecter la sécurité*.

17.1.2 Sauvegarde et restauration des fichiers Subversion

Cette section décrit les procédures conseillées pour effectuer des sauvegardes et récupérer des fichiers de sous-version. Un plan de sauvegarde et de récupération consiste en des précautions à prendre en cas de panne du système due à un événement de catastrophe naturelle ou de sinistre.

17.1.2.1 Pour sauvegarder des fichiers Subversion

Procédez aux étapes suivantes pour sauvegarder les fichiers de sous-version :

1. Sous Windows, allez à `<REPINSTALL>\SAP BusinessObjects Enterprise 4.0\CheckOut` ou, sous Unix, allez à `<REPINSTALL>/sap_bobj/enterprise_40/Subversion/CheckOut`.
2. Copiez le dossier `CheckOut` et stockez-le sur un dispositif de sauvegarde.
3. Copiez la totalité du référentiel `<LCM_Repository>` et stockez-le sur un dispositif de sauvegarde.

17.1.2.2 Pour restaurer les fichiers Subversion

Procédez aux étapes suivantes pour restaurer les fichiers de sous-version :

1. Restaurez le dossier d'extraction à partir de l'emplacement de sauvegarde précédent.

   > **Remarque**
   >
   > Dans la CMC, cliquez sur *Applications* > *Gestion des versions* > *Paramètres VMS* et veillez à ce que l'emplacement d'extraction entré dans le champ *Répertoire de l'espace de travail* soit correct.

2. Restaurez le référentiel LCM_Repository à partir de l'emplacement de sauvegarde précédent.

   > **Remarque**
   >
   > Dans la CMC, cliquez sur *Applications* > *Gestion des versions* > *Paramètres VMS* et veillez à ce que l'emplacement d'extraction entré dans le champ *Chemin d'installation* soit correct.

17.2 Gestion de différentes versions de ressources BI

L'application de gestion des versions permet de gérer les différentes versions de ressources BI qui se trouvent dans le référentiel de la plateforme de BI. Pour faciliter cette fonctionnalité, l'outil inclut le système de contrôle de version SubVersion.

Pour gérer différentes versions de travaux ou d'autres d'InfoObjects, procédez comme suit :

1. Connectez-vous à l'application de la CMC et sélectionnez *Gestion des versions*.
2. Dans le panneau de gauche de la fenêtre *Gestion des versions*, sélectionnez le dossier pour afficher les travaux ou d'autres InfoObjects dont vous souhaitez gérer les versions.
3. Sélectionnez les InfoObjects et cliquez sur *Ajouter à la gestion des versions*.

   > **Remarque**
   >
   > En cliquant sur *Ajouter à la gestion de versions* vous créez une version de base de l'objet dans le référentiel du Système de gestion des versions (VMS). Une version de base est requise pour la vérification consécutive.

4. En cas de modifications ultérieures du document et pour versionner le document progressivement modifié, cliquez sur *Vérification*. Cette opération met à jour le document présent dans le référentiel VSM.

   La boîte de dialogue *Commentaires de vérification* apparaît.
5. Saisissez vos commentaires et cliquez sur *OK*.
   La modification de numéro de version de l'InfoObject sélectionné est affichée dans les colonnes *Version VMS* et *Version CMS (Central Management Server)*.
6. Pour obtenir la version la plus récente du document depuis le VMS, sélectionnez l'InfoObject requis et cliquez sur *Obtenir la version la plus récente*.
   La dernière version du référentiel VMS est importée dans le CMS.
7. Pour créer une copie de la version la plus récente, cliquez sur *Créer une copie*.
   Une copie de la version sélectionnée est créée dans les référentiels VMS et CMS.

8. Sélectionnez *Historique* pour visualiser toutes les versions disponibles de l'InfoObject sélectionné.
   La fenêtre *Historique* s'affiche. Les options suivantes s'affichent :
   - *Obtenir la version* : En présence de plusieurs versions, et si vous avez besoin d'une version précise de la ressource de Business Intelligence, sélectionnez l'InfoObject requis et cliquez sur *Obtenir la version*.
   - *Obtenir une copie de la version* : permet d'obtenir une copie de la version sélectionnée.
   - *Exporter une copie de la version* : permet d'obtenir une copie de la version sélectionnée et de l'enregistrer sur votre système local.
   - *Comparer* : cette option permet de comparer les informations de métadonnées de deux versions d'un travail. Pour en savoir plus, voir « Comparaisons de différentes versions du même travail ».
9. Sélectionnez un InfoObject et cliquez sur *Verrouiller* pour le verrouiller, sur *Déverrouiller* pour le déverrouiller ou sur *Supprimer* pour supprimer tout le contenu de version du référentiel VMS. Le contenu du CMS n'est pas affecté.

   > **Remarque**
   >
   > Si vous verrouillez un InfoObject, vous ne pouvez réaliser aucune action sur celui-ci.

10. Lorsque la version du CMS est plus récente que celle du VMS, un indicateur apparaît en regard de l'InfoObject mis à jour. Lorsque vous placez le curseur sur l'indicateur, l'info-bulle `La version de CMS est plus récente` s'affiche.
11. Pour visualiser la liste de toutes les ressources vérifiées du CMS, cliquez sur *Afficher les ressources supprimées*.
    Cliquez sur une ressource supprimée pour visualiser l'historique de cette ressource. Vous pouvez sélectionner une ressource supprimée et cliquer sur *Obtenir la version* pour visualiser la version précise de la ressource.

    Cliquez sur *Supprimer* pour déposer l'objet du référentiel VMS de façon permanente.

    > **Remarque**
    >
    > Si vous utilisez *Obtenir la version*, la ressource est déplacée de la liste des fichiers manquant du VMS vers le CMS.

12. Sélectionnez un InfoObject et cliquez sur pour visualiser les propriétés de l'InfoObject.

    Vous pouvez également cliquer avec le bouton droit sur l'InfoObject et suivre les étapes 3 à 12.
13. Vous pouvez rechercher des actifs de BI dans l'application *Gestion des versions*. Vous pouvez utiliser les options telles que *Rechercher tous les champs*, *Rechercher le titre*, *Rechercher par mot-clé* et *Rechercher la description* pour effectuer une recherche spécifique pour obtenir des résultats plus rapides.

    > **Remarque**
    >
    > La fonctionnalité de recherche dans l'application *Gestion des versions* est contextuelle. Cela signifie que si vous sélectionnez un dossier tel que *Audit* et saisissez une chaîne pour rechercher un document, la plateforme de BI recherche le document uniquement dans le dossier *Audit*. De même, si vous sélectionnez *Tous les dossiers* et effectuez une recherche, la plateforme de BI recherche l'InfoObject dans chaque dossier.

17.3 Démarrage et arrêt manuels de Subversion sous Unix

Sous Unix, il est possible que Subversion ne démarre pas automatiquement après un redémarrage de l'ordinateur. A partir de la plateforme de BI 4.1 SP2, vous pouvez exécuter `<REPINSTALL>/svn_startup.sh` pour démarrer Subversion et `<REPINSTALL>/svn_shutdown.sh` pour l'arrêter.

> **Remarque**
>
> `svn_shutdown.sh` fonctionne uniquement si `svnserve` est démarré à l'aide de `svn_startup.sh`

> **Restriction**
>
> Si le processus Subversion est en cours d'exécution avant l'installation du correctif SP2, `svn_shutdown.sh` ne fonctionnera pas après l'installation du correctif. Pour redémarrer Subversion, vous devez manuellement arrêter le processus `svnserve`, puis exécuter `svn_startup.sh`.

17.4 Fichiers requis pour Subversion sous Solaris 10 et RedHat Linux 5

Les fichiers suivants sont requis pour exécuter Subversion.

> **Remarque**
>
> Si les fichiers binaires suivants sont manquants avant l'installation de la plateforme de BI 4.1 SP1, l'utilisateur doit exécuter `<REPINSTALL>/sap_bobj/lcm_installer.sh <MOTDEPASSE_SUBVERSION> <MOTDEPASSE_CMS>`, puis redémarrer le serveur de traitement adaptatif pour que la gestion des versions fonctionne normalement.

- Sous Solaris 10, vous devez installer les packages `CSWlibiconv2` et `CSWlibgcc-s1` contenant `libiconv.so.2` et `libgcc_s.so.1`.

  > **→ N'oubliez pas**
  >
  > Après l'installation des packages, veillez à ce que le chemin de ces bibliothèques soit inclus dans la variable d'environnement `LD_LIBRARY_PATH` de l'utilisateur.

- Sous RedHat Linux 5, vous devez déployer `libexpat.so.1`.

17.5 Utilisation de Apache SubVersion comme système de gestion des versions

Vous pouvez définir Apache SubVersion comme système de gestion des versions et configurer les options à partir de la Central Management Console.

1. Dans la CMC, cliquez sur *Applications*.
2. Cliquez deux fois sur *VMS*.
   L'écran des paramètres de gestion des versions s'affiche.
3. Sélectionnez *Paramètres VMS*.
4. Dans la liste *Systèmes de gestion des versions*, sélectionnez *SubVersion*.
   Le numéro de port du serveur, le mot de passe, le nom de référentiel, le nom de serveur, le nom d'utilisateur, le nom du répertoire d'espace de travail et le nom du chemin d'installation (fournis au cours du processus d'installation de l'outil de gestion des promotions) s'affichent dans les champs correspondants.
5. Modifiez les champs selon vos besoins.

   > **Remarque**
   >
   > Assurez-vous de saisir le chemin d'installation contenant le fichier `.exe`.

   Sous Windows : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   Sous Unix : `<REPINSTALL>/sap_bobj/enterprise_40/subversion/bin`
6. Sélectionnez *SVN*, *HTTP* ou *HTTPS*.

   > **Remarque**
   >
   > Pour en savoir plus sur la connexion à SubVersion à l'aide de HTTPS, voir la *Apache Subversion Documentation*.
7. (Facultatif) Cliquez sur *Tester VMS* pour valider les paramètres VMS.
8. Cliquez sur *Enregistrer*.

   > **Remarque**
   >
   > - Si vous souhaitez définir SubVersion comme VMS par défaut, sélectionnez *Utiliser comme VMS par défaut*.
   > - Si vous avez modifié les champs, redémarrez le serveur de traitement adaptatif.

17.6 Utilisation de Git comme système de gestion des versions

Vous pouvez définir Git comme système de gestion des versions et configurer les options à partir de la Central Management Console.

1. Dans la page d'accueil de la CMC, sélectionnez *Applications*.
2. Cliquez deux fois sur *Gestion des versions*.
   L'option *Paramètres VMS* dans l'écran *Paramètres de la gestion des versions* s'affiche.
3. Sélectionnez *Git* dans la liste *Systèmes de gestion des versions*.
   Les *options Git* et les paramètres requis s'affichent.
4. Sélectionnez un protocole et saisissez la valeur dans les champs vides. Pour en savoir plus sur chaque champ, consultez le tableau ci-dessous.

Termes de l'IU	Description
Protocole	Sélectionnez Local si Git est installé sur votre système local et sélectionnez HTTP(S) si Git est installé sur un serveur distant.
Nom d'utilisateur	Saisissez le nom d'utilisateur du serveur sur lequel Git est installé.
Mot de passe	Saisissez le mot de passe pour accéder au serveur sur lequel Git est installé.
URL serveur	Saisissez le lien vers le serveur sur lequel Git est installé.
Répertoire de l'espace de travail	Saisissez le chemin d'accès où vous souhaitez enregistrer votre espace de travail.
Nom du référentiel du serveur	Saisissez un nom pour le référentiel du serveur.
Chemin d'installation de GIT	Saisissez le répertoire d'installation de Git.

> **Remarque**
>
> Si vous souhaitez définir Git comme VMS par défaut, sélectionnez *Utiliser comme VMS par défaut*.

5. (Facultatif) Sélectionnez *Tester VMS* pour valider les paramètres VMS.
6. Sélectionnez *Enregistrer*.
7. Accédez à *Serveurs* > *Liste de serveurs* et sélectionnez *Redémarrer le serveur* dans le menu contextuel du *serveur de traitement adaptatif*.

Vous avez réussi à configurer Git comme système de gestion des versions.

17.7 Paramètres du système de gestion des versions par défaut

Lors de la réinitialisation du CMS, tous les paramètres d'application sont effacés. Voici les paramètres par défaut du système de gestion des versions :

Paramètre	Valeur
Nom du serveur	`localhost`
Port du serveur	`3690`
Nom d'utilisateur	`LCM`
Mot de passe	Saisi lors de l'installation.
Chemin d'installation	Sous Windows : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Subversion` Sous Unix : `<REPINSTALL>/sap_bobj/enterprise_xi40/subversion/bin`

Paramètre	Valeur
Nom du référentiel	Sous Windows : `svn_repository` Sous Unix : `LCM_repository`
Répertoire de l'espace de travail	Sous Windows : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` Sous Unix : `<REPINSTALL>/sap_bobj/enterprise_xi40/CheckOut`
Protocole	`SVN`

17.8 Comparaison de différentes versions du même travail

Vous pouvez visualiser les différences entre deux versions d'un même travail en procédant comme suit :

1. Connectez-vous à l'application CMC.
2. A partir de la page d'accueil de la CMC, sélectionnez *Gestion des versions*.
3. Dans l'écran Gestion des versions, sélectionnez le travail dont les versions doivent être comparées.
4. Cliquez sur *Historique*.
   La page Historique apparaît et affiche toutes les versions de l'InfoObject sélectionné.
5. Sélectionnez deux versions pour la comparaison.
6. Cliquez sur *Comparer*.
   Le processus de comparaison démarre. Les différences sont mises en surbrillance en orange et les objets manquants en rouge.
7. Cliquez sur *Enregistrer* pour enregistrer le rapport de différences.

17.9 Mise à niveau du contenu de SubVersion

Si vous possédez un ancien contenu SubVersion créé à l'aide d'une version antérieure de la plateforme de BI, vous pouvez effectuer une mise à niveau du contenu vers la dernière version en procédant comme suit :

1. Connectez-vous au VMS sur l'ordinateur de la plateforme SAP BusinessObjects Enterprise 4.2.
2. Vérifiez un objet quelconque. Par exemple, vérifiez deux fois les objets administrateur et invité.
3. Dans la CMC, cliquez sur *Utilisateurs* et vérifiez si `2` s'affiche dans les numéros de version du VMS et du CMS.
4. Déconnectez-vous du VMS.
5. Accédez à l'invite de commande, naviguez vers `C:\Program Files\Subversion\bin` et exécutez la commande d'exportation : `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`

6. Copiez le fichier `dumrepo` sur l'ordinateur de la plateforme de BI.
7. Accédez à l'invite de commande sur l'ordinateur de la plateforme de BI, naviguez vers `C:\Program Files (x86)\SAP` et exécutez les commandes suivantes :

   ```
   svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. Une fois les commandes exécutées, redémarrez le SIA.
9. Connectez-vous à la CMC et cliquez sur *Gestion des versions*.
10. Cliquez sur *Utilisateurs* et vérifiez si la version du VMS est `2`.
11. Sélectionnez l'objet *Administrateur* et cliquez sur *Obtenir la version la plus récente*.
12. Le numéro de version sur le VMS et le CMS est maintenant identique.

    Pour en savoir plus sur la mise à niveau d'Apache Subversion, consultez les Notes de version d'Apache Subversion 1.10 .

17.10 Configuration de Subversion pour les Job Server de traitement groupés

17.10.1 Option A : configurer l'ordinateur Subversion principal avant de réaliser une opération du système de gestion des versions

1. Vérifiez que le répertoire de la copie de travail n'a pas été créé à l'emplacement `<REPINSTALL>\CheckOut`.
2. Créez un répertoire pour vos fichiers de copie de travail Subversion et partagez-les pour qu'ils puissent être modifiés depuis les autres ordinateurs.
3. Dans la CMC, sur la page des paramètres du système de gestion des versions, remplacez la valeur **`localhost`** du champ *Nom du serveur* par l'adresse de votre ordinateur principal.
4. Remplacez la valeur du champ *Répertoire de l'espace de travail* par le partage de vos copies de travail, dans le format suivant : `\\<NOMHOTE>\<NOMPARTAGE>`
5. Arrêtez le Server Intelligence Agent (SIA) et remplacez le compte LocalSystem par l'administrateur du système d'exploitation.

   > **Remarque**
   >
   > LocalSystem ne dispose pas d'un accès réseau au répertoire partagé.

6. Démarrez le SIA.

   > **Remarque**
   >
   > Si le SIA a déjà été exécuté sous un compte avec un accès réseau au répertoire partagé, il vous suffit de redémarrer tous les Job Server de traitement qui hébergent le système de gestion des versions pour que les étapes 3 et 4 s'appliquent.

17.10.2 Option B : configurer Subversion après la création d'un répertoire de copie de travail par le système de gestion des versions

1. Vérifiez que Subversion est installé comme une partie de la plateforme de BI.
2. Partagez le répertoire de copie de travail situé à l'emplacement `<REPINSTALL>\CheckOut` et donnez accès en écriture aux autres ordinateurs.
3. Définissez le nom de l'espace de travail à l'aide de l'une des méthodes suivantes :
   - Réalisez une opération du système de gestion des versions (VMS) à partir de l'ordinateur principal. Ensuite, examinez le répertoire de la copie de travail Subversion pour déterminer le nom de l'espace de travail.
   - Calculez le nom de l'espace de travail en supprimant le symbole @ et en remplaçant tous les deux-points (:) par le caractère *B*. Par exemple, si le cluster s'appelle `ABCD-LCM:6400`, le VMS utilisera `ABCD-LCMB6400` comme nom de l'espace de travail.

> **Remarque**
>
> Subversion stocke son référentiel dans le répertoire de la copie de travail.

4. Modifiez l'URL par défaut, **`localhost`**, par une pouvant être utilisée par l'un des ordinateurs en exécutant la commande suivante :

```
svn switch --relocate svn://localhost:3690/
svn_repository svn://<SUBVERSION_MACHINE>:3690/svn_repository \
\<SUBVERSION_SHARE>\CheckOut\<WORKSPACE_NAME>-LCMB6400\WORKSPACE
```

5. Lorsque vous y êtes invité, saisissez le mot de passe de l'administrateur du système d'exploitation, l'utilisateur et le mot de passe.

   > **Remarque**
   >
   > Par défaut, l'utilisateur est LCM et le mot de passe est celui défini durant l'installation.

6. Dans la CMC, sur la page des paramètres du système de gestion des versions, remplacez la valeur **`localhost`** du champ *Nom du serveur* par l'adresse de votre ordinateur principal.
7. Remplacez la valeur **`localhost`** du champ *Répertoire de l'espace de travail* par votre partage de copie de travail : `\\<SUBVERSION_SHARE>\CheckOut`
8. Arrêtez le Server Intelligence Agent (SIA) et remplacez le compte LocalSystem par l'administrateur du système d'exploitation.
9. Démarrez le SIA.

   > **Remarque**
   >
   > Si le SIA a déjà été exécuté sous un compte avec un accès réseau au répertoire partagé, il vous suffit de redémarrer tous les Job Server de traitement qui hébergent le système de gestion des versions.

17.10.3 Configuration d'autres ordinateurs Subversion

Pour configurer d'autres ordinateurs Subversion, arrêtez le Server Intelligence Agent (SIA) et remplacez le compte LocalSystem par un compte disposant d'un accès réseau, pour que le Job Server de traitement puisse accéder au répertoire partagé (par exemple, le compte administrateur du système d'exploitation). Puis, redémarrez le SIA.

> **Remarque**
>
> Si le SIA a déjà été exécuté sous un compte avec un accès réseau au répertoire partagé, il vous suffit de redémarrer tous les Job Server de traitement qui hébergent le système de gestion des versions.

18 Gestion des applications

18.1 Désactivation du message pop-up RGPD

Depuis la version 4.2 SP5 de la plateforme SAP BusinessObjects Business Intelligence, un message pop-up d'avertissement relatif au RGPD (Règlement général sur la protection des données) est obligatoire pour tous les utilisateurs lorsqu'ils se connectent à des applications Web de la plateforme de BI telles que :

- Zone de lancement BI
- CMC
- Zone de lancement BI Fiori
- Open Document

Le message d'avertissement relatif au RGPD est obligatoire, mais vous avez la possibilité de désactiver l'affichage de ce message.

> ⚠ Attention
>
> Le message pop-up d'avertissement relatif au RGPD **ne doit pas**, et **ne peut pas** être désactivé de manière proactive. Pour assurer la conformité avec la législation RGPD de l'Union européenne, tous les utilisateurs doit activement accepter ce message avant de poursuivre.

Désactivation du message RGPD pour les utilisateurs se connectant à la zone de lancement BI

1. Sur une installation par défaut de Tomcat, accédez au fichier des propriétés :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Créez un fichier appelé `<Infoview.properties>` et saisissez `<properties file>` dans le chemin d'accès personnalisé :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Créez une nouvelle entrée de propriété pour `<disclaimer.enabled>` et définissez-la sur `<false>` :
   `disclaimer.enabled=false`
4. Enregistrez le fichier.
5. Redémarrez Tomcat.

Désactivation du message RGPD pour les utilisateurs se connectant à la CMC

1. Sur une installation par défaut de Tomcat, accédez au fichier des propriétés :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
2. Créez un fichier appelé `<CMCApp.properties>` et saisissez `<properties file>` dans le chemin d'accès personnalisé :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Créez une nouvelle entrée de propriété pour `<disclaimer.enabled>` et définissez-la sur `<false>` :
   `disclaimer.enabled=false`
4. Enregistrez le fichier.
5. Redémarrez Tomcat.

Désactivation du message RGPD pour les utilisateurs se connectant à la zone de lancement BI Fiori

1. Sur une installation par défaut de Tomcat, accédez au fichier des propriétés :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Créez un fichier appelé `<FioriBI.properties>` et saisissez `<properties file>` dans le chemin d'accès personnalisé :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Créez une nouvelle entrée de propriété pour `<disclaimer.enabled>` et définissez-la sur `<false>` :
   `disclaimer.enabled=false`
4. Enregistrez le fichier.
5. Redémarrez Tomcat.

Désactivation du message RGPD pour Open Document

1. Sur une installation par défaut de Tomcat, accédez au fichier des propriétés :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Créez un fichier appelé `<OpenDocument.properties>` et saisissez `<properties file>` dans le chemin d'accès personnalisé :
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`

Exemple : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`

3. Créez une nouvelle entrée de propriété pour `<disclaimer.enabled>` et définissez-la sur `<false>` : `disclaimer.enabled=false`
4. Enregistrez le fichier.
5. Redémarrez Tomcat.

18.2 Gestion des applications via la CMC

18.2.1 Présentation

La zone de gestion *Applications* de la CMC vous permet de modifier l'apparence et les fonctionnalités d'applications Web telles que la CMC et la zone de lancement BI, sans effectuer d'opérations de programmation. Elle permet également de modifier l'accès des utilisateurs, groupes et administrateurs aux applications en modifiant les droits associés à chaque application.

Cette section contient des informations contextuelles, des procédures et des instructions concernant la gestion de divers paramètres. Les applications suivantes contiennent des paramètres qui peuvent être modifiés via la CMC :

- *Application d'alerte*
- *Analysis, édition pour OLAP*
- *Analysis Office Runtime*
- *Configuration du serveur d'autorisation*
- *Applications Web BEx*
- *Cockpit de l'administrateur BI*
- *Zone de lancement BI*
- *Espaces de travail BI*
- *Central Management Console*
- *Collaboration*
- *Application de commentaires BI*
- *Configuration de Crystal Reports*
- *Authentification HANA*
- *Outil de conception d'information*
- *Application Information Steward*
- *Studio d'administration BI*
- *Outil de gestion de l'architecture mutualisée*
- *Open Document*
- *Application de recherche de plateformes*
- *Gestion de la promotion*
- *Application de la Corbeille*
- *Service Web RESTful*

- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- *Outil de gestion de la traduction*
- *Outil de conception d'univers*
- *Gestion des versions*
- *Gestion des versions*
- *Différence visuelle*
- *Web Intelligence*
- *Service Web*
- *Assistant du workflow*

18.2.2 Paramètres courants pour les applications

18.2.2.1 Définition de droits utilisateur sur les applications

Vous pouvez utiliser des droits pour contrôler l'accès des utilisateurs à certaines fonctionnalités des applications. La zone *Applications* de la CMC permet d'affecter des utilisateurs/groupes principaux à la liste de contrôle d'accès d'une application, de visualiser les droits dont dispose un utilisateur/groupe principal et de modifier les droits de l'utilisateur/groupe principal sur une application. Pour en savoir plus sur l'administration des droits, voir le *Guide d'administration de la plateforme SAP BI.*.

18.2.2.2 Définition du niveau de journalisation de suivi des applications Web dans la CMC

Pour suivre d'autres applications Web, vous devez configurer manuellement le fichier `BO_trace.ini` correspondant.

1. Dans la zone *Applications* de la CMC, faites un clic droit sur une application et sélectionnez *Paramètres du journal de suivi*.

   > **Remarque**
   >
   > Ces applications comportent des paramètres de journal de suivi : zone de lancement BI façon Fiori, CMC, Open Document, Gestion des promotions, Gestion des versions, Différence visuelle et Service Web.

   La boîte de dialogue *Paramètres du journal de suivi* s'affiche.
2. Sélectionnez un paramètre dans la liste *Niveau de journalisation*.
3. Cliquez sur *Enregistrer et fermer*.
4. Redémarrez le serveur d'applications Web.

Le nouveau niveau du journal de suivi prend effet après la prochaine connexion à l'application Web.

Informations associées

Niveaux du journal de suivi [page 709]

18.2.2.2.1 Niveaux du journal de suivi

Les niveaux du journal de suivi suivants sont disponibles pour les composants de la plateforme de BI :

Niveau	Description
Non spécifié	Le niveau du journal de suivi est spécifié par d'autres moyens, (généralement un fichier `.ini`).
Aucun	Aucun suivi n'est effectué.
Bas	Le filtre de journal de suivi autorise les messages d'erreur de journalisation tout en ignorant les messages d'avertissement et d'état. Les messages d'état importants sont journalisés pour des messages de démarrage ou d'arrêt d'un composant, ou pour les messages de requête de début et de fin. Ce niveau n'est pas recommandé pour les besoins du débogage.
Moyen	Le filtre du journal de suivi est défini pour inclure les messages d'erreur, d'avertissement et la plupart des messages d'état. Les messages d'état moins importants ou très détaillés sont refusés. Ce niveau n'est pas assez détaillé pour les besoins du débogage.
Elevé	Aucun message n'est filtré. Ce niveau est recommandé pour les besoins du débogage. ⚠ Attention Ce niveau du journal de suivi affecte considérablement les ressources du système, en augmentant l'utilisation de l'unité centrale et la consommation de l'espace de stockage.

18.2.3 Paramètres spécifiques aux applications

18.2.3.1 Gestion des paramètres de l'application CMC

18.2.3.1.1 Authentification et objets programme

Vous pouvez contrôler les types de programme que les utilisateurs peuvent exécuter et configurer les références de connexion nécessaires à l'exécution de ce type d'objet.

Soyez conscient des risques de sécurité potentiels associés à l'ajout d'objets programme au référentiel. Le niveau des autorisations de fichier associées au compte sous lequel un objet programme s'exécute détermine les modifications éventuelles que le programme peut apporter aux fichiers.

Activation ou désactivation d'un programme

En guise de premier niveau de sécurité, vous pouvez configurer les types de programme utilisables.

Authentification sous toutes les plateformes

Dans la zone de gestion *Dossiers* de la CMC, vous devez spécifier les références de connexion du compte sous lequel le programme doit s'exécuter. Cette fonctionnalité permet de configurer un compte utilisateur spécifique pour le programme et de lui attribuer des droits appropriés de sorte que l'objet programme s'exécute sous ce compte.

Une autre solution pour les utilisateurs qui ajoutent des objets programme aux Services de plateforme d'informations consiste à attribuer leurs propres références de connexion à un objet programme et à permettre au programme d'accéder au système. Par conséquent, le programme s'exécute sous ce compte utilisateur et les droits du programme sont limités à ceux de l'utilisateur. Si vous choisissez de ne pas spécifier de compte utilisateur pour un objet programme, celui-ci s'exécute sous le compte système par défaut, qui, en règle générale, dispose de droits localement mais pas sur le réseau.

> **Remarque**
>
> Par défaut, lorsque vous planifiez un programme, le travail échoue si vous ne spécifiez pas de références de connexion. Pour fournir des références de connexion par défaut, sélectionnez *CMC* dans la zone de gestion *Applications*. Dans le menu *Actions*, cliquez sur *Droits des objets du programme*. Cliquez sur *Effectuer la planification avec les références de connexion au système d'exploitation ci-dessous*, puis fournissez un nom d'utilisateur et un mot de passe par défaut.

Authentification pour les programmes Java

Les services de la plateforme d'informations permettent de configurer la sécurité pour tous les objets programme. Dans le cas des programmes Java, les Services de plateforme d'informations imposent l'utilisation

d'un fichier java.policy, dont le paramétrage par défaut est cohérent avec la valeur Java par défaut du code non protégé. Utilisez l'utilitaire java.policy disponible dans le kit de développement Java pour modifier le fichier java.policy en fonction de vos besoins.

Cet utilitaire Java possède deux entrées de base pour le code. La première entrée pointe vers le SDK Java de SAP BusinessObjects Enterprise et accorde aux objets programme les pleins droits sur tous les fichiers JAR de SAP BusinessObjects Enterprise. La seconde entrée de base pour le code concerne tous les fichiers locaux. Elle utilise les mêmes paramètres de sécurité pour le code non protégé que la valeur Java par défaut du code non protégé.

> **Remarque**
>
> Les paramètres de sécurité Java s'appliquent à tous les Program Job Servers fonctionnant sur le même ordinateur.

> **Remarque**
>
> Par défaut, le fichier java.policy est installé dans le répertoire du SDK Java, sous le répertoire racine d'installation des services de la plateforme d'informations. Par exemple, un emplacement habituel sous Windows est : `C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

18.2.3.1.1.1 Activation ou désactivation d'un objet de type programme

1. Dans la zone *Applications*, sélectionnez *Central Management Console*.
2. Cliquez sur *Actions* > *Droits des objets*.
   La boîte de dialogue *Droits des objets du programme* s'affiche.
3. Dans la zone *Autoriser les utilisateurs à*, sélectionnez les types d'objet programme que les utilisateurs doivent pouvoir exécuter.

   Vous pouvez sélectionner *Exécuter des scripts ou des fichiers binaires* ou *Exécuter les programmes Java*.

   Si vous sélectionnez *Exécuter les programmes Java*, vous pouvez activer ou désactiver la case *Utiliser l'emprunt d'identité*. Cette option fournit au programme Java un jeton qui lui permet de se connecter aux services de la plateforme d'informations.
4. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Si vous effectuez une mise à niveau vers la plateforme SAP BusinessObjects Business Intelligence 4.3 Support Package 3, les droits des objets du programme sont refusés pour tout le monde par défaut. Un utilisateur administrateur (ou tout utilisateur du groupe d'administrateurs) peut les activer.
>
> Sous *Exécuter les programmes Java*, il existe une case à cocher *Utiliser l'emprunt d'identité*. Dans la version 4.3 Support Package 3, la case *Utiliser l'emprunt d'identité* est supprimée.

18.2.3.1.2 Enregistrement des extensions de traitement à l'aide du système

> ⓘ Remarque
>
> Cette fonction ne s'applique pas aux documents Web Intelligence.

Avant d'appliquer vos extensions de traitement à des objets particuliers, vous devez donner l'accès de votre bibliothèque de codes à chaque ordinateur sur lequel seront traitées les requêtes de planification ou de visualisation appropriées. L'installation de la plateforme de BI crée un répertoire par défaut pour vos extensions de traitement sur chaque Job Server, serveur de traitement et RAS (Report Application Server). Il est recommandé de copier vos extensions de traitement dans le répertoire par défaut de chaque serveur. Sous Windows, le répertoire par défaut est `C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\ProcessExt`. Sous UNIX, il s'agit du répertoire `sap_bobj/ProcessExt`.

> → Conseil
>
> Il est possible de partager un fichier d'extension de traitement.

Selon la fonctionnalité que vous avez écrite dans l'extension, copiez la bibliothèque sur les machines suivantes :

- Si l'extension de traitement n'intercepte que les requêtes de planification, copiez votre bibliothèque sur chaque ordinateur servant d'Adaptive Job Server.
- Si votre extension de traitement n'intercepte que les requêtes de visualisation, copiez votre bibliothèque sur chaque ordinateur exécutant un serveur de traitement Crystal Reports ou un RAS.
- Si l'extension de traitement intercepte les requêtes d'affichage et de planification, copiez votre bibliothèque sur chaque ordinateur fonctionnant comme Crystal Reports Job Server, serveur de traitement Crystal Reports ou serveur RAS.

> ⓘ Remarque
>
> Si l'extension de traitement n'est nécessaire que pour les requêtes de planification/visualisation envoyées à un groupe de serveurs particulier, vous devez uniquement copier la bibliothèque sur chaque serveur de traitement du groupe.

18.2.3.1.2.1 Pour enregistrer une extension de traitement à l'aide du système

1. Accédez à la zone de gestion *Applications* de la CMC.
2. Sélectionnez *Central Management Console*.
3. Cliquez sur *Actions* > *Extensions de traitement*.
   La boîte de dialogue *Extensions de traitement : CMC* s'affiche.
4. Dans le champ *Nom*, saisissez un nom d'affichage pour votre extension de traitement.
5. Dans le champ *Emplacement*, saisissez le nom de fichier de votre extension de traitement ainsi que toute information supplémentaire relative au chemin.

- Si vous avez copié votre extension de traitement dans le répertoire par défaut sur chacune des machines appropriées, il vous suffit de saisir le nom de fichier (sans l'extension).
- Si vous avez copié votre extension de traitement dans un sous-dossier sous le répertoire par défaut, saisissez l'emplacement comme suit : **`<sousdossier>/<nomfichier>`**

6. Utilisez le champ *Description* pour ajouter des informations concernant votre extension de traitement.
7. Cliquez sur *Ajouter*.

> → Conseil
>
> Pour supprimer une extension de traitement, sélectionnez cette dernière dans la liste *Extensions existantes* et cliquez sur *Supprimer*. (Assurez-vous qu'aucun travail périodique n'est basé sur cette extension de traitement, car les éventuels travaux ultérieurs basés sur cette extension de traitement échoueront.)

8. Cliquez sur *Enregistrer et fermer*.
   L'extension de traitement est enregistrée avec la CMC.

Vous pouvez maintenant sélectionner cette extension de traitement pour appliquer sa logique à des objets particuliers.

18.2.3.1.2.2 Partage des extensions de traitement entre plusieurs serveurs

> ⓘ Remarque
>
> Cette fonctionnalité ne s'applique pas aux documents Web Intelligence ni aux rapports créés avec SAP Crystal Reports pour Enterprise.

Pour placer toutes les extensions de traitement dans un seul et même emplacement, remplacez le répertoire par défaut des extensions de traitement pour chaque Adaptive Job Server, pour chaque serveur de traitementCrystal Reports et pour chaque serveur RAS (Report Application Server). Tout d'abord, copiez vos extensions de traitement dans un répertoire partagé sur un lecteur de réseau qui est accessible à l'ensemble des serveurs. Mappez (ou montez) le lecteur réseau à partir de chaque machine serveur.

> ⓘ Remarque
>
> Les disques mappés sous Windows ne sont valides que jusqu'au redémarrage de l'ordinateur.

Si vous exécutez des serveurs à la fois sous Windows et sous UNIX, vous devez copier une version .dll et une version .so de chaque extension de traitement dans le répertoire partagé. De plus, le lecteur de réseau partagé doit être visible aux machines Windows et UNIX (via Samba ou tout autre système de partage de fichiers).

Enfin, modifiez la ligne de commande de chaque serveur pour changer le répertoire par défaut des extensions de traitement. Pour modifier la ligne de commande, accédez à l'onglet Serveurs de la CMC, sélectionnez un serveur, puis ouvrez sa page Propriétés. Ajoutez `-report_ProcessExtPath` **`<chemin absolu>`** à la ligne de commande. Remplacez `<chemin absolu>` par le chemin du nouveau dossier, en utilisant la convention d'écriture adaptée au système d'exploitation où s'exécute le serveur (par exemple, `M:\code\extensions`, `/home/shared/code/extensions`, etc.).

Pour modifier le répertoire par défaut des extensions de traitement, utilisez la CMC pour arrêter le serveur. Puis accédez aux Propriétés du serveur pour modifier la ligne de commande. Redémarrez le serveur, une fois l'opération terminée.

18.2.3.1.3 Gestion de l'accès aux onglets de la CMC

18.2.3.1.3.1 Administration déléguée et accès aux onglets de la CMC

En général, l'administrateur système de la plateforme de BI gère un grand nombre de documents, dossiers, utilisateurs, serveurs et autres objets. Cependant, les environnements d'entreprise étendus peuvent requérir plus de ressources qu'un seul administrateur. L'administrateur système qui veut se focaliser uniquement sur les tâches hautement prioritaires peut créer des administrateurs délégués et leur affecter des sous-ensembles de tâches de gestion (par exemple, l'administration du contenu d'un département ou d'un client). Contrairement aux administrateurs système, les administrateurs délégués réalisent un ensemble limité de tâches et ont moins de droits sur les objets du système.

La configuration par défaut de la Central Management Console permet aux utilisateurs d'accéder à tous les onglets de la CMC disponibles. L'administrateur système peut gérer l'accès aux onglets de la CMC afin de contrôler quels onglets sont visibles par les utilisateurs ou groupes d'utilisateurs principaux. Afin d'améliorer l'expérience utilisateur et le workflow des administrateurs délégués, l'administrateur système peut également masquer les onglets de la CMC qu'un administrateur délégué n'est pas censé utiliser.

> ⚠ Attention
>
> La gestion de l'accès aux onglets CMC affecte uniquement l'apparence visuelle de l'interface utilisateur de la CMC. Le masquage des onglets de la CMC n'est pas une mesure de sécurité car cela ne définit ni ne modifie aucun droit de sécurité sur les objets des onglets. Afin de garantir que les utilisateurs ne peuvent pas effectuer d'actions non autorisées sur des objets non autorisés (par exemple, gérer des serveurs par le biais du Central Configuration Manager ou un logiciel tiers sur base du SDK de la plateforme de BI), vous devez définir les droits de sécurité appropriés sur les objets (tels que les objets de serveur).

Informations associées

Pour gérer l'accès aux onglets de la CMC pour d'autres utilisateurs [page 716]
Pour gérer l'autorisation de configurer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs [page 718]

18.2.3.1.3.2 Utilisation de l'accès aux onglets de la CMC

18.2.3.1.3.2.1 Gestion de l'accès aux onglets de la CMC pour d'autres utilisateurs

Un administrateur système a toujours accès à tous les onglets de la CMC. Observez les instructions suivantes pour administrer les onglets de la CMC auxquels les utilisateurs ou groupes principaux peuvent accéder :

- Pour un processus de gestion plus simple et des besoins d'entretien et de dépannage réduits, il est recommandé aux administrateurs de gérer l'accès aux onglets de la CMC à un niveau de groupe d'utilisateurs (et non à un niveau d'utilisateur).
- En ce qui concerne les onglets de la CMC disposant de dossiers de niveau supérieur, l'administrateur peut accorder l'accès à un onglet et accorder le droit *Visualiser* sur le dossier de niveau supérieur de l'onglet. Les onglets CMC suivants prennent en charge les dossiers de niveau supérieur :
  - *Niveaux d'accès*
  - *Calendriers*
  - *Catégories*
  - *Connexions (aux univers)*
  - *Clés de cryptage*
  - *Evénements*
  - *Fédérations*
  - *Dossiers*
  - *Boîtes de réception*
  - *Connexion OLAP*
  - *Catégories personnelles*
  - *Dossiers personnels*
  - *Profils*
  - *Listes de réplication*
  - *Serveurs et groupes*
  - *Stockage temporaire*
  - *Univers*
  - *Utilisateurs et groupes*
  - *Requête de service Web*
- Pour une plus grande sécurité système, seuls les membres du groupe Administrateurs peuvent accéder aux onglets CMC suivants. Tout comme les administrateurs système, les membres du groupe Administrateurs peuvent accéder aux onglets CMC, peu importe les permissions d'accès à l'onglet CMC. Les permissions d'accès à l'onglet CMC permettent de contrôler l'accès aux onglets CMC pour les administrateurs délégués, c'est-à-dire les utilisateurs qui ne sont pas des membres du groupe Administrateurs.
  - *Audit*
  - *Authentifications*
  - *Clés de cryptage*
  - *Clés de licence*
  - *Surveillance*

- *Sessions*
- *Paramètres*
- *Gestion des attributs utilisateur*

> ⚠ Attention
>
> La gestion de l'accès aux onglets de la CMC affecte uniquement l'apparence visuelle de l'interface utilisateur de la CMC. Le masquage des onglets de la CMC n'est pas une mesure de sécurité car cela ne définit ni ne modifie aucun droit de sécurité sur les objets des onglets. Afin de garantir que les utilisateurs ne peuvent pas effectuer d'actions non autorisées sur des objets non autorisés (par exemple, gérer des serveurs par le biais du Central Configuration Manager ou un logiciel tiers sur base du SDK de la plateforme de BI), vous devez définir les droits de sécurité appropriés sur les objets (tels que les objets de serveur).

18.2.3.1.3.2.1.1 Pour gérer l'accès aux onglets de la CMC pour d'autres utilisateurs

1. Connectez-vous à la CMC
2. Dans l'onglet *Utilisateurs et groupes*, cliquez avec le bouton droit sur un utilisateur ou groupe principal et sélectionnez *Configuration de l'onglet CMC*.

   > ⓘ Remarque
   >
   > Si l'accès aux onglets de la CMC n'est pas restreint, le message suivant s'affichera : `Attention : L'accès à l'onglet de la CMC est actuellement illimité. Pour restreindre l'accès à la CMC, cliquez dans l'onglet "Application", sélectionnez "CMC" puis définissez l'accès à l'onglet de la CMC sur Restreint. Ces paramètres s'appliqueront une fois l'accès aux onglets de la CMC restreint :` Vous pouvez encore configurer l'accès aux onglets de la CMC. Toutefois, la configuration ne prendra pas effet tant que vous n'aurez pas restreint l'accès aux onglets de la CMC.

   Dans la boîte de dialogue *Configurer l'accès aux onglets de la CMC*, un tableau s'affiche :
   - ☐ ou ☐ indique à quels onglets de la CMC le principal peut accéder.
   - *Hérité* indique que l'accès aux onglets a été hérité de son ou ses groupes d'utilisateurs parent.
   - *Explicite* indique que l'accès aux onglets a été explicitement spécifié au niveau de l'utilisateur ou groupe principal.
3. Examinez les droits d'accès aux onglets de la CMC. Pour modifier les droits, vous pouvez utiliser les boutons de la barre d'outils :
   - Cliquez sur *Accorder* pour accorder explicitement l'accès à un onglet.
   - Cliquez sur *Refuser* pour refuser explicitement l'accès à un onglet.
   - Cliquez sur *Hériter* pour utiliser un droit d'accès hérité.

   > ⓘ Remarque
   >
   > Les modifications sont appliquées à l'utilisateur ou groupe principal sitôt que vous cliquez sur les boutons.

4. Lorsque vous avez terminé, cliquez sur *Fermer*.

L'accès à l'onglet désormais effectif s'affiche dans la colonne *Autorisation* du tableau.

Informations associées

Pour restreindre l'accès aux onglets de la CMC [page 720]

18.2.3.1.3.2.1.2 Héritage de l'accès aux onglets de la CMC

Les droits d'accès aux onglets de la CMC et l'autorisation de configurer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs s'appliquent et sont hérités de la même façon que les autres droits de sécurité de la plateforme de BI. Si aucun accès aux onglets n'est spécifié pour des utilisateurs ou groupes principaux, ceux-ci hériteront l'accès aux onglets des groupes d'utilisateurs auxquels ils appartiennent.

Si un utilisateur appartient à deux groupes d'utilisateurs, l'accès aux onglets est calculé de la même manière que tous les autres droits de la plateforme de BI. Par exemple, si l'accès est accordé à un onglet de la CMC dans un des groupes et refusé dans l'autre, l'utilisateur ou groupe principal ne sera pas en mesure d'accéder à l'onglet de la CMC.

> ⓘ Remarque
>
> - La modification du droit d'accès aux onglets de la CMC d'un groupe d'utilisateurs entraîne la modification du même accès aux onglets pour tous les utilisateurs ou groupes d'utilisateurs qui héritent les droits du groupe d'utilisateurs si leur accès aux onglets de la CMC est défini sur *Hérité*.
> - L'accès aux onglets défini sur le niveau d'utilisateur a toujours priorité sur l'accès aux onglets hérité de groupes d'utilisateurs.

18.2.3.1.3.2.1.3 Groupes d'utilisateurs d'administrateurs délégués

Vous pouvez créer un ensemble de groupes d'utilisateurs d'administrateurs délégués pour simplifier la gestion des onglets de la CMC. Afin d'éviter de configurer individuellement l'accès aux onglets de la CMC, vous pouvez faire d'un utilisateur ou groupe d'utilisateurs existant un membre d'un groupe d'utilisateurs d'administrateurs délégués. La configuration suivante est recommandée mais peut être modifiée pour des besoins professionnels précis.

> ⓘ Remarque
>
> L'appartenance à plusieurs groupes entraînera l'ajout de droits si les droits sont définis sur *Hérité*.

Groupes d'utilisateurs d'administrateurs délégués	Droits recommandés
Administrateurs système	Accordez l'accès à tous les onglets.
Administrateurs d'utilisateurs	Accordez l'accès à *Niveaux d'accès*, *Dossiers*, *Boîtes de réception*, *Dossiers personnels*, *Catégories personnelles*, *Résultats de requête*, *Sessions* et *Utilisateurs et groupes*. Définissez tous les autres onglets sur *Hérité*.
Administrateurs de contenu	Accordez l'accès à *Calendriers*, *Catégories*, *Evénements*, *Dossiers*, *Gestionnaire d'instances*, *Catégories personnelles*, *Dossiers personnels*, *Profils*, *Résultats de requête* et *Univers*. Définissez tous les autres onglets sur *Hérité*.
Administrateurs de serveurs	Accordez l'accès à *Serveurs* et *Applications.* Définissez tous les autres onglets sur *Hérité*.

18.2.3.1.3.2.1.4 Pour gérer l'autorisation de configurer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs

Dans un environnement d'entreprise étendu, il se peut qu'un administrateur système ait besoin de déléguer à un administrateur délégué la gestion de l'accès aux onglets de la CMC. Dans un système d'architecture mutualisée également, chaque client peut avoir un administrateur délégué responsable de la gestion de l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs.

1. Connectez-vous à la CMC.
2. Dans l'onglet *Utilisateurs et groupes*, cliquez avec le bouton droit sur un utilisateur ou groupe principal et sélectionnez *Configuration de l'onglet de la CMC*.
   Dans la boîte de dialogue *Configurer l'accès à l'onglet de la CMC*, *Permission de configurer l'accès à l'onglet de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs* s'affiche pour le principal.

   > **Remarque**
   >
   > Si cette autorisation est accordée, l'utilisateur ou groupe principal sera en mesure de gérer l'accès aux onglets de la CMC (uniquement en ce qui concerne les onglets auxquels il a accès) pour les utilisateurs sur lesquels il dispose du droit *Modifier en toute sécurité les droits*. En outre, l'utilisateur ou groupe principal sera en mesure de déléguer la gestion de l'accès aux onglets de la CMC pour d'autres utilisateurs en accordant la *Permission de configurer l'accès à l'onglet de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs* à des utilisateurs sur lesquels il dispose du droit *Modifier en toute sécurité les droits*.

   - ☐ ou ☐ indique si l'utilisateur ou groupe principal a l'autorisation de configurer les onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs.
   - *Hérité* indique que l'autorisation a été héritée de son ou ses groupes d'utilisateurs parent.
   - *Explicite* indique que l'autorisation a été explicitement spécifiée au niveau de l'utilisateur ou groupe principal.
3. Examinez les autorisations pour configurer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs. Pour modifier les autorisations, vous pouvez sélectionner un des paramètres suivants dans la liste :

- Cliquez sur *Accorder* pour accorder explicitement l'autorisation de gérer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs.
- Cliquez sur *Refuser* pour refuser explicitement l'autorisation de gérer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs.
- Cliquez sur *Hériter* pour hériter l'autorisation pour l'accès géré aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs.

> **Remarque**
>
> La sélection d'un paramètre dans la liste modifie l'autorisation du principal immédiatement.

4. Lorsque vous avez terminé, cliquez sur *Fermer*.

La nouvelle autorisation effective s'affiche.

Informations associées

Administration déléguée et accès aux onglets de la CMC [page 714]
Héritage de l'accès aux onglets de la CMC [page 717]

18.2.3.1.3.2.1.5 Pour ajouter un onglet Personnalisation pour un utilisateur ou un groupe d'utilisateurs

L'accès à l'onglet CMC doit être défini sur « Restreint » pour pouvoir ajouter un onglet *Personnalisation* pour un utilisateur ou un groupe d'utilisateurs.

1. Dans la CMC, accédez à la zone de gestion *Utilisateurs et groupes*.
2. Faites un clic droit sur un utilisateur ou un groupe d'utilisateurs et sélectionnez *Configuration de l'onglet CMC*.

   La boîte de dialogue *Configurer les onglets CMC* apparaît : elle répertorie tous les titres d'onglet CMC et les niveaux de permission pour les groupes d'utilisateurs.

   Si le message d'avertissement suivant apparaît en rouge en haut de la boîte de dialogue, vous devez définir l'accès à l'onglet CMC sur Restreint avant de pouvoir ajouter un onglet *Personnalisation* :

   ```
   Attention : L'accès à l'onglet de la CMC est actuellement illimité. Pour
   restreindre l'accès à la CMC, cliquez dans l'onglet "Application", sélectionnez
   "CMC" puis définissez l'accès à l'onglet de la CMC sur Restreint. Ces paramètres
   s'appliqueront une fois l'accès à l'onglet de la CMC restreint :
   ```
3. (Si nécessaire) Pour définir l'accès de l'onglet CMC sur restreint :
   a. Dans la zone de gestion *Applications* de la CMC, faites un clic droit sur *Central Management Console* et sélectionnez *Configuration de l'accès à l'onglet CMC*.
   b. Sous *Accès à l'onglet CMC*, sélectionnez l'option *Restreint* puis cliquez sur *Enregistrer et fermer*.
4. Dans la boîte de dialogue *Configurer les onglets CMC* pour le groupe d'utilisateurs, sélectionnez pour chaque onglet CMC *Accordé*, *Refusé* ou *Hérité* dans la liste.

A chaque fois que vous modifiez l'autorisation pour un onglet, la boîte de dialogue Configurer les onglets CMC met à jour l'autorisation du groupe d'utilisateurs pour configurer l'accès à l'onglet pour les autres utilisateurs ou groupes d'utilisateurs.

5. Cliquez sur *Fermer*.

18.2.3.1.3.2.2 Pour restreindre l'accès aux onglets de la CMC

Il est recommandé de configurer d'abord l'accès aux onglets de la CMC pour les utilisateurs ou serveurs principaux, puis de restreindre l'accès aux onglets de la CMC. Si vous restreignez l'accès aux onglets de la CMC avant de le configurer, vos utilisateurs ne seront en mesure d'accéder à aucun onglet de la CMC tant qu'un administrateur ne leur aura pas accordé l'accès.

Pour garantir la cohérence avec les versions précédentes de la plateforme de BI, l'accès aux onglets de la CMC n'est initialement pas restreint après l'installation de la plateforme de BI et tous les utilisateurs pouvant accéder à la CMC peuvent accéder à tous les onglets disponibles. Afin d'empêcher les utilisateurs d'accéder à des onglets auxquels ils n'ont pas de droit d'accès, l'administrateur système peut restreindre l'accès aux onglets de la CMC.

Vous pouvez supprimer la restriction de l'accès aux onglets de la CMC en cas d'urgence ou pour un dépannage de la configuration de l'accès aux onglets de la CMC (par exemple, si un administrateur délégué ne parvient pas à accéder à un onglet de la CMC essentiel).

1. Connectez-vous à la CMC.
2. Dans l'onglet *Applications*, cliquez à l'aide du bouton droit sur *Central Management Console* et sélectionnez *Configuration de l'accès à l'onglet de la CMC*.
   La boîte de dialogue *Accès à l'onglet de la CMC* s'affiche.
3. Configurez la règle d'accès aux onglets de la CMC.
   - Pour limiter l'accès de vos utilisateurs aux onglets pour lesquels ils ont des droits, sélectionnez *Restreint*.
   - Pour permettre aux utilisateurs d'accéder à tous les onglets, sélectionnez *Non restreint*.
4. Lorsque vous avez terminé, cliquez sur *Enregistrer et Fermer*.

La règle d'accès aux onglets de la CMC s'applique au système.

Informations associées

Pour dépanner l'accès aux onglets de la CMC [page 720]

18.2.3.1.3.2.3 Pour dépanner l'accès aux onglets de la CMC

Pour empêcher tout accès non autorisé ou dépanner l'accès limité d'un utilisateur aux onglets de la CMC, vous pouvez dépanner les droits d'accès aux onglets de la CMC d'un utilisateur.

1. Connectez-vous à la CMC en tant qu'administrateur.

> **Remarque**
>
> Assurez-vous que vous avez accès à l'onglet à dépanner et que vous disposez du droit *Modifier en toute sécurité les droits* sur l'utilisateur.

2. Dans l'onglet *Utilisateurs et groupes*, cliquez avec le bouton droit sur un utilisateur ou groupe principal et sélectionnez *Configuration de l'onglet CMC*.
   La fenêtre *Configurer l'accès aux onglets de la CMC*, s'affiche.
3. Examinez l'accès effectif aux onglets de la CMC. Vous pouvez accorder ou refuser de manière explicite l'accès aux onglets disponibles.

   Si l'accès aux onglets de la CMC est hérité mais que l'accès effectif aux onglets ne correspond pas aux besoins de l'utilisateurs :

   a. Compilez une liste de tous les groupes d'utilisateurs auxquels appartient le principal sélectionné.
   b. Répétez les étapes 1 à 3 pour chaque groupe dont l'utilisateur hérite l'accès à des onglets.
   c. Corrigez l'accès aux onglets de la CMC au niveau de l'utilisateur ou groupe principal ou sous le niveau du groupe en fonction de vos besoins.

> **Remarque**
>
> La réalisation de cette tâche au niveau du groupe affecte l'accès aux onglets de la CMC pour tous les utilisateurs appartenant à ce groupe et tous ceux appartenant à des groupes d'utilisateurs hérités de celui-ci tant que l'accès aux onglets de la CMC des utilisateurs est défini sur *Hérité*.

4. Lorsque vous avez terminé, cliquez sur *Fermer*.

Informations associées

Pour gérer l'accès aux onglets de la CMC pour d'autres utilisateurs [page 716]
Héritage de l'accès aux onglets de la CMC [page 717]

18.2.3.2 Gestion des paramètres de la zone de lancement BI

Cette section vous indique comment gérer les paramètres suivants dans la zone de lancement BI :

- Modification des paramètres d'affichage de la zone de lancement BI
- Configuration des détails de l'URL RESTful dans la Central Management Console pour se connecter à la zone de lancement BI
- Configuration de l'onglet Authentification et de la visibilité du CMS dans la zone de lancement BI
- Configuration du lien de courrier électronique pour l'option *Contacter l'administrateur* dans la zone de lancement BI

18.2.3.2.1 Configuration des détails de l'URL RESTful dans la CMC pour se connecter à la zone de lancement BI façon Fiori

Après avoir installé ou mis à niveau BI 4.2 SP4, vous devez configurer l'URL des services Web RESTful pour que l'utilisateur puisse se connecter à la zone de lancement BI façon Fiori.

Pour configurer les détails de l'URL des services Web RESTful dans la CMC, exécutez les étapes suivantes :

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Accédez à *Gérer* > *Applications* > *Services Web RESTful* > *Propriétés*.
3. Fournissez l'URL WACS (nom d'hôte ou nom de domaine complet où le serveur WACS est déployé).

18.2.3.2.2 Configuration des paramètres de proxy pour activer l'Assistant Web dans la zone de lancement BI façon Fiori

Après avoir installé ou mis à niveau BI 4.2 SP5, vous devez configurer les paramètres de proxy pour qu'un utilisateur puisse accéder à l'aide intégrée à l'application Assistant Web dans la zone de lancement BI façon Fiori.

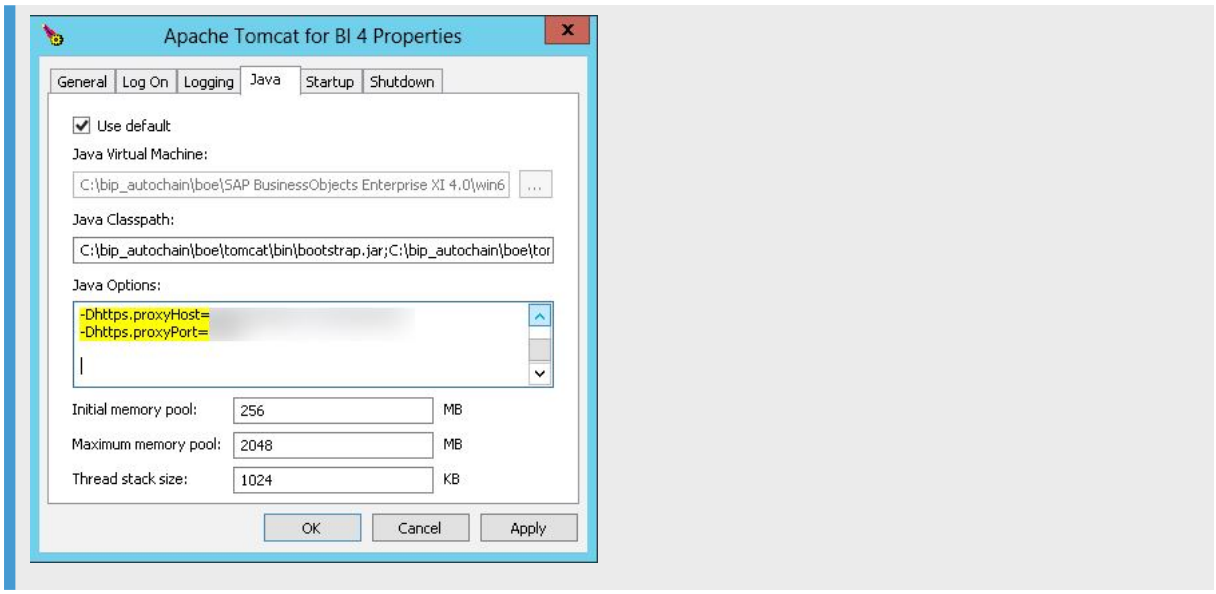
Pour cela, procédez comme suit :

Conditions prérequises :

Vous êtes connecté à Internet.

1. Accédez aux propriétés système du serveur Web.
2. Ajoutez les propriétés `https.proxyHost` et `https.proxyPort`.

> **Exemple**
>
> Système d'exploitation : Windows. Serveur Web : Tomcat 8.5
>
> 1. Accédez à *Windows* > *Tomcat*.
> La fenêtre *Propriétés Apache Tomcat pour BI 4* s'ouvre.
> 2. Cliquez sur l'onglet *Java*.
> 3. Dans le champ d'options Java, ajoutez les propriétés suivantes à la liste :
>  ```
>  -Dhttps.proxyHost=<proxy_host>
>  -Dhttps.proxyPort=<proxy_port>
>  ```
> 4. Redémarrez Tomcat.



18.2.3.2.3 Configuration du lien de courrier électronique pour l'option Contacter l'administrateur dans la zone de lancement BI façon Fiori

Configuration du lien de courrier électronique pour l'option *Contacter l'administrateur* dans la zone de lancement BI façon Fiori, exécutez les tâches suivantes :

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Si vous utilisez la version Tomcat installée avec la plateforme BI, vous pouvez également accéder à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Créez un fichier à l'aide de Notepad et enregistrez le fichier avec le nom suivant : FioriBI.properties.
3. Modifiez la propriété suivante dans le fichier : `admin.user.email=administrator@bilp.com`, pour inclure l'ID de courrier électronique de l'administrateur.

18.2.3.2.4 Configuration de l'onglet Authentification et visibilité du CMS dans la zone de lancement BI façon Fiori

Pour configurer l'onglet Authentification et visibilité du CMS dans la zone de lancement BI façon Fiori, exécutez les tâches suivantes :

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

Si vous utilisez la version Tomcat installée avec la plateforme BI, vous pouvez également accéder à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.

2. Créez un fichier à l'aide de Notepad et enregistrez le fichier avec le nom suivant : FioriBI.properties.
3. Pour inclure les options d'authentification à l'écran de connexion à la zone de lancement BI, ajoutez la ligne suivante : `authentication.visible=true`.

   Remplacez <authentication> par les types d'authentification par défaut : "secEnterprise, secLDAP, secWinAD, secSAPR3".
4. Pour modifier le type d'authentification par défaut, ajoutez ceci : `authentication.default=<authentication>`.
5. Pour demander aux utilisateurs de fournir le nom du CMS dans l'écran de connexion à la zone de lancement BI, ajoutez l'élément suivant : `cms.visible=true`.
6. Enregistrez le fichier et fermez-le.
7. Redémarrez le serveur d'applications Web.

18.2.3.2.5 Modification des paramètres d'affichage de la zone de lancement BI

1. Accédez à la zone *Applications* de la CMC, puis cliquez deux fois sur la *zone de lancement BI*.
   La boîte de dialogue *Propriétés de la zone de lancement BI* s'affiche.
2. Pour activer les filtres de planification, cochez la case *Afficher l'onglet "Filtres" sur la page Planifier*.

   Ce paramètre détermine si les utilisateurs peuvent saisir des formules de sélection d'enregistrements ou de groupes lors de la planification d'un rapport Crystal.
3. Cliquez sur *Enregistrer et fermer*.

18.2.3.3 Gestion des paramètres de Web Intelligence

Vous pouvez contrôler les fonctionnalités accessibles par les utilisateurs pour les documents Web Intelligence en définissant les propriétés de l'application Web Intelligence.

18.2.3.3.1 Pour modifier les paramètres d'affichage de Web Intelligence

1. Accédez à la zone *Applications* de la CMC, puis sélectionnez *Web Intelligence*.
2. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
3. Définissez une des options d'affichage suivantes :

Option	Description
Options d'affichage des données modifiées > *Dimensions et détails*	Utilisez les options figurant dans cette zone pour définir la façon dont les données ajoutées apparaissent dans les rapports ; modifiez le style de police, la couleur du texte et la couleur d'arrière-plan. Une fenêtre d'aperçu présente automatiquement vos modifications. Cliquez sur *OK* lorsque vous avez terminé.
Options d'affichage des données modifiées > *Valeurs fluctuantes (indicateurs numériques)*	Utilisez les options figurant dans cette zone pour modifier et mettre en forme l'en-tête de page ; modifiez le style de police, la couleur du texte et la couleur d'arrière-plan. Une fenêtre d'aperçu présente automatiquement vos modifications. Cliquez sur *OK* lorsque vous avez terminé.
Propriétés de l'image incorporée	Saisissez la taille maximale de l'image incorporée.
Prise en charge des cartes géographiques	Activez ou désactivez la prise en charge des cartes géographiques dans Web Intelligence.
Propriétés du mode d'affichage rapide	Dans les champs appropriés, saisissez le nombre maximal d'enregistrements verticaux, le nombre minimal d'enregistrements horizontaux, la largeur minimale de page, la hauteur minimale de page, la valeur de remplissage droite et la valeur de remplissage bas.
Paramètres d'enregistrement automatique	Définissez l'intervalle d'enregistrement automatique des documents. Cet intervalle est réinitialisé chaque fois qu'un document est enregistré manuellement ou automatiquement. Par ailleurs, le document enregistré automatiquement est supprimé lorsque vous fermez un document manuellement.
Actualisation automatique	Active l'actualisation automatique des documents Web Intelligence quand leur propriété *Actualisation automatique* est sélectionnée. Pour en savoir plus, voir le *Guide de l'utilisateur de SAP BusinessObjects Web Intelligence*.
Fusion automatique	Active la fusion automatique des dimensions quand la propriété de document Web Intelligence *Fusionner automatiquement les dimensions* est sélectionnée. Pour en savoir plus, voir le *Guide de l'utilisateur de SAP BusinessObjects Web Intelligence*.
Actualisation automatique du document à l'ouverture du paramètre du droit de sécurité	Décochez cette option pour permettre à Web Intelligence d'actualiser les documents automatiquement à l'ouverture, sans activer l'option *Actualisation à l'ouverture* dans les propriétés du document Web Intelligence. La sélection de cette option sélectionne le droit de sécurité *Documents : désactiver l'actualisation automatique à l'ouverture*.
Vue intelligente	Cette option détermine quelle version du document est affichée lorsque les utilisateurs ouvrent des documents dans Web Intelligence. • Visualiser la dernière instance La dernière instance de l'objet est ouverte. Par exemple, si un document est planifié pour une actualisation toutes les heures et qu'il a été enregistré pour la dernière fois et fermé cinq heures auparavant, la dernière instance est ouverte. • Afficher l'objet Le document est ouvert dans l'état où il était lors de son dernier enregistrement, sans tenir compte des actualisations planifiées susceptibles de s'être produites.

Option	Description
JavaScript	L'option que vous sélectionnez ici (Lire le contenu comme HTML ou Lire le contenu comme lien hypertexte) définit le rendu des cellules dans les documents Web Intelligence : • *Désactiver JavaScript et activer les liens hypertextes et uniquement les éléments HTML utilisés par Web Intelligence* Cette option par défaut active les liens hypertextes et l'ensemble limité d'éléments HTML requis pour les fonctions Web Intelligence. Elle supprime les éléments JavaScript et autres éléments HTML des documents. • *Activer uniquement les éléments HTML définis dans la page Éléments HTML autorisés* Cette option active uniquement les éléments et attributs HTML que vous spécifiez dans la page *Éléments HTML autorisés*. • *Activer JavaScript, les éléments HTML et les liens hypertextes* Cette option active JavaScript, ainsi que l'ensemble des éléments HTML et des liens hypertextes. Lorsque vous modifiez l'option, pour afficher les modifications dans Web Intelligence, déconnectez-vous de l'application et reconnectez-vous à l'application. ⚠ Attention • Web Intelligence active le code Javascript/HTML intégré dans les cellules du document grâce à ses fonctionnalités de formule. Ce code peut être activé ou désactivé dans la Central Management Console. Cependant, en autorisant JavaScript, les HTML et les liens hypertexte, vous reconnaissez votre risque qu'exposition à Cross-Site Scripting. Cross-Site Scripting permet aux attaquants de modifier des sites Web ou d'exécuter du code sur d'autres systèmes. Cette vulnérabilité affecte des produits tels que les navigateurs Internet lorsqu'ils exécutent des scripts. La majorité des attaques Cross-Site Scripting résultent d'une programmation non sécurisée sur le système cible. • Le code peut être ajusté en autorisant les balises et attributs HTML dans *Studio d'administration BI* > *Applications* > *Éléments HTML*. Toutefois, SAP n'est pas responsable de la compatibilité de ce code et de ses éventuels effets secondaires. Il est possible, par exemple, que votre code nécessite quelques adaptations en raison de mises à jour du navigateur, de la prise en charge de la version Javascript ou du mode d'intégration dynamique du code dans la page Web. Le code nécessitera peut-être des ajustements pour pouvoir s'exécuter dans ce nouveau contexte.
Alignement du contenu pour les nouveaux documents	Utilisez ces options pour définir si le contenu du nouveau document doit être aligné de droite à gauche, de gauche à droite ou s'il doit dépendre des paramètres régionaux de visualisation préférés de l'utilisateur et/ou des paramètres régionaux du produit.
Features Toggle	Utilisez ce champ de texte pour saisir des boutons à bascule afin d'activer les fonctionnalités d'aperçu. Ces boutons à bascule peuvent également être utilisés dans les notes SAP pour modifier le comportement par défaut. Cette liste de boutons à bascule doit être saisie sous forme de liste au format JSON.

4. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Pour remplacer vos sélections par les variables d'affichage par défaut, cliquez sur *Réinitialiser*.

18.2.3.3.2 Services d'éléments personnalisés

Les éléments personnalisés sont des visualisations dont le rendu est délégué par Web Intelligence à des services tiers.

Dans les documents Web Intelligence, les éléments personnalisés sont intégrés et affichés comme n'importe quel autre élément de rapport (diagramme, table, etc.). Pour que les utilisateurs puissent visualiser les éléments personnalisés dans les documents Web Intelligence, les services d'éléments personnalisés doivent être préalablement configurés dans la CMC.

Comme vos données seront transférées du serveur BOE vers le serveur tiers d'éléments personnalisés, il est recommandé de déployer le serveur d'éléments personnalisés sur votre intranet. Si cela n'est pas possible, il est recommandé d'utiliser exclusivement HTTPS pour accéder au serveur d'éléments personnalisés.

> **Attention**
>
> Le service d'éléments personnalisés que vous déployez ajoute du code à Web Intelligence, et peut générer des problèmes de sécurité potentiels tels qu'une vulnérabilité de type XSS (cross-site scripting). Une vulnérabilité XSS permet à des attaquants d'exécuter du code et des scripts sur les ordinateurs d'autres utilisateurs. Un avertissement de sécurité vous invite à donner votre consentement explicite avant de déployer votre service d'éléments personnalisés. Votre consentement est obligatoire pour pouvoir déployer le service d'éléments personnalisés.

Migration

Lors de la migration d'un document Web Intelligence d'un CMS vers un autre, le service d'éléments personnalisés utilisé pour créer le contenu du document doit être recréé dans le nouveau CMS avec un nom identique. Si le service d'éléments personnalisés n'est pas recréé (avec un nom identique) dans le nouveau CMS, les éléments personnalisés du document migré ne sont plus modifiables.

18.2.3.3.2.1 Ajout d'un service d'éléments personnalisés

Pour les utilisateurs finaux qui peuvent utiliser des éléments personnalisés, vous devez d'abord indiquer, en tant qu'administrateur, le service tiers qui gère le rendu. Par défaut, aucun service d'éléments personnalisés n'est activé. Ce paramètre est facultatif et doit être activé dans la CMC.

Vous avez ajouté l'URL de service personnalisé à la liste des URL approuvées. Si ce n'est pas le cas, reportez-vous à la section Ajout d'URL approuvées à la liste des URL autorisées [page 733].

1. Ouvrez la CMC (Central Management Console).

2. Cliquez sur *Applications*.
3. Cliquez avec le bouton droit de la souris sur *Web Intelligence*.
4. Cliquez sur *Propriétés*.
5. Cliquez sur *Éléments personnalisés*.
6. Cliquez sur *Ajouter un service*.
7. Donnez un nom au service.

> ⚠ Attention
>
> Le nom du service sera affiché tel quel dans les clients Web Intelligence et doit être unique. Vous ne pouvez pas réutiliser le nom d'un service existant. Si vous modifiez le nom d'un service, vous ne pourrez plus modifier les éléments personnalisés créés avec ce service dans les documents Web Intelligence.

8. Saisissez une URL avec le numéro de port.
9. Cliquez sur *Tester*.
10. Sélectionnez un *type de support*.

    Web Intelligence est compatible avec les types de support HTML et bitmap. Le type de support privilégié est HTML (text/html), car il permet une interactivité dans les clients Web Intelligence et offre une meilleur expérience utilisateur. Les types de support bitmap peuvent être au format .PNG (image/png), .JPG (image/JPG) ou .GIF (image/gif).
11. Entrez la *résolution d'image*.

> ⓘ Remarque
>
> Il s'agit de la résolution des images bitmap générées par le service. Le format bitmap est requis pour la publication des rapports Web Intelligence sous forme de fichiers PDF ou Excel dans lesquels les éléments personnalisés sont représentés par des images. Sans le format bitmap, ces publications affichent un bloc vide à la place de l'élément personnalisé attendu.

12. Cliquez sur *OK*.

> ⓘ Remarque
>
> Vous pouvez utiliser plusieurs services d'éléments personnalisés à la fois. Un service unique peut fournir plusieurs éléments personnalisés.

Informations associées

URL d'autorisation [page 732]

18.2.3.3.3 Actualisation parallèle des fournisseurs de données

La fonction d'actualisation parallèle des fournisseurs de données améliore les performances d'actualisation des données dans les documents Web Intelligence contenant plusieurs fournisseurs de données.

Pour actualiser les requêtes en parallèle, Web Intelligence répartit tous les fournisseurs de données sur plusieurs threads. Cette fonction est activée par défaut et Web Intelligence peut actualiser jusqu'à 64 requêtes en parallèle. Les fournisseurs de données reposant sur des connexions relationnelles, OLAP et BICS sont pris en charge ainsi que les fournisseurs de données personnels (fichiers texte, FHSQL).

> **⚠ Restriction**
>
> Les fournisseurs de données ne sont pas pris en charge.

Vous pouvez diminuer cette valeur dans la CMC (Central Management Console) si le matériel exécutant Web Intelligence ne prend pas en charge une telle charge de travail. Vérifiez que votre matériel a suffisamment de cœurs pour garantir des performances optimales

Deux paramètres globaux sont disponibles dans la CMC :

- *Requêtes parallèles maximum par document* : définit le nombre maximal de fournisseurs de données que Web Intelligence peut actualiser en parallèle par document. La valeur par défaut est 64.
- *Activer les requêtes parallèles pour la planification* : activer ou désactiver le traitement en parallèle des requêtes lors de la planification des documents. Cette option est activée par défaut.

Nous conseillons également d'optimiser chaque connexion de base de données avec un paramètre permettant de spécifier le nombre de requêtes pouvant être exécutées en parallèle. Ce paramètre, nommé Maximum de requêtes parallèles, est disponible :

- Dans la CMC (Central Management Console) ou dans l'outil de conception d'information pour les connexions OLAP et BICS.
- Dans l'outil de conception d'information ou dans l'outil de conception d'univers pour les connexions relationnelles.

Pour chaque connexion, le nombre de fournisseurs de données pouvant être actualisé en parallèle est fixé à 4 par défaut. L'administrateur de base de données peut modifier cette valeur en fonction du matériel qui exécute la base de données. Cependant, pour les fichiers texte, la valeur par défaut est fixée à 1.

Exemple

Dans cet exemple, toutes les valeurs par défaut ont été conservées et chaque connexion prend en charge un maximum de 4 tâches d'actualisation en parallèle.

Connexion	Nombre de fournisseurs de données à actualiser
2 connexions OLAP	6 (5 à la première connexion, 1 à la deuxième connexion)
1 connexion relationnelle	2

Connexion	Nombre de fournisseurs de données à actualiser
2 connexions BICS	2
Fichiers Excel d'un fournisseur de données personnel	2

Les deux fichiers Excel sont actualisés en séquence car il ne sont pas pris en charge par la fonction d'actualisation en parallèle des fournisseurs de données.

Quatre des fournisseurs de données de la première connexion OLAP sont actualisés en parallèle sur les threads 1, 2, 3 et 4. Le cinquième est mis en file d'attente et sera traité dès qu'un fournisseurs de données (d'une connexion quelconque) aura été actualisé, alors que celui provenant de la deuxième connexion OLAP est actualisé sur le thread 5 parce qu'il dépend d'une connexion différente.

Les quatre fournisseurs de données des deux connexions relationnelle et BICS sont actualisés en parallèle sur les threads 5, 6, 7 et 8.

> **Remarque**
>
> S'il existe plus de fournisseurs de données du même type que la valeur définie, ils sont placés en file d'attente jusqu'à ce que d'autres fournisseurs de données aient terminé.

Informations associées

Pour modifier le nombre de fournisseurs de données actualisés en parallèle par document [page 730]
Pour modifier le nombre de fournisseurs de données actualisés en parallèle pour une connexion OLAP spécifique [page 731]

18.2.3.3.3.1 Pour modifier le nombre de fournisseurs de données actualisés en parallèle par document

1. Dans l'écran d'accueil de la CMC, cliquez sur *Serveurs*.
2. Cliquez sur *Services Web Intelligence*.
3. Cliquez avec le bouton droit sur *Serveur de traitement Web Intelligence*, puis sur *Propriétés*.
4. Saisissez un nombre dans le champ de saisie *Maximum de requêtes parallèles*.

   Les valeurs possibles vont de 0 à 64.

   > **Remarque**
   >
   > Si vous saisissez 0, la fonction d'actualisation en parallèle des fournisseurs de données est désactivée.

18.2.3.3.3.2 Pour désactiver le traitement des requêtes parallèles pour la planification

1. Dans l'écran d'accueil de la CMC, cliquez sur *Serveurs*.
2. Cliquez sur *Services Web Intelligence*.
3. Cliquez avec le bouton droit sur *Serveur de traitement Web Intelligence*, puis sur *Propriétés*.
4. Décochez *Activer les requêtes parallèles pour la planification*.

18.2.3.3.3.3 Pour modifier le nombre de fournisseurs de données actualisés en parallèle pour une connexion OLAP spécifique

1. Dans l'écran d'accueil, cliquez sur *Connexions OLAP*.
2. Accédez à la connexion à configurer et cliquez dessus avec le bouton droit.
3. Sélectionnez *Organiser* > *Modifier*.
4. Saisissez un nombre dans le champ de saisie *Maximum de requêtes parallèles*.

   Les valeurs possibles vont de 1 à 64.

   > **Remarque**
   >
   > Si vous entrez 1, les fournisseurs de données sont actualisés séquentiellement.

18.2.3.3.4 Protection des exportations CSV

Web Intelligence fournit une mesure de sécurité destinée à empêcher l'injection de commandes lorsque les utilisateurs ouvrent un fichier CSV généré à partir d'un document dans Microsoft Excel. Vous pouvez désactiver cette protection pour les exportations CSV.

Par défaut, Web Intelligence ajoute un espace avant les caractères suivants lors d'une exportation vers un fichier ou une archive CSV :

- = (Egal)
- + (Plus)
- - (Moins)
- @ (Arobase)

L'espace supplémentaire empêche l'exécution sous forme de commandes des valeurs contenant ces caractères, qui pourrait entraîner un problème de sécurité sur votre système.

Informations associées

Pour désactiver la protection des exportations CSV [page 732]

18.2.3.3.4.1 Pour désactiver la protection des exportations CSV

Dans Web Intelligence, pour désactiver la mesure de sécurité par défaut qui empêche l'injection de commandes lorsque les utilisateurs ouvrent un fichier CSV exporté dans Microsoft Excel, modifiez la clé de registre correspondante.

Définissez la valeur de la clé de registre `EscapeCharactersForCSVExport` sur false pour désactiver la mesure de sécurité. Par défaut, la clé de registre n'est pas présente et sa valeur est true, c'est pourquoi vous devrez peut-être la créer pour définir sa valeur sur false.

La modification prend effet après la fermeture et la réouverture de l'application par les utilisateurs Web Intelligence.

Modifiez la clé de registre comme suit :

- Sous Windows, sur les serveurs et ordinateurs client, définissez la clé de registre sur false : `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.
- Sous UNIX, sur les serveurs, dans le fichier `$installdir/setup/boconfig.cfg`, définissez la clé de déclaration de registre suivante sur false `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.

18.2.3.3.5 URL d'autorisation

Web Intelligence utilise des URL pour :

- Les liens hypertexte dans le document
- Les liens hypertexte dans les conseils d'invite
- Image d'arrière-plan
- Source de données OData
- Éléments personnalisés ou extensions externes

Ces URL peuvent potentiellement créer des menaces pour la sécurité.

En tant qu'administrateur, vous devez créer dans la Central Management Console une liste d'URL approuvées que les utilisateurs peuvent utiliser. Cette liste contrôle l'utilisation de ces URL dans Web Intelligence.

18.2.3.3.5.1 Ajout d'URL approuvées à la liste des URL autorisées

Lorsque vous souhaitez utiliser une URL dans Web Intelligence en tant que lien hypertexte dans le document ou un conseil d'invite, une image d'arrière-plan, une source de données OData ou un nouveau service personnalisé ou une extension externe, vous devez d'abord l'autoriser.

1. Dans l'écran d'accueil de la CMC, cliquez sur *Applications*.
2. Cliquez sur *Web Intelligence*.
3. Dans le menu contextuel, sélectionnez *Propriétés*.
4. Sélectionnez la section *Catégorie d'URL autorisées*.
5. Cliquez sur le bouton *Ajouter une nouvelle URL* pour ajouter une URL approuvée.
6. Dans le champ *URL autorisée*, spécifiez une URL unique, avec son protocole, son nom d' hôte et son port.

   > → Conseil
   >
   > Vous pouvez saisir le caractère * pour autoriser n'importe quelle URL pour un lien hypertexte ou une image d'arrière-plan ou une source de données OData. Vous devez ensuite cocher la case *J'accepte le risque* pour confirmer que vous comprenez le risque potentiel pour activer toutes les URL.

7. Si l'URL saisie est une URL vers une extension ou un service d'élément personnalisé accessible via un proxy, vous pouvez cocher la case *Si cette URL est utilisée pour un élément personnalisé ou une extension qui nécessite un proxy, saisissez son serveur et son port* pour définir ce serveur proxy et ce port.
8. Cliquez sur *OK*.

18.2.3.4 Gestion des paramètres de Crystal Reports

18.2.3.4.1 Activation de la fonctionnalité Vue intelligente dans Crystal Reports

1. Accédez à la zone *Applications* de la CMC, puis sélectionnez *Crystal Reports*.
2. Sélectionnez *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
3. Sélectionnez *Zone de lancement BI*.
4. Définissez l'option d'affichage suivante :

Option	Description
Vue intelligente	Cette option détermine quelle version du document est affichée lorsque les utilisateurs ouvrent un document Crystal Report. • Afficher la dernière instance La dernière instance réussie de l'objet est ouverte. Par exemple, si un document est planifié pour une actualisation toutes les heures et qu'il a été enregistré pour la dernière fois, puis fermé cinq heures auparavant, la dernière instance réussie est ouverte. • Afficher objet Le document est ouvert dans l'état où il était lors de son dernier enregistrement, sans tenir compte des actualisations planifiées susceptibles de s'être produites.

18.2.3.4.2 Activation de la bibliothèque de fonctions utilisateur Java pour Crystal Reports pour Enterprise

Vous pouvez afficher et planifier le rapport contenant la bibliothèque de fonctions utilisateur Java (UFL). Suivez la procédure ci-dessous :

1. Connectez-vous à la CMC.
2. Sélectionnez *Applications* dans la liste déroulante.
3. Sélectionnez *Configuration de Crystal Reports*.
4. Dans le panneau de gauche, sous *Propriétés*, sélectionnez *Crystal Reports pour Enterprise*.
5. Sélectionnez l'option *Ajouter nouveau* et renseignez les propriétés suivantes :

Propriété	Valeur	Informations supplémentaires
classpath	Chemin de classe pour l'UFL Java	• Utilisez un point-virgule comme séparateur pour plusieurs fichiers jar. • Vous devez utiliser une double barre oblique (\\) ou une barre oblique (/) à la place. • Exemple : C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\java\\lib\\MyFirstUFL.jar

Propriété	Valeur	Informations supplémentaires
ExternalFunctionLibraryClassNames.classname	Nom complet de l'UFL	Exemple : samples.ufl.InternationalizationLibrary

6. Redémarrez les services liés à Crystal Reports.
   Vous pouvez maintenant exécuter la visualisation et la planification des workflows.

18.2.3.4.3 Activation de la bibliothèque de fonctions utilisateur .NET/COM pour Crystal Reports pour Enterprise

Vous pouvez afficher et planifier le rapport contenant la bibliothèque de fonctions utilisateur .NET/COM (UFL). Suivez la procédure ci-dessous :

1. Copiez la version 64 bits de .Net UFL sur `<Répertoire d'installation>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

   > **Remarque**
   >
   > Crystal Reports pour Enterprise Designer est en 64 bits et requiert donc une UFL .NET 64 bits, alors que Crystal Reports pour Enterprise services on Business Intelligence Platform est en 64 bits et requiert donc une UFL .NET 64 bits.

2. Enregistrez et ajoutez au GAC le fichier dll 64 bits à l'aide de "regasm <dll>" et "gacutil /if <dll>".
3. Connectez-vous à la CMC.
4. Sélectionnez *Applications* dans la liste déroulante.
5. Sélectionnez *Configuration de Crystal Reports*.
6. Dans le panneau de gauche, sous *Propriétés*, sélectionnez *Crystal Reports pour Enterprise*.
7. Sélectionnez l'option *Ajouter nouveau* et renseignez la propriété suivante :

Catégorie	Propriété	Valeur
Laisser cette colonne vide	NonJavaExternalFunctionLibraries.managerDirectory	Chemin d'accès au fichier UFL 64 bits • Vous devez utiliser une double barre oblique (\\) ou une barre oblique (/) à la place. • Exemple : C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\win64_x64).

8. Redémarrez les services liés à Crystal Reports.
   Vous pouvez maintenant exécuter la visualisation et la planification des workflows.

18.2.3.5 Gestion des paramètres d'alerte

Dans la zone *Applications* de la CMC de la plateforme de BI, il est possible de spécifier des paramètres au niveau système pour les alertes.

Pour l'application *Alertes*, vous pouvez contrôler et définir la manière dont les utilisateurs système accèdent aux alertes en :

- activant le dossier *Mes alertes* pour les abonnés aux alertes
- activant et mettant en forme les messages d'alerte envoyés par voie électronique
- paramétrant une limite pour le nombre d'alertes dans le système
- paramétrant une période d'expiration pour les messages d'alerte

Informations associées

Définition de droits utilisateur sur les applications [page 708]

18.2.3.5.1 Modification des propriétés de la destination des alertes

1. Dans la zone *Applications* de la CMC, cliquez deux fois sur *Application d'alerte*.
2. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Alertes* s'affiche.
3. (Obligatoire) Effectuez l'une des actions suivantes :
   - Sélectionnez *Activer Mes alertes* pour permettre aux abonnés aux alertes de recevoir des notifications sous *Mes alertes* dans la zone de lancement BI.
   - Sélectionnez *Activer l'adresse électronique* pour permettre aux abonnés aux alertes de recevoir des notifications par courrier électronique.
     Options globales de courrier électronique pour que les alertes s'affichent.
4. Si vous avez sélectionné *Activer l'adresse électronique*, effectuez l'une des actions suivantes :
   - Dans la case *De*, saisissez l'adresse électronique à partir de laquelle seront envoyées les notifications d'alerte.
     Les abonnés recevront des courriers électroniques d'alerte envoyés depuis cette adresse. Utilisez une adresse électronique valide reconnue par votre système.
   - Dans la case *A*, saisissez l'adresse électronique de l'abonné à l'alerte.
     Par défaut, toutes les alertes système seront envoyées à cette adresse électronique.

     > → Conseil
     >
     > Ne spécifiez pas d'adresse électronique ni de destinataire. Utilisez l'espace réservé *%SI_EMAIL_ADDRESS%*.
   - Dans la case *Cc*, entrez toutes les adresses électroniques des destinataires qui doivent recevoir des copies des alertes.

- Dans la case *Objet*, saisissez un en-tête d'objet par défaut à utiliser dans les courriers électroniques contenant les alertes.
- Dans la case *Message*, saisissez un message par défaut à inclure dans les courriers électroniques contenant les alertes.
- Sélectionnez *Ajouter une pièce jointe* pour permettre d'inclure des pièces jointes par défaut aux courriers électroniques contenant des alertes système.
  Par exemple, sélectionnez cette option pour inclure des rapports Crystal associés aux alertes déclenchées.
- Si vous avez sélectionné *Ajouter une pièce jointe*, dans *Nom du fichier*, sélectionnez *Généré automatiquement* ou *Nom spécifique* pour indiquer comment nommer les pièces jointes aux courriers électroniques.

5. Cliquez sur *Enregistrer et fermer*.

Informations associées

Définition de droits utilisateur sur les applications [page 708]
Gestion des paramètres d'alerte [page 736]

18.2.3.5.2 Modification des propriétés par défaut des alertes

1. Accédez à la zone *Applications* de la CMC, puis sélectionnez *Application d'alerte*.
2. Cliquez sur *Gérer* > *Propriétés* > *Paramètres par défaut* >.
3. Définissez les valeurs appropriées pour les propriétés ci-dessous.

Option	Description
Période d'expiration	Spécifie la période pendant laquelle les messages d'alerte seront conservés dans le système avant d'être supprimés.
Nombre maximal de massages d'alerte	Spécifie le nombre maximal de messages d'alerte pris en charge par le système. Une fois le seuil atteint, le système supprime 20 % des messages d'alerte, en commençant par les plus anciens.

4. Cliquez sur *Enregistrer et fermer*.

Informations associées

Gestion des paramètres d'alerte [page 736]

18.2.3.6 Gestion des paramètres de l'application des commentaires BI

L'application Commentaires BI a été introduite dans la CMC. Elle permet aux utilisateurs de documents de collaborer en commentant toutes les données et statistiques disponibles dans un document donné.

Avec les Commentaires BI, les utilisateurs peuvent publier des commentaires sur les données et statistiques au sein des rapports.

→ Recommandation

Par défaut, l'application Commentaires BI crée et gère ses tables dans la base de données d'audit.

ⓘ Remarque

Pour utiliser les Commentaires BI avec la base de données d'audit sur une plateforme autre que Windows, reportez-vous au Guide d'accès aux données pour configurer les pilotes ODBC.

Toutefois, SAP vous conseille de configurer une nouvelle base de données pour stocker les commentaires de l'application Commentaires BI. Les bases de données prises en charge pour l'application Commentaires BI sont les mêmes que celles prises en charge pour l'Audit. Les bases de données et les fichiers jar JDCB certifiés correspondants qui sont pris en charge pour les commentaires BI comprennent :

- IBM DB2 Workgroup Edition : db2jcc4.jar
- Microsoft SQL Server : sqljdbc4.jar
- MySQL : com.mysql.jdbc_5.1.5.jar
- Oracle : ojdbc6.jar
- SAP HANA : ngdbc.jar
- Sybase Adaptive Server Enterprise : jconn4.jar
- Sybase SQL Anywhere : jconn4.jar

ⓘ Remarque

Que vous souhaitiez configurer des commentaires BI avec la base de données d'audit ou avec une autre base de données prise en charge, pour que les commentaires BI fonctionnent avec la base de données MySQL, vous devez mettre le fichier jar JDBC MySQL à l'emplacement suivant : `<REP_INSTALL\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

Si vous configurez Commentaires BI avec IBM DB2, vous aurez besoin d'un espace de table système temporaire de 8 Ko, 16 Ko ou 32 Ko. Par défaut, la taille de page est 4K.

ⓘ Remarque

Si la base de données d'audit n'est pas configurée/activée par défaut, alors les Commentaires BI ne fonctionnent pas. Il vous faut configurer manuellement une nouvelle base de données pour cette application.

Si vous configurez des commentaires BI avec la base de données d'audit et que vous supprimez la base de données d'audit, tous les commentaires stockés dans la base de données d'audit sont également supprimés.

La base de données d'audit utilise des types de pilotes de base de données natifs ou ODBC. Pour configurer une nouvelle base de données Commentaires, vous devez utiliser un pilote JDBC.

> **Remarque**
>
> La taille d'un commentaire est limitée à 2000 octets de caractères UTF-8 ou 666 octets de caractères UTF-16.

> **Remarque**
>
> Vous ne pouvez pas migrer les commentaires à l'aide de l'outil de fédération.

> **Remarque**
>
> Les commentaires BI ne sont pas pris en charge pour les connexions MaxDB.

> **Remarque**
>
> Pour supprimer les entrées de commentaire effectuées par l'utilisateur, utilisez la requête suivante :
>
> `DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'`

18.2.3.6.1 Configuration d'une nouvelle base de données pour les Commentaires BI

Vous avez créé une connexion JDBC.

> **Remarque**
>
> Lorsque vous configurez une nouvelle base de données pour les Commentaires BI, le service des commentaires hébergé sur le serveur de traitement adaptatif écrit les informations Commentaires dans la base de données. Les étapes suivantes sont requises sur chaque ordinateur du cluster exécutant le service des commentaires.

Pour créer une nouvelle connexion JDBC, suivez les étapes suivantes :

1. Placez le fichier jar du pilote JDBC pour la base de données que vous souhaitez configurer à l'emplacement suivant : `<REP_INSTALL\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > **Remarque**
   >
   > Si vous effectuez une mise à niveau vers la plateforme SAP BusinessObjects Business Intelligence 4.2 Support Package 2 et que vous avez déjà configuré une nouvelle base de données pour les Commentaires BI des versions précédentes, vous devez déplacer le fichier du pilote de base de données du dossier "jdbc" présent dans `<REP_INSTALL\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` vers `<REP_INSTALL\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

2. Redémarrez le SIA.

Pour configurer une nouvelle base de données pour les Commentaires BI, suivez cette procédure :

1. Connectez-vous à la CMC.
2. Sur la page d'accueil de la CMC; sélectionnez *Applications* dans le menu déroulant.
3. Dans la liste *Nom de l'application*, sélectionnez *Application de commentaires BI*.

   La fenêtre contextuelle *Commentaires BI* apparaît. La case d'option *Utiliser la base de données d'audit* est cochée par défaut.
4. Cochez la case d'option *Utiliser une autre base de données prise en charge*.
5. Saisissez le *Type*, le *Nom de la base de données*, l'*Hôte*, le *Port*, le *Nom d'utilisateur* et le *Mot de passe* dans le volet *Configurer la base de données de commentaires*.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez l'APS.

   Toute modification de la configuration de la base de données des Commentaires BI n'entre en vigueur qu'après redémarrage du serveur de traitement adaptatif (APS).

   Vous pouvez valider votre connexion en sélectionnant *Tester la connexion*.

   > **Remarque**
   >
   > Si vous effectuez une mise à niveau vers la plateforme SAP BusinessObjects Business Intelligence 4.3 Support Package 3 et que vous avez déjà configuré une base de données pour les commentaires BI pour JDBC dans les versions précédentes, le champ de mot de passe sera désormais vide lors de la sélection de *Tester la connexion*, *Enregistrer et fermer* ou *Enregistrer*.

   Vous pouvez choisir de supprimer ou nettoyer les anciens commentaires en cochant la case *Supprimer tous les commentaires datant de plus de* et en indiquant le nombre de jours.

   > **Remarque**
   >
   > Vous devez redémarrer tous les serveurs APS qui hébergent le service Commentaires BI pour que les modifications prennent effet.

Vous avez correctement configuré une nouvelle base de données afin de stocker les commentaires de l'application Commentaires BI.

18.2.3.7 Gestion des paramètres de l'application Studio d'administration BI

> **Remarque**
>
> Pour accéder à Studio d'administration BI, vous devez faire partie du groupe Administrateur.

Si vous refusez des droits d'accès spécifiques comme : *Autoriser l'accès au cockpit d'administration de BI*, *Autoriser l'accès à la surveillance* et *Autoriser l'accès à la différence visuelle*, vous ne pourrez peut-être pas accéder à l'application spécifique dans Studio d'administration BI.

Specific Rights for BI Admin Studio	Implicit Value
Allow access to BI Admin Cockpit	Granted
Allow access to Monitoring	Granted
Allow access to Visual Difference	Granted
Visual Difference - Create comparison	Granted
Visual Difference - Delete comparison	Granted
Visual Difference - Rerun comparison	Granted
Visual Difference - View comparison	Granted

Si les droits *Différence visuelle* sont refusés, vous pouvez également restreindre l'utilisation de l'application VD.

18.2.3.8 Gestion de l'intégration d'application de collaboration

Ce guide est destiné aux administrateurs de la plateforme de BI qui procèderont à l'intégration de l'application de collaboration SAP Jam dans la plateforme de BI.

Utilisez la zone *Applications* de la Central Management Console (CMC) dans la plateforme de BI pour activer et configurer la collaboration.

La configuration supplémentaire suivante est requise dans l'agent Enterprise de l'application de collaboration :

- Etablir la connexion HTTPS avec le fournisseur de services
- Remplir les conditions préalables à l'authentification

Une fois l'application SAP Jam configurée, les flux de l'application de collaboration sont disponibles dans la zone de lancement BI.

SAP Jam ne prend pas en charge Microsoft Internet Explorer 11.

18.2.3.8.1 Prérequis pour la collaboration

Certaines conditions de prérequis doivent être remplies avant d'intégrer la plateforme de BI à une application de collaboration.

- La plateforme de BI doit être installée avec au moins un CMS.
- L'application de collaboration (SAP Jam) doit être configurée dans la Central Management Console (CMC).
- Une organisation Enteprise de l'application de collaboration (SAP Jam) doit être définie.
- Les utilisateurs de SAP Jam doivent appartenir à l'organisation Enterprise.
- Un agent Enterprise SAP Jam est requis pour mettre en service les utilisateurs qui utilisent un service de répertoire LDAP/AD sur site.

18.2.3.8.2 Configuration de la plateforme de BI

18.2.3.8.2.1 Options de configuration de la collaboration

Les options de collaboration s'affichent dans la boîte de dialogue *Propriétés :Collaboration* dans la CMC (Central Management Console) sur la plateforme de BI.

Pour accéder à la boîte de dialogue *Propriétés :Collaboration*, dans l'onglet *Applications* de la CMC, cliquez sur *Collaboration* et sélectionnez *Gérer* > *Propriétés*.

Option	Description
Activer la collaboration	Cochez cette case, puis sélectionnez *SAP Jam*.
URL de connexion	Saisissez l'URL de l'application de collaboration.
ID du fournisseur d'identité unique	Saisissez une valeur unique pour le déploiement de la plateforme de BI. Cette valeur doit être associée au certificat utilisé pour configurer l'intégration sur la console d'administration de l'application de collaboration. L'application qui réalise l'assertion d'une identité pour la connexion unique doit être configurée comme une application OAuth administrative.
Certificat en base 64 du fournisseur d'identité	Lorsque vous cliquez sur *Générer*, un certificat est créé dans cette zone. Utilisez le certificat dans la console d'administration de l'application de collaboration pour générer une clé consommateur OAuth. Le certificat définit la relation de confiance entre l'application de collaboration et la plateforme de BI. Le fournisseur d'identité externe lui-même est identifié par un certificat X509, utilisé pour signer toutes les assertions d'identité. Le certificat doit être codé en base 64.
Clé du consommateur OAuth	Saisissez la clé consommateur OAuth générée par la console d'administration de l'application de collaboration.
Connexion à l'aide du proxy	Cochez cette case pour activer la connexion par proxy et saisissez les informations d'hôte proxy dans les zones *Hôte proxy HTTP* et *Port*. Pour autoriser les connexions entrantes à partir des serveurs d'applications de collaboration dans votre réseau d'entreprise, vous devez disposer d'un proxy inverse dans la DMZ. Pour ajouter un certificat sécurisé d'un fournisseur de certificats SSL au proxy inverse, vous devez posséder un nom de domaine ou de sous-domaine pour le proxy inverse.

Option	Description	
	Hôte proxy HTTP	Dans la configuration du proxy inverse, saisissez une adresse externe accessible à l'application de collaboration. Par exemple, utilisez `https://<ProxyInverse>/`, où `<ProxyInverse>` est le nom de domaine ou de sous-domaine du proxy inverse. L'application de collaboration utilise cette adresse pour envoyer des informations à la plateforme de BI. Le proxy inverse utilise cette adresse pour rediriger les informations reçues à partir de l'application de collaboration vers l'ordinateur qui contient l'agent Enterprise de l'application de collaboration.
	Port	L'agent Enterprise de l'application de collaboration est configuré pour une écoute sur le port 8443.

18.2.3.8.2.2 Activation et configuration de la collaboration dans la CMC

Cette tâche requiert une connexion valide à la console d'administration (SAP Jam) de l'application de collaboration. Vous devrez transmettre et extraire des détails de sécurité à partir de la console.

Pour des raisons de sécurité, les comptes par défaut suivants ne peuvent ni envoyer ni planifier de contenu vers SAP Jam :

- Guest
- SMAdmin
- Administrateur
- WaaWSServletPrincipal

1. Dans la CMC (Central Management Console) de la plateforme de BI, accédez à la zone *Applications*, puis cliquez deux fois sur *Collaboration*.
2. Dans la boîte de dialogue *Propriétés : Collaboration*, cochez la case *Activer la collaboration*, puis sélectionnez *SAP Jam*.
3. Dans la zone *URL de connexion*, saisissez l'URL de l'application de collaboration.
4. Dans la zone *ID du fournisseur d'identité unique*, saisissez une valeur de fournisseur d'identité unique pour le déploiement de la plateforme de BI.

   Notez la valeur du fournisseur d'identité, vous l'utiliserez pour configurer l'application de collaboration.
5. Cliquez sur *Générer* (ou *Regénérer*, si un certificat a été créé avant).
   Un certificat s'affiche dans la zone *Certificat en Base64 du fournisseur d'identité*. Vous utiliserez la valeur du certificat pour configurer l'application de collaboration.
6. Dans la zone *Clé du consommateur OAuth*, saisissez une clé consommateur OAuth valide.
7. Si vous êtes connecté via un proxy au serveur exécutant SAP Jam, effectuez les actions suivantes :
   a. Cochez la case *Connexion à l'aide du proxy*.
   b. Dans la zone *Hôte proxy HTTP*, saisissez le nom de l'hôte proxy du serveur.
   c. Dans la zone *Port*, saisissez le numéro de port du serveur.

8. Cliquez sur *Enregistrer et fermer*.

18.2.3.8.3 Configuration de SAP Jam

18.2.3.8.3.1 Enregistrement d'un nouvel IDP sécurisé SAML pour SAP Jam

Vous devez enregistrer chaque utilisateur avec une adresse électronique unique correspondant à l'adresse électronique Enterprise de l'utilisateur dans la zone de lancement BI. Les adresses électroniques seront mappées entre la plateforme de BI et SAP.

Avant de pouvoir enregistrer un nouvel IDP sécurisé SAML :

- Votre entreprise doit être ajoutée et configurée dans SAP.
- Vous devez posséder un compte utilisateur SAP valide associé à votre entreprise dans SAP.
- Vous devez disposer des droits d'administration d'entreprise pour votre entreprise dans SAP ainsi que des droits administrateur complets sur la plateforme de BI et dans la zone de lancement BI.
- La zone de lancement BI doit être enregistrée en tant que client OAuth qui agit comme un représentant de la zone de lancement dans SAP Jam.

SAP Jam ne prend pas en charge Microsoft Internet Explorer 11.

1. Dans le coin supérieur droit de la Central Management Console (CMC) de la plateforme de BI, sélectionnez *Administrateur*, puis *Admin*.
   Des informations concernant votre entreprise, notamment votre licence SAP, s'affichent. Prenez note de ces informations.
2. Dans le menu *Admin*, sélectionnez *SAML Trusted ID's* (ID sécurisés SAML)et cliquez sur *Register your identity provider* (Enregistrer votre fournisseur d'identité).

   Vous devez enregistrer l'IDP créé dans la zone de lancement BI.
3. Dans la zone *IDP ID* (ID d'IDP), saisissez la valeur du fournisseur d'identité unique créé lors de la configuration de SAP sur la plateforme de BI.

   Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.

   Par exemple, saisissez **`<NomEntreprise>_<IdSystème>_<client>`**
4. Dans la zone *Single Sign-On URL* (URL de connexion unique), saisissez l'URL permettant d'accéder directement à SAP.

   SAP utilise cette URL de connexion unique avec le fournisseur d'identité unique.
5. Dans la zone *Single Log-Out URL* (URL de déconnexion unique), saisissez l'URL à afficher après toute déconnexion de SAP.

   SAP utilise cette URL de déconnexion unique avec le fournisseur d'identité unique.
6. Dans la zone *Default Name ID Format* (Format par défaut de l'ID de nom), saisissez le format de l'ID de nom à utiliser dans les requêtes d'authentification.
7. Dans la zone *Default Name ID Policy SP Name Qualifier* (Qualificateur du nom de SP par défaut de la politique d'ID de nom), saisissez l'identificateur du nom de SP à utiliser dans les requêtes d'authentification.
8. Dans la liste *Allowed Assertion Scope* (Périmètre d'assertion autorisé), sélectionnez *Users in my company* (Utilisateurs de mon entreprise).

Cette option spécifie l'ensemble des utilisateurs pour lesquels SAP acceptera les assertions à partir de l'IDP.

9. Dans la zone *X509 Certificate (Base64)* (Certificat X509 (Base64)), saisissez la valeur du certificat en Base64 générée lors de la configuration de SAP sur la plateforme de BI.

   Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.

10. Cliquez sur *Enregistrer*.

18.2.3.8.3.2 Création d'un client OAuth pour SAP Jam

Avant de pouvoir créer une clé du consommateur OAuth :

- Votre entreprise doit être ajoutée à SAP Jam et configurée.
- Vous devez posséder un compte utilisateur SAP Jam valide associé à votre entreprise dans SAP Jam.
- Vous devez disposer des droits d'administration d'entreprise pour votre entreprise dans SAP Jam ainsi que des droits administrateur complets sur la plateforme de BI et dans la zone de lancement BI.
- La zone de lancement BI doit être enregistrée avec SAP Jam en tant que client OAuth qui agit comme un représentant de la zone de lancement dans SAP Jam.
- Chaque utilisateur doit être enregistré dans SAP Jam avec une adresse électronique unique correspondant à l'adresse électronique Enterprise de l'utilisateur dans la zone de lancement BI. Les adresses électroniques seront mappées entre la plateforme de BI et SAP Jam.

SAP Jam ne prend pas en charge Microsoft Internet Explorer 11.

1. Dans SAP Jam, à partir du menu *Administrateur* dans le coin supérieur droit, sélectionnez *Admin*.
   Des informations concernant votre entreprise, notamment votre licence SAP Jam, s'affichent.
2. Dans le menu *Admin*, sélectionnez *Clients OAuth*, puis cliquez sur *Ajouter un client OAtuh*.
3. Dans la boîte de dialogue *Register a new OAuth Client* (Enregistrer un nouveau client OAuth), dans la zone *Name* (Nom), entrez la valeur du fournisseur d'identité unique créé lors de la configuration de SAP Jam sur la plateforme de BI.

   Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.

   SAP Jam affiche le nom de l'application sous forme de lien hypertexte (vers l'URL saisie) lorsqu'une action est effectuée au nom d'un utilisateur.

   Par exemple, saisissez **`<NomEntreprise>_<IdSystème>_<Client>_<Application>`**
4. Dans la zone *URL d'intégration URL*, saisissez l'URL de la zone de lancement BI.

   SAP Jam affiche le nom de l'application sous forme de lien hypertexte renvoyant vers l'URL lorsqu'une action est effectuée au nom d'un utilisateur.
5. Dans la zone *X509 Certificate (Base64)* (Certificat X509 (Base64)), saisissez la valeur du certificat en Base64 générée lors de la configuration de SAP Jam sur la plateforme de BI.

   Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.

   Si vous laissez ce champ vide, SAP Jam fournit un secret de consommateur.
6. Cliquez sur *Enregistrer*.

La clé du consommateur OAuth est générée. Notez la valeur de la clé du consommateur OAuth pour que l'administrateur de la plateforme de BI l'utilise.

18.2.3.9 Gestion du service de notifications push dans SAP BusinessObjects Mobile

Le serveur SAP BusinessObjects Mobile transmet les notifications push aux périphériques iOS des utilisateurs de l'application SAP BusinessObjects Mobile. Les notifications sont transmises dans les scénarios suivants :

- Lorsque les documents BI téléchargés sur le périphérique de l'utilisateur sont mis à jour ou qu'une nouvelle instance est disponible sur le serveur.
- Lorsque l'utilisateur reçoit un nouveau document dans sa boîte de réception BI.
- Lorsque la plateforme de BI ou l'administrateur BOE diffuse un message.

Les notifications sont automatiquement envoyées au périphérique depuis le serveur Mobile via Apple Push Notification Server (APNS). Les utilisateurs n'ont pas besoin d'être connectés au serveur pour recevoir les notifications push. Ils les reçoivent même si l'application n'est pas en cours d'exécution dans le système. Les "paramètres de notification" doivent être activés dans l'application. Pour en savoir plus sur la configuration des notifications push, consultez le *Guide de configuration et de déploiement du serveur Mobile* pour le serveur Mobile 4.2.

> **Remarque**
>
> Pour activer les notifications push sur Mobile, le service BI Mobile doit être en cours d'exécution dans l'APS.
>
> Comme le service BI Mobile ne consomme pas beaucoup de mémoire, vous pouvez l'exécuter avec d'autres services dans l'APS.

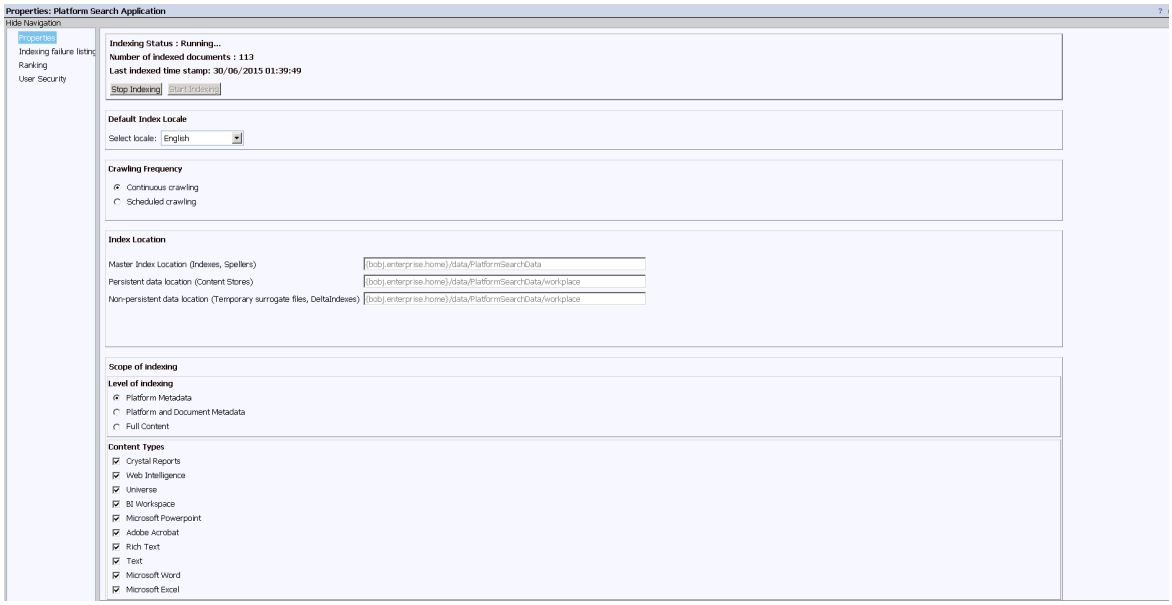
18.2.3.10 Gestion des paramètres de recherche de plateformes

Dans la zone *Applications* de la CMC de la plateforme de BI, il est possible de spécifier des paramètres au niveau système pour l'application de recherche de plateformes.

18.2.3.10.1 Configuration des propriétés de l'application dans la CMC

Pour configurer les propriétés de l'application de recherche de plateformes, procédez comme suit :

1. Accédez à la zone *Applications* de la CMC.
2. Sélectionnez *Application de recherche de plateformes*.
3. Cliquez sur *Gérer* > *Propriétés*. La boîte de dialogue *Propriétés* s'affiche.



4. Configurez les paramètres de la recherche de plateformes :

Option	Description
Statistiques de recherche	La recherche de plateformes fournit les statistiques de recherche suivantes : • Statut de l'indexation : affiche le statut du processus d'indexation. • Nombre de documents indexés : affiche le nombre de documents indexés. • Dernier horodatage indexé : affiche l'horodatage de la dernière indexation du document.
Arrêter/Démarrer l'indexation	Les options de démarrage ou d'arrêt d'indexation permettent de démarrer ou d'arrêter le processus d'indexation pour basculer de l'analyse continue à l'analyse planifiée ou à des fins de maintenance. Pour arrêter l'indexation, cliquez sur *Arrêter l'indexation*.
Paramètres régionaux de l'index par défaut	La recherche de plateformes utilise les paramètres régionaux spécifiés dans la CMC pour l'indexation de tous les documents BI non localisés. Une fois le document localisé, l'analyseur de langage correspondant procède à l'indexation. La recherche est basée sur les paramètres régionaux du produit du client et la pondération est accordée aux paramètres régionaux du produit du client. Vous pouvez configurer la pondération dans les propriétés de configuration de la CMC.

Option	Description
Fréquence de l'analyse	Vous pouvez indexer l'ensemble du référentiel de la plateforme de BI à l'aide des options suivantes : • Analyse continue : avec cette option, l'indexation est continue. Le référentiel est indexé à chaque fois qu'un objet est ajouté, modifié ou supprimé. Cela permet de visualiser ou d'utiliser le plus récent contenu de la plateforme de BI. Définie par défaut, l'analyse continue met à jour de façon continue le référentiel en fonction des actions que vous réalisez. L'analyse continue fonctionne sans intervention de l'utilisateur et réduit le temps nécessaire à l'indexation d'un document. • Analyse planifiée : avec cette option, l'indexation est basée sur la planification définie par les options de planification. Pour en savoir plus sur la planification d'un objet, consultez la section *Planification d'un objet* de l'application de recherche de plateformes dans l'*Aide en ligne de la CMC de la plateforme SAP BusinessObjects Business Intelligence*. **Remarque** • Si vous sélectionnez *Analyse planifiée* et définissez la *Périodicité* sur une option autre que *Maintenant*, l'application de recherche de plateformes affiche la date et l'horodatage de la prochaine indexation planifiée du document. • Si vous sélectionnez *Analyse planifiée*, le bouton *Démarrer l'indexation* est activé et le bouton *Arrêter l'indexation* est désactivé. • Une fois la planification terminée, le bouton *Arrêter l'indexation* est désactivé.

Option	Description
Emplacement de l'index	Les index sont stockés dans des dossiers partagés aux emplacements suivants : • Emplacement de l'index maître (index, vérificateur d'orthographe) : les index maître et de vérificateur d'orthographe sont stockés à cet emplacement. Au cours d'une recherche, les résultats initiaux sont extraits à l'aide de l'index maître tandis que les index de vérificateur d'orthographe sont utilisés pour extraire des suggestions. Dans un déploiement de la plateforme de BI en cluster, cet emplacement doit être situé sur un système de fichiers partagé accessible depuis tous les nœuds du cluster. • Emplacement des données persistantes (stockages de contenu) : le stockage de contenu est situé à cet emplacement. Il est créé depuis l'emplacement de l'index maître et reste synchronisé avec lui. Le stockage de contenu sert à générer des facettes à traiter les accès initiaux générés depuis l'emplacement de l'index maître. Dans un déploiement en cluster de la plateforme de BI, les stockages de contenu sont générés à tous les nœuds. L'emplacement des données persistantes est le seul emplacement d'index affecté par l'environnement en cluster, étant donné qu'il contient les dossiers de stockage du contenu. Si un ordinateur ne dispose que d'un seul service de recherche, il n'existe qu'un seul emplacement de stockage de contenu. Par exemple, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur>\ContentStores. Toutefois, dans un environnement en cluster, s'il existe plusieurs services de recherche, chacun possède un emplacement de stockage de contenu. Par exemple, si deux instances d'un même serveur sont en cours d'exécution, les emplacements de stockage de contenu sont les suivants : 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur 1>\ContentStores. • Emplacement des données non persistantes (fichiers temporaires, index Delta) : les index delta sont créés et stockés temporairement à cet emplacement avant d'être fusionnés avec l'index maître. Les index de cet emplacement sont supprimés après avoir été fusionnés avec l'index maître. En outre, les fichiers de substitution (résultat des extracteurs) sont créés à cet emplacement et stockés temporairement jusqu'à ce qu'ils soient convertis en index delta. **Remarque** • L'emplacement de l'index maître doit être un emplacement partagé. • Vous devez cliquer sur *Arrêter l'indexation* pour modifier l'emplacement de l'index. • Si vous modifiez l'emplacement d'un index, vous devez copier le contenu sur un nouvel emplacement, sinon les informations d'index existantes seront perdues. • Les fichiers d'index peuvent contenir des informations personnelles et confidentielles, en particulier si vous choisissez d'indexer le contenu du document.

Option	Description
	Vous devez autoriser un seul utilisateur système à accéder au dossier partagé et vous devez stocker les dossiers partagés dans un environnement chiffré afin d'éviter tout vol de données.

Niveau d'indexation	Vous pouvez ajuster le contenu de la recherche en définissant le niveau d'indexation de l'une des façons suivantes :
	• Métadonnées de plateformes : un index est créé uniquement pour les informations de métadonnées de plateforme telles que titres, mots clés et descriptions des documents. Par défaut, cette option est sélectionnée.
	• Métadonnées de plates-formes et de documents : cet index comprend les métadonnées de plates-formes ainsi que les métadonnées de documents. Les métadonnées du document comprennent la date de création, la date de modification et le nom de l'auteur.
	• Contenu complet : cet index comprend les métadonnées de plateformes, les métadonnées de documents et les autres contenus tels que :
	  • Le contenu réel du document
	  • Le contenu des invites et listes de valeurs
	  • Diagrammes, graphiques et étiquettes
	Remarque
	L'indexation de l'ensemble du contenu n'est pas prise en charge pour les documents Analysis Office et Lumira. Seule l'indexation des métadonnées est prise en charge pour les documents Analysis Office et Lumira.
	Remarque
	Lorsque vous modifiez le niveau d'indexation, l'indexation est initialisée pour l'actualisation de l'ensemble du référentiel de la plateforme de BI.

Option	Description
Types de contenus	Vous pouvez sélectionner les types de contenu suivants pour l'indexation : • Crystal Reports • Web Intelligence • Univers • Espace de travail BI • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Texte enrichi • Texte • Microsoft Word • Microsoft Excel Le filtre de type de contenu n'est pas applicable à l'indexation des métadonnées de plateformes. Quels que soient les types de contenu sélectionnés, l'indexation des métadonnées de plateformes s'effectue pour tous les types d'objet pris en charge et la recherche entraîne le renvoi par la zone de lancement BI de tous les objets pour le mot clé associé aux métadonnées de plateformes. Le filtre de type de contenu concerne l'indexation des métadonnées de documents (auteur du document, en-tête du document, pied de page du document, etc.) et l'indexation de contenu (diagrammes, graphiques, tableau avec un rapport). En fonction du niveau d'indexation et des types de contenu sélectionnés, la recherche de plateformes indexe les métadonnées et le contenu des documents pour les types d'objet sélectionnés dans le référentiel et seuls ces objets s'affichent dans les résultats de la recherche de la zone de lancement BI lors de la recherche d'un mot clé associé aux métadonnées et au contenu de documents.
Régénérer l'index	Cette option supprime les index existants et réindexe l'ensemble du référentiel. Vous pouvez sélectionner l'option *Régénérer l'index*, que l'indexation soit en cours ou arrêtée. L'index existant est supprimé lorsque vous enregistrez vos modifications dans la page Propriétés. Cependant, si l'indexation est arrêtée, l'index ne commence pas à se régénérer tant que l'indexation n'est pas redémarrée. Si vous ne souhaitez pas que l'application de recherche de plateformes réindexe les documents, désélectionner l'option *Régénérer l'index* avant de cliquer sur *Démarrer l'indexation*.

Option	Description
Documents exclus de l'indexation	L'option *Documents exclus de l'indexation* exclut des documents de l'indexation. Par exemple, vous pouvez décider que les rapports Crystal extrêmement volumineux ne puissent pas être recherchés afin d'éviter de surcharger les ressources des serveurs d'applications de rapports. De même, vous pouvez décider que les publications incluant des centaines de rapports personnalisés ne soient pas indexées. En excluant des documents particuliers, vous pouvez empêcher que les utilisateurs y accèdent à partir de la recherche de plateformes. Il est important de noter que lorsqu'un document est déjà indexé avant d'être ajouté à ce groupe, il peut toujours faire l'objet d'une recherche. Pour que les documents du groupe *Documents exclus de l'indexation* ne puissent pas être recherchés, vous devez régénérer l'index. Par défaut, seul le compte Administrateur dispose du contrôle complet de l'option *Documents exclus de l'indexation*. Les autres utilisateurs disposant des droits suivants peuvent seulement ajouter des documents aux *Documents exclus de l'indexation*. • Droits de visualisation et de modification sur la catégorie • Modifier le document directement
Autre configuration - Ignorer l'instance	Par défaut, les instances de documents sont sélectionnées pour être indexées. De ce fait, la taille de l'index augmente, ce qui entraîne une consommation d'autant plus importante de l'espace disque. La taille du dossier "Lucene Index Engine" dans le dossier PlatformSearchData augmente de façon démesurée en raison de l'indexation d'un très grand nombre d'instances dans le référentiel. S'il y a des millions de documents (ou plus) et que la plupart de ces documents ont également un grand nombre d'instances existantes (ainsi que des instances planifiées générées à intervalles réguliers) dans le système, alors la taille du dossier "Lucene Index Engine" augmente de façon excessive même si le niveau d'indexation est défini sur "Métadonnées de plateformes". La fonctionnalité Ignorer l'instance lors de la recherche de plateformes vous permet de contrôler l'indexation d'instances en l'activant ou la désactivant, via une case à cocher disponible sous "Autre configuration - Ignorer l'instance" dans la page des propriétés de l'application de recherche de plateformes dans la CMC. **Remarque** • Si vous Activez/Désactivez Ignorer l'instance, vous devez redémarrer le serveur de traitement adaptatif de la recherche de plateformes. Cette modification affecte tous les niveaux de l'indexation. • Si vous modifiez Ignorer l'instance et que vous voulez que ces modifications soient appliquées à toutes les instances existantes (c'est à dire toutes les instances devant être sélectionnées pour être indexées), alors vous devez régénérer l'index.

Option	Description
Objets exclus de l'indexation	L'option *Objets exclus de l'indexation* exclut des objets de l'indexation. Par exemple, vous pouvez décider que certains objets ne puissent pas être recherchés afin d'éviter de surcharger les ressources des serveurs d'applications de rapports. En excluant des objets particuliers, vous pouvez empêcher que les utilisateurs y accèdent à partir de la recherche de plateformes. Il est important de noter que lorsqu'un objet est déjà indexé avant d'être ajouté à ce groupe, il peut toujours faire l'objet d'une recherche. Pour que les documents du groupe *Objets exclus de l'indexation* ne puissent pas être recherchés, vous devez régénérer l'index. Liste des objets pouvant être exclus de l'indexation : • Rapport Crystal • Webi • LCMJob • Univers • Excel • PDF • PowerPoint • Rtf • Txt • Word • Page de tableau de bord AF • Lot d'objets • QaaWS • Profil • Événement • Discussions • InformationDesigner • Analyse MD • Publication • Agnostique • Analyses • Lien hypertexte • Programme • pQuery • Fichier de métadonnées DSL • Raccourci • Album DataDiscovery • Classeur AO • Récit VISI • Jeu de données VISI

Option	Description
	• VISI.Lums • VISILums • Utilisateur • Groupe d'utilisateurs

5. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Si l'utilisateur ne sélectionne pas l'option *Régénérer l'index* et modifie le niveau d'indexation ou sélectionne/désélectionne des extracteurs, l'index est progressivement mis à jour sans supprimer l'index existant.

18.2.3.11 Configuration de l'intégration Web BEx

Les applications Web BEx sont des applications Web de Business Explorer (BEx) de SAP Business Warehouse (BW) pour les applications d'analyse de données, de reporting et analytiques sur le Web.

Le Business Explorer est la suite Business Intelligence de SAP NetWeaver, qui fournit des outils de reporting et d'analyse souples pour la prise en charge d'analyses stratégiques et de prise de décision. Ces outils comprennent les fonctions de requête, de reporting et d'analyse. En tant qu'employé disposant de droits d'accès, vous pouvez évaluer les données historiques et actuelles à différents niveaux de détail et depuis différentes perspectives, tant sur le Web que dans Microsoft Excel.

Les utilisateurs accèdent aux données depuis le SAP NetWeaver Portal ou depuis la zone de lancement BI de la plateforme SAP BI. Les auteurs des BEx Web Applications peuvent exécuter les applications Web directement dans la zone de lancement BI à partir du BEx Web Application Designer.

Pour intégrer des applications Web BEx à la plateforme de BI, vous devez suivre la procédure de configuration suivante :

1. Configurez un serveur pour les BEx Web Applications dans la CMC (Central Management Console).

   Vous pouvez utiliser un serveur général ou autonome pour les BEx Web Applications.

   > **→ Conseil**
   >
   > Il est recommandé de configurer un serveur autonome pour les BEx Web Applications car le serveur général est normalement utilisé par beaucoup d'autres services.

2. Configurez les paramètres du serveur.
3. Vérifiez la connexion au système BW.
4. Pour garantir que les auteurs puissent accéder aux BEx Web Applications directement dans la zone de lancement BI à partir du BEx Web Application Designer, vous devez définir les paramètres appropriés dans la table *Portails connectés* (**RSPOR_T_PORTAL**) du système BW.

Après la configuration du serveur de la plateforme de BI, les utilisateurs peuvent ouvrir des applications Web BEx dans la zone de lancement BI. Ils peuvent y parcourir les données et enregistrer les BEx Web Applications sous forme de signets dans les favoris du navigateur Web.

⚠ Restriction

L'intégration est prise en charge à partir des versions suivantes de SAP NetWeaver :

SAP NetWeaver 7.0, package d'extension 1, Support Package Stack 8
SAP NetWeaver 7.3 Support Package Stack 1

La pile Java SAP NetWeaver n'étant pas nécessaire pour cette intégration, les restrictions suivantes sont d'application :

La diffusion des informations BEx n'est pas prise en charge.
Le portail et Knowledge Management de SAP NetWeaver n'étant pas nécessaires, l'intégration de documents et l'utilisation de moteurs de portail ne sont pas prises en charge par les BEx Web Applications.
L'élément Web *Rapport* n'est pas pris en charge. Nous recommandons l'utilisation de SAP Crystal Reports pour le reporting mis en forme.
La bibliothèque d'exportation pour SAP Business Explorer est utilisée pour créer des versions à imprimer des BEx Web Applications. Les services Adobe Document (ADS) ne sont pas disponibles.
Les applications Web BEx intégrées à la plateforme de BI ne peuvent contenir que des sources de données stockées dans le système maître BW. Dans l'administration système, vous définissez quel système est configuré en tant que système maître BW sur la plateforme de BI.
La connexion unique entre la plateforme de BI et le système SAP NetWeaver BW n'est pas activée. Pour chaque session de la plateforme de BI, les utilisateurs des applications Web BEx doivent se connecter au système maître BW correspondant.
L'interface rapport-rapport depuis et vers les applications Web BEx n'est pas prise en charge. Les commandes correspondantes ne seront pas exécutées.
Les tableaux de bord basés sur des requêtes ou des vues de requêtes BEx et créés avec SAP BusinessObjects Dashboards ne sont pas pris en charge.

Pour en savoir plus sur les fonctionnalités des applications Web BEx, voir le SAP Help Portal à l'adresse http://help.sap.com : *SAP NetWeaver 7.3* > *SAP NetWeaver Library: (Bibliothèque SAP NetWeaver) Function-Oriented View (Vue orientée sur les fonctions)* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Analysis & Reporting: (Analyse et reporting) BEx Web Applications (Applications Web BEx)* >.

Pour en savoir plus sur l'accès aux applications Web BEx et leur enregistrement dans la zone de lancement BI, voir le *Guide de l'utilisateur de la zone de lancement BI* à l'adresse suivante : http://help.sap.com.

Informations associées

Démarrage d'un serveur pour les applications Web BEx [page 756]
Démarrage d'un serveur autonome pour les BEx Web Applications [page 756]
Configuration des paramètres de serveur [page 756]
Vérification de la connexion au système BW [page 757]
Configuration d'une connexion entre BEx Web Application Designer et la plateforme de BI [page 758]

18.2.3.11.1 Démarrage d'un serveur pour les applications Web BEx

Pour pouvoir exécuter cette tâche, le serveur de traitement adaptatif doit être arrêté.

1. Connectez-vous à la CMC (Central Management Console).
2. Choisissez *Serveurs*.
3. Développez le nœud *Catégories de service* et sélectionnez *Analysis Services*.
4. Sélectionnez *Serveur de traitement adaptatif* et choisissez *Sélectionner des services* dans le menu contextuel.
5. Déplacez *Service d'applications Web BEx* de la liste *Services disponibles* vers la liste Services située à droite.
6. Redémarrez le service d'applications Web BEx en redémarrant le serveur de traitement adaptatif.

18.2.3.11.2 Démarrage d'un serveur autonome pour les BEx Web Applications

1. Connectez-vous à la CMC (Central Management Console).
2. Choisissez *Serveurs*.
3. Développez le nœud *Catégories de service* et choisissez *Analysis Services*.
4. Sélectionnez *Serveur de traitement adaptatif* et choisissez *Cloner un serveur* dans le menu contextuel.
5. Saisissez le nom du serveur (**`ServeurTraitementAdaptatif`**, par exemple) et sélectionnez le nœud requis dans la case *Cloner sur le nœud*.
6. Sélectionnez le serveur cloné et choisissez *Sélectionner des services* dans le menu contextuel.
7. Sélectionnez *Service d'applications Web BEx* dans la liste *Services disponibles* et déplacez-le vers la liste Services située à droite.
8. Démarrez le service d'applications Web BEx en démarrant le nouveau serveur de traitement adaptatif.

18.2.3.11.3 Configuration des paramètres de serveur

1. Connectez-vous à la CMC (Central Management Console).
2. Choisissez *Serveurs*.
3. Développez le nœud *Catégories de service* et choisissez *Analysis Services*.
4. Sélectionnez le serveur qui héberge le service d'applications Web BEx et choisissez *Propriétés* dans le menu contextuel.
5. Sous *Configuration du service d'applications Web BEx* dans la zone *Service d'applications Web BEx*, définissez les paramètres suivants :
   a. Vérifiez (et modifiez si besoin) le nombre maximal de sessions client.
   b. Sous *Système maître SAP BW*, entrez le nom de la connexion OLAP au système BW que vous avez créé sur la plateforme de BI. Le nom par défaut est *SAP_BW*.

c. Entrez le nom de la *destination RFC du serveur JCo* que vous avez entré dans le système BW sous *Configuration des connexions RFC* (code de transaction **sm59**).
d. Entrez le nom de l'*hôte passerelle du serveur JCo* que vous avez défini dans le système BW sous *Configuration des connexions RFC* (code de transaction **sm59**).
e. Entrez le nom du *service de passerelle du serveur JCo* que vous avez défini dans le système BW sous *Configuration des connexions RFC* (code de transaction **sm59**).
f. Vérifiez (et modifiez si besoin) le *nombre de connexions du serveur JCo*.

6. Cliquez sur *Enregistrer et fermer*.
7. Sélectionnez le serveur qui héberge le service d'applications Web BEx et choisissez *Redémarrer le serveur* dans le menu contextuel.

   Pour appliquer les paramètres sélectionnés, vous devez redémarrer le serveur.

> ⓘ Remarque
>
> Avant de redémarrer le serveur, la destination RFC du système ABAP doit avoir été créée.

Informations associées

Création d'une destination RFC dans le système ABAP [page 758]

18.2.3.11.4 Vérification de la connexion au système BW

1. Connectez-vous à la CMC (Central Management Console).
2. Choisissez *Connexions OLAP*.
3. Vérifiez si une connexion au système BW a été établie. Si ce n'est pas le cas, cliquez sur le bouton *Nouvelle connexion* pour en configurer une. Le nom par défaut de la connexion est **SAP_BW**. Vous pouvez lui attribuer un autre nom.
4. Vérifiez que *Prédéfini* est sélectionné sous *Authentification* et que les entrées requises pour l'utilisateur et le mot de passe ont été complétées.

> ⓘ Remarque
>
> Ce compte utilisateur est requis pour la destination RFC du serveur JCo, qui permet l'intégration de BEx Web Application Designer, du système BW et de la plateforme de BI.

> → Conseil
>
> Pour sécuriser la connexion, assurez-vous que seuls les administrateurs puissent y accéder.
> 1. Pour ce faire, cliquez avec le bouton droit sur la connexion au système BW (nom par défaut : **SAP_BW**) et choisissez *Sécurité de l'utilisateur*.
> 2. Configurez les paramètres de sécurité requis et limitez si possible les droits d'accès aux administrateurs.

18.2.3.11.5 Configuration d'une connexion entre BEx Web Application Designer et la plateforme de BI

Pour garantir que les auteurs puissent exécuter les BEx Web applications directement dans la zone de lancement BI à partir du BEx Web Application Designer, vous devez configurer les paramètres appropriés dans la table *Portails connectés* (**RSPOR_T_PORTAL**) du système BW.

1. Dans le système BW, appelez la transaction **SM30** (*Vue tableau Maintenance*).
2. Sous *Vue/Tableau*, entrez **RSPOR_T_PORTAL**.
3. Choisissez *Maintenir*.
4. Pour créer une entrée, choisissez *Nouvelles entrées*.
5. Définissez les paramètres comme suit :
   a. Pour garantir l'intégration entre le système BW et la plateforme de BI, vous devez créer une destination RFC dans la transaction **SM59**. Entrez cette destination RFC sous *Destination*.
   b. Sélectionnez *Portail standard*. Ainsi, les applications du Web Application Designer sont toujours appelées sur la plateforme de BI.
   c. Sous *Préfixe URL*, entrez l'URL du serveur WACS (Web Application Container Server) de la plateforme de BI en indiquant le protocole, le nom d'hôte et le port, par exemple **http://<wacs><domaine>:<port>**.
   d. Sous *Plateforme*, sélectionnez *BOE*.
   e. Sélectionnez *Utiliser bib. d'exportation SAP (PDF)* si vous souhaitez activer la bibliothèque d'exportation de SAP Business Explorer afin d'autoriser l'exportation de fichiers PDF, PostScript et PCL depuis des BEx Web applications.
6. Enregistrez vos entrées.

Informations associées

Création d'une destination RFC dans le système ABAP [page 758]

18.2.3.11.5.1 Création d'une destination RFC dans le système ABAP

Pour intégrer le système BW et la plateforme de BI, une destination RFC est requise. Cette destination RFC permet au système BW et à la plateforme de BI de communiquer entre elles.

1. Appelez *Configuration des connexions RFC* (code de transaction **SM59**).
2. Choisissez *Créer*.
3. Gérez la destination RFC :
   a. Entrez un nom pour la destination RFC.
   b. Sélectionnez *T pour connexion TCP/IP* comme type de connexion.
   c. Saisissez une description.

      Vous pouvez gérer indépendamment la description de la langue de destination RFC.

d. Sous *Paramètres techniques*, sélectionnez *Programme du serveur enregistré* comme type d'activation.
e. Sous *Paramètres techniques*, entrez l'ID de programme.

   L'ID de programme doit être identique à celui (Destination RFC de serveur JCo) que vous avez spécifié lors de la création de la destination pour ce système BW dans le serveur de la plateforme de BI.
f. Sous *Paramètres techniques*, dans *Options de passerelle*, saisissez l'hôte de passerelle et le service de passerelle que le serveur de la plateforme de BI utilise pour communiquer avec le système BW.

4. Dans la page de l'onglet *Connexion et sécurité*, activez l'option *Envoyer le ticket de connexion à SAP*.
5. Enregistrez vos entrées.

Informations associées

Configuration des paramètres de serveur [page 756]

18.2.3.12 Configuration de la connexion unique SAP HANA

Dans la zone *Applications* de la CMC de la plateforme de BI, vous pouvez configurer la connexion unique pour les connexions à la base de données SAP HANA. La connexion unique est implémentée à l'aide de SAML (Security Assertion Markup Language).

Après avoir ouvert une session de la plateforme de BI, vous pouvez générer un ticket SAML qui peut être utilisé pour se connecter à SAP HANA sans que l'utilisateur n'ait à fournir de mot de passe.

Voici le workflow de base utilisé pour se connecter aux sources de données SAP HANA :

1. Un administrateur configure une approbation entre SAP HANA et la plateforme de BI dans la CMC.
2. Un utilisateur se connecte à la plateforme de BI en utilisant un des fournisseurs d'authentification pris en charge.
3. Si les ID utilisateur de SAP HANA et de la plateforme de BI correspondent, la plateforme de BI est capable de générer une assertion SAML que SAP HANA peut accepter pour établir une connexion pour l'utilisateur actuel. L'ID utilisateur transmis à SAP HANA est l'ID utilisateur de la plateforme de BI pour l'utilisateur qui s'est connecté.
4. Une application client de la plateforme de BI crée une connexion SAP HANA.

> **Remarque**
>
> Avant de configurer la connexion unique SAP HANA avec SAML, vous devez configurer SSL sur l'ordinateur SAP HANA. Pour en savoir plus, consultez la documentation SAP HANA.

18.2.3.12.1 Paramètres de connexion SAP HANA

Le tableau ci-dessous résume les paramètres disponibles dans la CMC pour configurer les connexions SAP HANA.

Paramètre	Description
Nom d'hôte HANA	Fournissez le nom de votre hôte SAP HANA.
Port HANA	Fournissez le numéro de port de votre hôte SAP HANA.
ID du fournisseur d'identité unique	Nom unique au sein d'une installation SAP HANA donnée. L'installation SAP HANA acceptera les tickets correctement signés provenant de ce nom de fournisseur d'identité pour les connexions.
Certificat en base 64 du fournisseur d'identité	Lorsque vous cliquez sur *Générer*, un certificat est créé dans le champ *Certificat en base 64 du fournisseur d'identité*. Copiez ce certificat dans le fichier `trust.pem` de votre déploiement SAP HANA. Ce certificat établit la relation de confiance entre SAP HANA et la plateforme de BI. Le fournisseur d'identité externe lui-même est identifié par un certificat X509, utilisé pour signer toutes les assertions d'identité. Le certificat doit être codé en base 64.
Numéro d'instance HANA	Indiquez le numéro d'instance de votre base de données SAP HANA.
Base de données de locataires HANA	Indiquez le nom de votre base de données de locataires SAP HANA.

18.2.3.12.2 Création d'une connexion SAP HANA

1. Obtenez les paramètres pertinents de la base de données SAP HANA.
   a. Ouvrez l'application SAP HANA Studio.
   b. Ouvrez la page Propriétés de votre système et recherchez l'URL de la connexion à la base de données.
   c. Notez le nom de l'ordinateur hôte, le numéro de port, le numéro d'instance et le nom de la base de données du client.

      Vous aurez besoin de ces informations à l'étape 2.
2. Configurez une connexion SAP HANA sur la plateforme BI.
   a. Accédez à la zone *Applications* de la CMC, puis cliquez deux fois sur la *zone de lancement BI*.
   b. Dans la boîte de dialogue *Authentification HANA*, cliquez sur le bouton *Créer une connexion*.
      La boîte de dialogue *Créer une connexion d'authentification HANA* s'ouvre.
   c. Choisissez un *Type de connexion*.

      > **Remarque**
      >
      > Il est conseillé de sélectionner *SAP HANA* pour une connexion JDBC et *SAP HANA HTTP* pour une connexion HTTP.

   d. Entrez le numéro de port, le nom de l'ordinateur hôte, le numéro d'instance et le nom de la base de données du client que vous avez notés à l'étape 1.
   e. Dans le champ *ID du fournisseur d'identité unique*, spécifiez une valeur à utiliser pour le déploiement de la plateforme BI.
   f. Saisissez *Nom du fournisseur de services*.

      > **Remarque**
      >
      > Vous pouvez vérifier la configuration du nom du fournisseur de service dans HANA en accédant à `indexserver.ini -> Authentication -> saml_service_provider_name`.

> Vous pouvez également modifier la valeur dans HANA en saisissant le code mentionné ci-dessous : `ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;` Dans le code, DEV 00 est le nom du fournisseur de services et vous pouvez le saisir si vous le souhaitez. La meilleure solution pour nommer le fournisseur de services est de combiner l'ID système (DEV) et le numéro d'instance (00).

g. Sélectionnez *Connexion sécurisée*.

> **Remarque**
>
> Vous devez sélectionner *Connexion sécurisée* pour établir une connexion JDBC ou HTTPS sécurisée.
>
> - Pour établir une connexion HTTPS, vous devez sélectionner *HTTP SAP HANA* comme *Type de connexion*, puis *Connexion sécurisée*.
> - Pour établir une connexion HTTPS, vous devez sélectionner *HTTP SAP HANA* comme *Type de connexion*, puis *Connexion sécurisée*.

h. Cliquez sur *Générer*.
Un certificat est créé dans la zone *Certificat en Base64 du fournisseur d'identité*.

3. Configurez votre déploiement SAP HANA.
   a. Connectez-vous au système SAP HANA.
   b. Développez *SSL and Trust Configuration* et sélectionnez *PSE Management*.
   c. Sélectionnez le fichier PSE dans la liste déroulante près de *Gérer PSE*.
   d. Sélectionnez *Importer les certificats*.
   e. Collez le certificat généré à l'étape précédente dans la plateforme de BI.
   f. Sélectionnez *Importer*.
   g. Lancez SAP HANA Studio.
   h. Dans la vue *Systèmes*, développez votre système SAP HANA. Reportez-vous à Guide d'administration SAP HANA One.
   i. Ouvrez (Éditeur de sécurité) à partir du dossier de sécurité.
   j. Sélectionnez (Importer fournisseur d'identités SAML pour fichier de certificat).
   k. Sélectionnez votre fournisseur d'identités dans la liste *Fournisseurs d'identités SAML*.
   l. Sélectionnez (déployer).
   m. Naviguez jusqu'à l'utilisateur SAP HANA dans la vue *Systèmes*.
   n. Ouvrez l'utilisateur SAP HANA dans la zone Éditeurs.
   o. Dans l'onglet *Utilisateur*, vérifiez que l'authentification est bien *SAML* et sélectionnez *Configurer*.
   p. Dans l'assistant *Configurer les identités SAML externes*, sélectionnez *Ajouter*.
   q. Sélectionnez votre fournisseur d'identités.
   r. Sélectionnez OK.
   s. Sélectionnez votre fournisseur d'identités et entrez le nom de l'utilisateur de la plateforme de BI qui est mappé à l'utilisateur HANA pour celui-ci.
   t. Sélectionnez OK.
   u. Sélectionnez (déployer).
   v. Redémarrez le système SAP HANA.
      1. Ouvrez le menu contextuel de votre système SAP HANA.

2. Sélectionnez *Configuration et supervision*.
3. Sélectionnez *Redémarrer le système*.

4. Testez la configuration de SAP HANA.
   a. Accédez à la zone *Applications* de la CMC, puis cliquez deux fois sur *Authentification HANA*,
   b. Dans la boîte de dialogue *Authentification HANA*, ouvrez la connexion créée à l'étape 2.
      La boîte de dialogue *Modifier la connexion d'authentification HANA* s'ouvre.
   c. Sous *Tester la connexion pour cet utilisateur*, saisissez un nom d'utilisateur et cliquez sur le bouton *Tester la connexion* pour vérifier la validité de vos paramètres de connexion.

      Par exemple, saisissez le nom d'utilisateur **`Administrateur`**. Si les paramètres ne sont pas valides, un message d'erreur s'affiche. Vous pouvez essayer ces étapes de dépannage :
      - Vérifiez qu'aucun autre certificat du fichier `trust.pem` ne contient un objet ou un expéditeur ayant la même valeur de propriété CN. Pour voir les composants du certificat, recherchez sur Internet « décodeur de certificat x509 » pour trouver un décodeur de certificat.
      - Essayez ces commandes pour contrôler la configuration côté HANA :

        ```
        select * from "SAML_PROVIDERS"
        select user_name, is_saml_enabled from users where user_name =
        '<UserName>'
        select * from "PUBLIC"."SAML_USER_MAPPINGS"
        ```

      - Si une erreur d'authentification SAML s'affiche lors de la configuration de connexion unique à SAP HANA, essayez cette procédure :
        1. Dans le fichier `indexserver.ini`, définissez le paramètre `sslCreateSelfSignedCertificate` sur **`false`**.
        2. Dans le même fichier, définissez les paramètres `sslKeyStore` et `sslTrustStore` de façon à utiliser des chemins d'accès absolus.
        3. Régénérez les fichiers `key.pem` et `trust.pem`.

Si le fichier `key.pem` n'existe pas dans le répertoire `.ssl`, SAP HANA n'a pas été configuré correctement pour utiliser SSL.

18.2.3.12.3 Configuration d'une connexion SAP HANA HTTPS

La configuration de SAP HANA HTTPS comprend l'ajout du serveur SAP HANA et du certificat émis par l'autorité de certification (CA) du serveur SAP HANA dans le fichier de stockage ou à l'emplacement de votre choix.

> ⓘ Remarque
>
> Vous devez exporter le certificat de serveur SAP HANA du système SAP HANA avant d'ajouter le certificat au TrustStore ou à un autre emplacement.

Ajout du certificat dans le fichier de stockage sécurisé

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.

2. Exécutez la commande suivante : `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. Le serveur SAP HANA et le certificat CA du serveur SAP HANA sont stockés dans le fichier de stockage sécurisé.

> **Remarque**
>
> Les modifications qui ont été apportées au fichier de de stockage des clés sont perdues à l'issue de la mise à niveau de Support Package 4 au Support Package 5 de SAP Business Intelligence Platform si le fichier se trouve à l'emplacement par défaut `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`. Il est donc recommandé d'ajouter le certificat à un autre emplacement.

Ajout du certificat à un emplacement différent

1. Accédez à `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Exécutez la commande suivante : `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Remarque**
   >
   > L'emplacement ci-dessus est fourni à titre d'exemple seulement. Vous pouvez ajouter l'emplacement de votre choix.

3. Pour que le serveur de traitement adaptatif identifie l'emplacement du fichier, exécutez la commande suivante :

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Remarque**
   >
   > cacerts_PATH et Password sont de simples exemples d'emplacement de fichier de stockage des clés et de mot de passe de certificat. Vous pouvez utiliser l'emplacement et le mot de passe de votre choix.

18.2.3.13 Gestion des paramètres de SAP Lumira

Dans la zone "Applications" de la CMC, vous pouvez gérer les droits relatifs à la fonctionnalité d'acquisition de données et de partage de contenu de SAP Lumira pour chaque utilisateur ou groupe d'utilisateurs.

Pour gérer les droits de SAP Lumira, procédez comme suit :

1. Dans la page Accueil de la CMC, sélectionnez *Applications* > *SAP Lumira* > *Sécurité de l'utilisateur*.
2. Sélectionnez l'utilisateur ou le groupe dont vous souhaitez définir les droits.

3. Sélectionnez *Affecter la sécurité*.
4. Sélectionnez *Avancé*.
5. Sélectionnez *Ajouter/Supprimer des droits*.
6. Définissez les droits dont doit disposer l'utilisateur pour SAP Lumira.
7. Cliquez sur *Appliquer*.

18.2.3.14 Gestion des paramètres de SAP Analytics Cloud

18.2.3.14.1 Envoi d'actifs Hub dans SAP Analytics Hub

Vous pouvez ajouter des actifs de BI à une nouvelle catégorie *Actif Hub* et accéder aux mêmes actifs de BI à partir de SAP Analytics Hub.

Créez un *client OAuth* dans SAP Analytics Cloud et notez les valeurs des paramètres comme *URL du client SAP Analytics Cloud*, *URL du jeton*, *ID du Client OAuth* et *Secret*. Vous pouvez consulter la rubrique *Gestion du client OAuth* dans l'aide SAP Analytics Cloud sur le SAP Help Portal pour savoir comment créer un client OAuth.

SAP Analytics Hub vous permet d'accéder à vos actifs de BI sur site et sur le Cloud sur une plate-forme unique. Vous devez configurer la sécurité entre la plateforme de BI et SAP Analytics Cloud, qui sert de fournisseur d'identités pour SAP Analytics Hub, pour permettre à la plateforme de BI de télécharger les actifs de BI vers SAP Analytics Hub.

> **Remarque**
>
> Les publications ne sont pas prises en charge dans la catégorie *Actif Hub*.

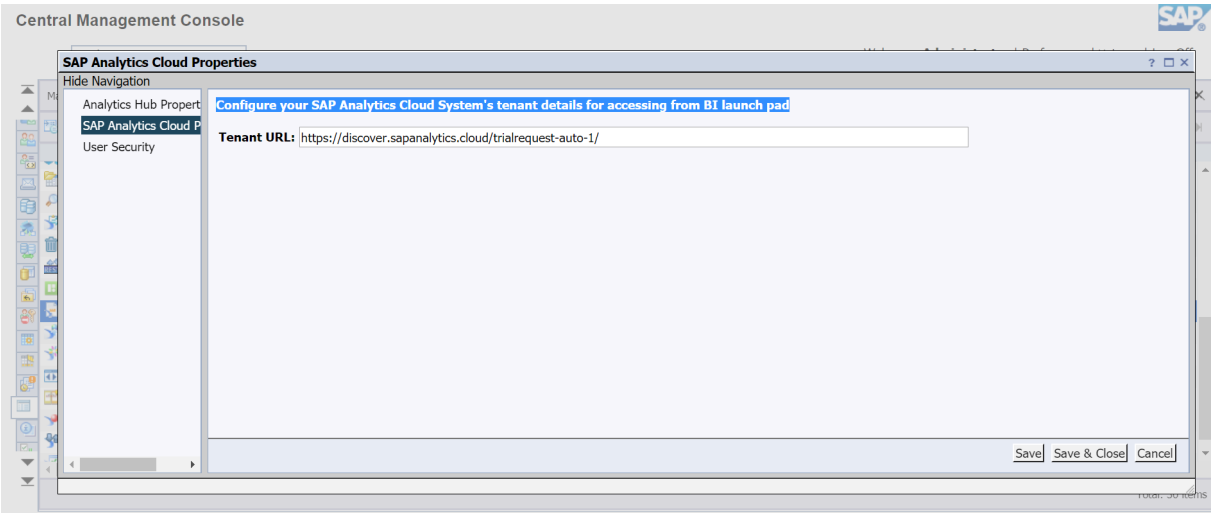
1. Connectez-vous à la CMC et accédez à *Applications* > *SAP Analytics Cloud*.
2. Sélectionnez *Autoriser la plateforme de BI à envoyer les actifs de BI dans SAP Analytics Hub*.
3. Entrez les paramètres suivants :
   - *URL du client SAP Analytics Cloud*
   - *URL du jeton*
   - *ID du Client OAuth*
   - *Secret*
4. Sélectionnez *Enregistrer et fermer*.

Vous avez réussi à configurer SAP Analytics Cloud sur la plateforme de BI pour télécharger les actifs de BI dans la catégorie *Actif Hub* vers SAP Analytics Hub.

18.2.3.14.2 Configuration des paramètres d'URL du client SAP Analytics Cloud

Vous pouvez maintenant configurer les détails du client de votre système SAP Analytics Cloud pour y accéder à partir de la vignette SAC dans les applications de la zone de lancement BI.

> **Remarque**
>
> Par défaut, l'URL est configurée sur l'URL du compte d'essai SAP Analytics Cloud.



18.2.3.15 Configuration du serveur d'autorisation

L'application Configuration du serveur d'autorisation permet d'accéder à toutes les ressources de base de données via le protocole ou le mécanisme du serveur d'autorisation.

Prise en charge OAuth SSO de bout en bout – Prise en charge d'un ou plusieurs serveurs OAuth

Dans la Central Management Console, l'application *Configuration du serveur d'autorisation* permet de configurer et de gérer les serveurs d'autorisation dans la plateforme de BI. Dans l'application, l'administrateur est responsable de l'enregistrement et de la gestion des configurations via les objets de référence d'autorisation. Chaque configuration de serveur d'autorisation possède un objet de référence d'autorisation. Vous pouvez créer des configurations de serveur d'autorisation pour les ressources agnostiques, Google Drive, Microsoft Drive ou OData.

Pour créer une configuration de serveur d'autorisation, renseignez les zones obligatoires sous *Saisir des informations de configuration pour un serveur d'autorisation*.

Le *périmètre d'autorisation* peut être défini en fonction de vos besoins pour permettre de contrôler les accès des utilisateurs finaux, en ligne ou hors ligne.

18.2.3.15.1 Configuration d'un serveur d'autorisation

Vous pouvez configurer un serveur d'autorisation.

1. Lancez et connectez-vous à la Central Management Console en tant qu'administrateur.
2. Sur la page d'accueil, sélectionnez *Applications* sous la colonne *Gérer*.
3. Dans la page *Applications*, double-cliquez sur *Configuration du serveur d'autorisation*.
4. Dans la boîte de dialogue *Configurations du serveur d'autorisation*, effectuez l'une des opérations suivantes :
   - Sélectionnez *Gérer* > *Nouvelle configuration du serveur d'autorisation*.
   - Cliquez sur l'icône de la barre d'outils *Créer une nouvelle configuration du serveur d'autorisation*.
5. Renseignez les paramètres suivants dans la boîte de dialogue *Créer une nouvelle configuration du serveur d'autorisation* :
   - *Nom de référence*.
     Sélectionnez une chaîne aléatoire unique et saisissez-la pour identifier la configuration, reconnaître et sélectionner la configuration dans différents workflows afin d'obtenir une connexion unique basée sur l'autorisation.
   - *Description* (facultatif)
     Saisissez une instruction ou un mot-clé pour décrire et identifier facilement la configuration à partir de la liste des configurations disponibles.
   - **Champs propres à OpenID Connect**
     Les champs suivants sont propres à l'authentification OpenID Connect et ne sont pas requis pour la connexion unique basée sur l'autorisation :
     - Case à cocher *Activé pour l'authentification "OpenID Connect"*
     - *URI de l'émetteur*
     - *URI de jeux de clés Web JSON (jwks_uri)*
     - *ID de l'algorithme de signature du jeton*
   - *Point de terminaison d'autorisation*
     Saisissez l'URL du serveur d'autorisation avec lequel vous pouvez obtenir l'attribution d'autorisation.
   - *Point de terminaison du jeton*
     Saisissez l'URL du serveur d'autorisation avec lequel vous pouvez demander un jeton d'accès en échangeant le code d'autorisation.
   - *ID client*
     Saisissez le nom de l'application utilisée pour enregistrer l'infrastructure BI avec le serveur d'autorisation.
   - *Clé secrète du client*
     Saisissez le code secret spécifique correspondant à l'application utilisée pour enregistrer l'infrastructure BI avec le serveur d'autorisation.
   - *URL de redirection*
     Saisissez l'URL du point de terminaison de l'infrastructure BI auquel le code d'autorisation doit être envoyé par le serveur d'autorisation après la validation réussie de l'autorisation.
   - *Point de terminaison de révocation* (facultatif)
     Saisissez l'URL du serveur d'autorisation avec lequel l'application peut demander la révocation de tous les jetons d'accès précédemment émis via un jeton d'actualisation spécifique.
   - *Périmètre d'autorisation*

Saisissez les périmètres d'autorisation pris en charge par le serveur d'autorisation pour définir les limites d'accès de l'application (infrastructure BI) aux différentes ressources API disponibles.

> **Remarque**
>
> L'implémentation de la plateforme de BI de la connexion unique OAuth est basée sur l'accès hors ligne. Si votre objectif de configuration du serveur d'autorisation dans la plateforme de BI est d'actualiser les données ou d'accéder aux ressources sans qu'il soit nécessaire de valider l'autorisation à chaque fois, vous devez alors configurer ce champ avec le paramètre de périmètre requis et un paramètre obligatoire (par exemple, "refresh_token" ou "offline_access" en fonction du fournisseur du serveur d'autorisation.

- *Type de ressource*
  Sélectionnez le type de ressource souhaité dans la liste des types de ressources pris en charge par la plateforme de BI. Voici la liste actuelle des types de ressources pris en charge dans la plateforme de BI pour la configuration et l'accès via le serveur d'autorisation correspondant :
  - *Agnostique* (valeur par défaut)
    Non spécifique à un fournisseur ou à un protocole. Permet d'indiquer toute ressource accessible avec une attribution d'autorisation réussie par un serveur d'autorisation.
  - *GoogleDrive*
    Permet d'indiquer que la configuration est celle du serveur d'autorisation Google qui peut être utilisé pour accéder à Google Drive vers différents scénarios de la plateforme de BI. À tout moment, une seule configuration de type GoogleDrive peut exister dans le système.
  - *Microsoft Drive*
    Permet d'indiquer que la configuration est celle du serveur d'autorisation Microsoft qui peut être utilisé pour accéder à Microsoft Drive vers différents scénarios de la plateforme de BI. À tout moment, une seule configuration de type Microsoft Drive peut exister dans le système.
  - *OData*
    Non spécifique à un fournisseur, mais permet d'indiquer que la configuration est liée à une ressource accessible via le protocole OData avec une autorisation accordée par un serveur d'autorisation. Comme pour GoogleDrive, à tout moment, une seule configuration de type OData peut exister dans le système.

> **Remarque**
>
> Le paramètre *Type de ressource* n'a rien à voir avec la norme OAuth 2.0. Cependant, cela est introduit dans la configuration pour éviter toute ambiguïté possible dans l'identification de certaines ressources dans la plateforme de BI. Par conséquent, les configurations correspondantes peuvent facilement être sélectionnées et utilisées dans certains scénarios pour obtenir une autorisation.

- *Type d'accès*
  Ce paramètre est spécifique à la configuration de l'autorisation de type *GoogleDrive*. Il sera renseigné automatiquement lorsque la valeur du champ *Type de ressource* sera *GoogleDrive*.
- *Paramètres personnalisés* (facultatif)
  Saisissez les paramètres personnalisés requis à envoyer lors de la demande d'autorisation. Le système se base sur les besoins personnalisés (si nécessaire) du serveur d'autorisation en cours de configuration.

> **Remarque**
>
> Le nom du paramètre personnalisé doit être unique dans la configuration.

> Dans toute configuration d'autorisation, cinq paramètres personnalisés au maximum peuvent être configurés.

6. Après avoir renseigné tous les paramètres requis, sélectionnez *OK* pour valider les détails et enregistrer la configuration.

   La configuration sera sauvegardée en tant qu'objet système dans le référentiel avec le type *Référence d'autorisation*. Vous pouvez vous référer à la configuration dans tous les scénarios pris en charge avec son *Nom de référence*.

18.2.3.15.2 Test de la configuration du serveur d'autorisation

Vous pouvez tester la configuration de votre serveur d'autorisation.

1. Une fois la configuration du serveur d'autorisation enregistrée, lancez la zone de lancement BI et connectez-vous pour tester votre configuration.

   > ⓘ Remarque
   >
   > Il n'est actuellement pas possible de tester la configuration à partir de la CMC.
   >
   > Connectez-vous en tant qu'administrateur ou avec un compte utilisateur de la plateforme de BI, qui n'est pas limité à l'utilisation de la configuration d'autorisation enregistrée ci-dessus.
   >
   > Utilisez la méthode de connexion actuelle configurée pour la zone de lancement BI (par exemple, Enterprise ou toute méthode d'authentification).

2. Sélectionnez l'icône Utilisateur.
3. Dans le menu déroulant qui s'affiche, sélectionnez *Paramètres*.
4. Dans la boîte de dialogue *Paramètres*, sélectionnez *Jetons d'autorisation* dans la section *Compte utilisateur*.
5. Sélectionnez *Générer* dans la colonne *Gestion des jetons*.
6. Conformément à la politique de votre organisation, en fonction de la configuration des autorisations dans votre serveur d'autorisation, la validation du compte sera effectuée en fonction des certificats configurés dans le système ou vous serez invité à saisir le nom d'utilisateur, le mot de passe et/ou l'authentification multifacteur en fonction des paramètres de configuration.
7. Une fois les identifiants ou le certificat validés, la plateforme de BI doit avoir reçu le jeton d'actualisation. Il doit être stocké en toute sécurité dans le référentiel de la plateforme de BI. Une fois cette opération effectuée, vous devez voir les modifications suivantes dans l'onglet *Jetons d'autorisation* :
   - Dans la colonne *Expire le*, vous devez voir la valeur d'expiration du jeton émis par le serveur d'autorisation. Si votre serveur d'autorisation émet un jeton sans expiration, la valeur de la colonne sera mise à jour sur *Aucune expiration*.
   - Sous la colonne *Gestion des jetons*, un bouton *Supprimer* doit apparaître en regard du bouton *Générer*.
     - Le bouton *Supprimer* permet de supprimer le jeton émis par le serveur d'autorisation et cette suppression ne se limite pas à supprimer le jeton du stockage du référentiel de la plateforme de BI. Il peut également se répercuter au serveur d'autorisation en fonction de la configuration et du support.
     - Si le paramètre facultatif *Point de terminaison de révocation* est renseigné avec l'URL appropriée en fonction de la prise en charge par votre serveur d'autorisation, le jeton émis sera également

bloqué au niveau du serveur d'autorisation et effacé du stockage du référentiel de la plateforme de BI.

8. Si le jeton est émis et que la colonne *Expire le* est mise à jour en fonction de l'expiration du jeton émis, la configuration fonctionne et est prête pour le développeur et l'utilisateur final BI.

18.2.3.16 Configuration de la classification des informations

Dans la plateforme de BI, vous pouvez configurer le serveur de la politique Azure de votre organisation afin de permettre à votre infrastructure BI de classer le contenu BI. Ces fonctionnalités de classification peuvent s'appliquer en fonction des étiquettes de confidentialité définies par l'administrateur du serveur de la politique Azure de votre organisation.

> **Remarque**
>
> Cette option d'intégration permettant de configurer un serveur de politique est uniquement prise en charge pour la plateforme Microsoft Azure Information Protection.
>
> La version SAP BusinessObjects BI 4.3 SP04 inclut une option d'intégration pour la plateforme Microsoft Azure Information Protection. Cependant, il est important de noter que l'application permettant de configurer les détails du serveur de la politique Azure dans la plateforme de BI n'est pas activée par défaut. Elle est fournie en tant que fonctionnalité masquée. Pour afficher cette fonctionnalité masquée, voir 3409349.

Cette fonctionnalité est disponible uniquement sur la plateforme Windows.

18.2.3.16.1 Configuration de la classification des informations

1. Connectez-vous à la *Central Management Console* en tant qu'administrateur.
2. Naviguez jusqu'à *Applications*.
3. Cliquez avec le bouton droit de la souris sur l'application *Configuration de la classification des informations*.
4. Sélectionnez *Configuration pour la classification des informations*.
5. Cochez la case *Activer la classification des informations* pour activer la configuration et les champs.
6. Saisissez l'URL de jeton disponible dans le champ *URL du serveur de la politique* du serveur de la politique Azure de votre organisation.
   Le format de l'URL doit être le suivant : `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`.
7. Saisissez les valeurs *ID client* et *Clé secrète du client* de votre application client sur Azure.
   Ces champs sont activés pour le mode de flux d'informations d'identification du client pour l'accès au serveur de la politique Azure de votre organisation.
8. Cliquez sur *Enregistrer et tester la configuration* pour tester la connexion.
9. Si le test de la configuration réussit, cliquez sur *Enregistrer* ou *Enregistrer et fermer*.

> **Remarque**
>
> Ne cochez pas la case liée à *Activée pour l'authentification de certificat*, car ce mode de configuration d'authentification n'est pas pris en charge.

18.3 Gestion des applications à l'aide des propriétés de la couche sémantique

Les options de configuration de la bibliothèque DSL (Dimensional Semantic Layer) peuvent être définies lors de l'exécution afin de modifier le comportement de l'accès direct à HANA et de l'accès direct à BW via les connexions BICS dans les outils de BI tels que Web Intelligence, l'outil de conception d'information, Dashboards et Crystal Reports pour Enterprise. Ces options sont spécifiées via les options de ligne de commande Java de type :

-DoptionName=optionValue

La gestion et la modification de ces paramètres peut poser des problèmes :

- Les options de ligne de commande doivent être spécifiées pour chaque processus Java exécutant DLS. Il n'existe pas d'emplacement commun pour effectuer les modifications.
- Chaque processus Java DSL doit être redémarré pour que les paramètres révisés soient effectifs. Les modifications ne sont pas effectives immédiatement.

Pour simplifier la tâche administrative de gestion des options de configuration DSL-BICS, un nouveau mécanisme a été introduit, qui permet de stocker les options dans un fichier. Les modifications apportées au fichier propagent les nouveaux paramètres d'options à tous les processus DSL qui lisent le fichier.

Le nom et la valeur des options sont stockés dans un fichier comme code XML valide pour java.util.Propertes, comme défini à la page http://java.sun.com/dtd/properties.dtd .

Lorsque vous lancez ce nouveau mécanisme pour la première fois en exécutant DSL, les deux fichiers suivants sont automatiquement générés :

- DSLBICSConfiguration.xml ou DSLConfiguration.xml : ce fichier contient toutes les options disponibles et leurs valeurs par défaut. Ce fichier ne doit pas être modifié.
- DSLBICSConfiguration_custom.xml ou DSLConfiguration_custom.xml : ce fichier contient toutes les options avec les valeurs spécifiées par l'administrateur.

> **Remarque**
>
> - Les fichiers DSLBICSConfiguration.xml et DSLBICSConfiguration_custom.xml sont utilisés pour gérer le comportement de l'accès direct à BW via des connexions BICS.
> - Les fichiers DSLConfiguration.xml et DSLconfiguration_custom.xml sont utilisés pour gérer le comportement de l'accès direct à HANA.

Les fichiers `DSLBICSConfiguration_custom.xml` et `DSLConfiguration_custom.xml` générés contiennent tous les paramètres d'options spécifiés via la ligne de commande, ainsi que les paramètres par défaut d'autres options. Après leur génération initiale, les fichiers `DSLBICSConfiguration_custom.xml` et `DSLConfiguration.xml` peuvent être modifiés pour ajouter ou modifier des valeurs d'options. Le mécanisme

ne met pas à jour le fichier après sa génération initiale. Il met à jour le fichier `DSLBICSConfiguration.xml` avec les nouvelles options disponibles ou en cas d'évolution d'une valeur par défaut.

Pour modifier l'une des propriétés par défaut, utilisez le fichier de configuration personnalisé afin d'enregistrer les nouveaux paramètres de propriétés globales ou spécifiques à l'application. L'emplacement par défaut des fichiers du répertoire est le suivant : `SAP BusinessObjects Enterprise XI 4.0\java\lib`

Ne modifiez pas les propriétés du fichier de configuration par défaut.

18.4 Gestion des applications via les propriétés du fichier BOE.war

18.4.1 Fichier war BOE

Vous pouvez modifier les paramètres des applications Web de la plateforme de BI en écrasant les propriétés par défaut du fichier BOE.war. Ce fichier est déployé sur l'ordinateur hébergeant le serveur d'applications Web. Pour en savoir plus sur le mode de déploiement du fichier, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

Les propriétés contenues dans le fichier BOE.war contrôlent les spécifications du comportement de connexion par défaut, les méthodes d'authentification par défaut et les paramètres de connexion unique. Vous pouvez spécifier deux types de propriétés :

- Propriétés globales : Ces propriétés affectent toutes les applications Web contenues dans le fichier BOE.war.
- Propriétés spécifiques à l'application : Ces propriétés affectent uniquement une application Web spécifique.

Pour modifier l'une des propriétés par défaut, utilisez le répertoire de configuration personnalisé pour enregistrer les nouveaux paramètres de propriétés globales ou spécifiques à l'application. L'emplacement par défaut du répertoire est le suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Ne modifiez pas les propriétés du répertoire `config\default`.

> **Remarque**
>
> Sur certains serveurs d'applications Web comme la version Tomcat fournie avec la plateforme de BI, vous pouvez accéder directement au fichier BOE.war. Dans ce scénario, vous pouvez définir les paramètres personnalisés directement sans annuler le déploiement du fichier WAR. Si vous ne pouvez pas accéder directement aux applications Web déployées, vous devez annuler le déploiement existant, personnaliser, puis redéployer le fichier. Pour en savoir plus, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

18.4.1.1 Propriétés générales de BOE.war

Le tableau suivant répertorie les paramètres inclus dans le fichier `global.properties` par défaut pour BOE.war.

Pour remplacer des paramètres, créez un fichier dans : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Paramètre	Valeurs par défaut	Description
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Active ou désactive les cookies persistants de la page de connexion de l'application Web.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Spécifie quelle méthode d'authentification utiliser avec SiteMinder. Les seules options sont secLDAP et secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Active et désactive l'authentification avec SiteMinder.
`sso.enabled`	`sso.enabled=false`	Active et désactive la connexion unique (SSO) à la plateforme de BI.
`sso.sap.primary`	`sso.sap.primary=false`	Attribuez la valeur `true` pour utiliser la connexion unique SAP comme mécanisme de connexion unique principal de l'application. S'applique uniquement aux cas où les connexions uniques SAP et SiteMinder sont utilisées.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Spécifie le seuil auquel le contrôle d'arborescence n'affiche pas l'ensemble des nœuds, mais un message "Nombre d'enfants trop important".
`trusted.auth.shared.secret`	Aucun	Spécifie le nom de variable de session utilisé pour extraire le secret pour l'authentification sécurisée. Uniquement d'application si la session Web est utilisée pour transmettre le secret partagé.
`trusted.auth.user.param`	Aucun	Spécifie la variable utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée et peut être défini sur l'une des valeurs suivantes : • `Header` • `URL Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	Aucun	Spécifie la méthode utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée et peut être défini sur l'une des valeurs suivantes : • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"`

Paramètre	Valeurs par défaut	Description
		• `"USER_PRINCIPAL"` N'attribuez aucune valeur pour désactiver l'authentification sécurisée.
`trusted.auth.user.namespace.enabled`	`trusted.auth.user.namespace.enabled=false`	Active et désactive la liaison dynamique des alias aux comptes utilisateur existants. Si la propriété est définie sur `true`, l'authentification sécurisée utilise la liaison d'alias pour authentifier les utilisateurs de la plateforme de BI. Avec la liaison d'alias, votre serveur d'applications peut fonctionner comme un fournisseur de service SAML, activant par conséquent l'authentification sécurisée pour fournir une connexion unique SAML au système. Si la valeur `false` est définie, l'authentification sécurisée utilise la correspondance de noms pour authentifier les utilisateurs.

`vintela.enabled`	`vintela.enabled=false`
	`idm.realm=YOUR_REALM`
	`idm.princ=YOUR_PRINCIPAL`
	`idm.allowUnsecured=true`
	`idm.allowNTLM=false`
	`idm.logger.name=simple`
	`idm.logger.props=error-log.properties`
		Permet d'activer ou de désactiver les paramètres Vintela pour l'authentification Windows AD.

`pinger.showWarningDialog.cmc`	`pinger.showWarningDialog.cmc=true`	Spécifie s'il faut ou non afficher le dialogue d'avertissement avec le message indiquant que la session en cours va prochainement expirer dans la CMC.
`pinger.showWarningDialog.bilaunchpad`	`pinger.showWarningDialog.bilaunchpad=true`	Spécifie s'il faut ou non afficher le dialogue d'avertissement avec le message indiquant que la session en cours va prochainement expirer dans la zone de lancement BI.
`pinger.warningPeriod.pingIncrementsInSeconds`	`pinger.warningPeriod.pingIncrementsInSeconds=15`	Spécifie la fréquence d'envoi d'une requête de serveur Web pendant l'affichage de l'avertissement d'expiration de session. Il est important de synchroniser le dialogue d'avertissement à travers les applications.
`pinger.warningPeriod.lengthInMinutes`	`pinger.warningPeriod.lengthInMinutes=5`	Spécifie combien de temps avant l'expiration de session l'avertissement doit être affiché.
`logoff.on.websession.expiry`	`logoff.on.websession.expiry=true`	Spécifie si toutes les sessions d'application se déconnectent lorsque la session Web expire.
`pinger.enabled`	`pinger.enabled=true`	Active ou désactive le mécanisme de message d'avertissement d'expiration de session.

Paramètre	Valeurs par défaut	Description
`system.com.sap.bip.jcomanager.destinations.maxsize`	`system.com.sap.bip.jcomanager.destinations.maxsize=1000`	Spécifie le nombre maximal de connexions Java en cache.
`httpproxy.username`	`httpproxy.username=myusername`	Spécifie le nom d'utilisateur pour se connecter au serveur proxy HTTP.
`httpproxy.password`	`httpproxy.password=mypassword`	Spécifie le mot de passe pour se connecter au serveur proxy HTTP.
`logon.embed.secret`	Aucun	Secret partagé entre un portail qui intègre les applications de la plateforme de BI et le serveur d'applications de celle-ci, qui est utilisé pour déterminer si les applications de la plateforme de BI peuvent être intégrées en sécurité dans d'autres pages.
`logon.embed.timeout`	`logon.embed.timeout=300`	Nombre de secondes après lequel les applications de la plateforme de BI telles que la zone de lancement BI refuseront d'être intégrées dans un portail. Vérifiez que le décalage entre les horloges système du serveur Web de la plateforme de BI et des ordinateurs des serveurs du portail n'est pas supérieur à ce nombre de secondes.
`iview.autologoff`	`iview.autologoff=true`	Définissez sur `true` pour permettre une déconnexion automatique immédiate des iViews de la plateforme technologique SAP NetWeaver.
`pinger.showWarningDialog`	`pinger.showWarningDialog=true`	Spécifie s'il faut ou non afficher la boîte de dialogue d'avertissement avec le message indiquant que la session en cours va prochainement expirer. Ne s'applique pas à la CMC ni à la zone de lancement BI.
`ure.request.queue.timeout.seconds`	`ure.request.queue.timeout.seconds=20`	Nombre de seconde d'attente des demandes précédentes attendues par une demande avant l'expiration. Lorsque les utilisateurs naviguent ou développent des dossiers dans l'arborescence de la zone de lancement BI, les demandes d'AJAX concernant ces actions sont mises en file d'attente. L'interface utilisateur attend l'aboutissement de ces demandes pour rendre le contrôle à l'utilisateur. Ce paramètre détermine le nombre de secondes qu'attendra l'interface utilisateur pour chaque demande si un délai inttendu se produit dans la requête back-end.
`enable.safe.html`	`enable.safe.html=true`	Permet l'utilisation de page URL sécurisées dans les URL du module de page Web pour l'espace de travail BI.

Paramètre	Valeurs par défaut	Description
`upload.file.maxsize.in MB`	`upload.file.maxsize.in MB = 0`	Spécifie la taille de fichier maximale pour le téléchargement de fichiers en mégaoctets. Lorsque la valeur par défaut, c'est-à-dire 0 est définie, des fichiers de toutes les tailles peuvent être téléchargés.
`upload.file.allowed.fo rmats`	Aucun	Spécifie les formats de fichier autorisés pour le téléchargement de fichiers. Pour en savoir plus, voir 2296060.
`upload.file.maxsize.in MB=0`	Aucune	Taille maximale du fichier pour le chargement de documents locaux en mégaoctets ; il doit s'agir d'un nombre entier, par exemple : 10, etc.
`upload.file.allowed.fo rmats=`	Aucune	Cette propriété permet de contrôler les différents types de fichiers autorisés pour le chargement de documents locaux. Pour accéder à la liste des formats de fichiers pris en charge, consultez le note SAP 2296060. Si vous définissez plusieurs formats, séparez chaque format de fichier suivi d'une virgule, par exemple txt,doc,xls.
`offlinehelp.enabled=fa lse`	Aucun	Définissez l'indicateur OfflineHelp sur true (vrai) pour activer l'aide hors ligne. Par défaut, cette valeur est définie sur false (faux).
`offlinehelp.url=`	Aucun	Offlinehelp.url sera utilisé si l'utilisateur a défini l'indicateur hors ligne sur true.

18.4.1.2 Propriétés de la zone de lancement BI

Le tableau suivant répertorie les paramètres inclus dans le fichier `bilaunchpad.properties` par défaut pour le fichier BOE.war. Pour remplacer des paramètres, créez un fichier à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Paramètre	Description
`app.name`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name=BI launch pad`
`app.name.short`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name.short=BI launch pad`

Paramètre	Description
`app.url.name`	Spécifie le nom d'URL de l'application, précédé par le caractère « / ». Par défaut : `app.url.name=/BI`
`authentication.default`	Spécifie la méthode d'authentification par défaut utilisée pour authentifier les utilisateurs dans l'application. Vous pouvez utiliser l'une des méthodes suivantes pour ce paramètre : **Authentification** / **Valeur de paramètre** Enterprise — `secEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3` PeopleSoft — `secpsenterprise` JD Edwards — `secPSE1` Siebel — `secSiebel7` Oracles EBS — `secOraApps` Par défaut : `authentication.default=secEnterprise`
`authentication.visible`	Spécifie si les utilisateurs se connectant à la zone de lancement BI ont la possibilité de visualiser et de modifier la méthode d'authentification. Par défaut : `authentication.visible=false`
`Authentication.VisibleList`	Indique la visibilité de la liste de types d'authentification disponibles dans l'écran de connexion. Voici la liste de types d'authentification disponibles : `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. Dans la liste, vous pouvez choisir d'activer ou de désactiver les types d'authentification en les ajoutant ou en les retirant de `Authentication.VisibleList`. Par défaut : `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
 	
`authentication.sapSystem`
 	
`authentication.sapClient`
	Indique la visibilité des champs *Système SAP* et du *Client SAP* lorsque vous sélectionnez le type d'authentification "SAP". Par défaut : `sap.system.client.visible=true`. Lorsque la propriété `sap.system.client.visible` est définie sur `sap.system.client.visible=false`, vous pouvez spécifier les valeurs des champs Système SAP et Client SAP dans le fichier des propriétés à l'aide des paramètres `authentication.sapSystem` et `authentication.sapClient` respectivement.

Paramètre	Description
`cms.default`	Spécifie le nom de CMS par défaut. Par défaut : `cms.default=[name of host machine]`
`cms.visible`	Spécifie si les utilisateurs se connectant à la zone de lancement BI ont la possibilité de visualiser et de modifier le nom du CMS. Par défaut : `cms.visible=true`
`dialogue.prompt.enabled`	Spécifie si les utilisateurs doivent recevoir une invite lorsqu'ils quittent une page d'entrée dans une boîte de dialogue. Par défaut : `dialogue.prompt.enabled=false`
`logontoken.enabled`	Spécifie si la création d'un jeton doit ou non être activée pour la session après la connexion d'un utilisateur à la zone de lancement BI. Le jeton sera stocké dans un cookie. Par défaut : `logontoken.enabled=false`
`SMTPFrom`	Active ou désactive le champ *De* lors de la planification d'un objet vers une destination. Par défaut : `SMTPFrom=true` Lorsque la valeur est définie sur `false`, le champ *De* n'est pas affiché et le système tente d'extraire la valeur d'e-mail *De* dans l'ordre suivant : 1. D'abord à partir du rapport par défaut pour un objet rapport. 2. Ensuite, à partir de l'adresse électronique dans le profil de l'utilisateur connecté. 3. Pour terminer, à partir du Job Server par défaut.
`url.exit`	Spécifie vers quelle URL les utilisateurs doivent être redirigés une fois leur session de zone de lancement BI terminée. Ce paramètre s'applique uniquement aux utilisateurs s'étant connectés à l'application par le biais d'un processus de vérification externe.
`disable.locale.preference`	Active ou désactive la visualisation et, par conséquent, la modification par l'utilisateur des préférences de paramètres régionaux pour la zone de lancement BI. Par défaut : `disable.locale.preference=false`
`extlogon.allow.logoff`	Active ou désactive automatiquement la déconnexion des sessions utilisateur une fois que les utilisateurs ont fermé leur session de zone de lancement BI. Attribuez la valeur false à ce paramètre si vous voulez que les sessions utilisateur ne se terminent pas lorsque les utilisateurs se déconnectent de la zone de lancement BI. Par défaut : `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Spécifie si l'intégration d'autres pages à cette application (sous forme de cadre) sans transmettre de jeton d'intégration valide est autorisée ou non. Par défaut : `logon.allowInsecureEmbedding=false`

Paramètre	Description
`sso.types.and.order`	Spécifie une liste séparée par des virgules des types de connexion unique à activer et l'ordre dans lequel elles sont exécutées. Une liste vide indique que l'ordre hérité doit être utilisé. Si une liste est spécifiée, les options d'héritage sont ignorées. Options valides : `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` et `siteminder`. Pour ne spécifier aucune liste, saisissez : `none`
`allowed.cms`	Afin de garantir une connexion sécurisée et d'empêcher la falsification des requêtes côté serveur, vous pouvez créer une liste blanche des noms ou adresses IP de CMS valides, avec les numéros de port correspondants. Vous êtes connecté à l'application uniquement si la valeur saisie pendant la connexion correspond exactement à la valeur dans la liste blanche. Entrez la liste des noms ou adresses IP de CMS avec le numéro de port dans la propriété allowed.cms. Par exemple, `allowed.cms =<cms name or IP>:<port number>.` Si vous disposez de plusieurs CMS, entrez les valeurs en les séparant au moyen d'une virgule (,), comme indiqué ci-dessous : `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Remarque** • Pour vous connecter à l'aide du nom ou de l'adresse IP du CMS, ajoutez ces valeurs dans la propriété `allowed.cms`. • Le numéro de port est facultatif dans l'écran de connexion, c'est pourquoi vous pouvez l'omettre de la liste blanche. Vous serez alors connecté au port par défaut. Cependant, si le numéro de port est inclus dans la liste blanche, mais n'est pas saisi à la connexion, celle-ci échoue. L'utilisation d'une liste blanche n'est pas requise dans les scénarios suivants :

Paramètre	Description
	• Si la valeur `cms.visible` est définie sur false et qu'un CMS est défini pour `cms.default`. • Si le CMS réside dans un cluster et que vous vous connectez avec le nom du cluster. Si vous tentez de vous connecter à un cluster spécifique (CMS), le nom de CMS doit être spécifié dans la propriété `allowed.cms`. • Si la connexion s'effectue via la fonction de connexion unique.

18.4.1.3 Propriétés de la zone de lancement BI façon Fiori

Le tableau suivant répertorie les paramètres contenus dans le fichier `FioriBI.properties` par défaut pour le fichier BOE.war. Pour remplacer des paramètres, créez un fichier à l'emplacement suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **Remarque**
>
> Dans BI 4.2 SP5, le fichier « Bing.properties » est renommé « FioriBI.properties ». Lorsque vous mettez à jour ou mettez à niveau BI 4.2 SP5 à partir d'une version plus ancienne, vous devez modifier manuellement le nom du fichier des propriétés de la zone de lancement BI façon Fiori de « Bing.properties » en « FioriBI.properties » pour conserver les configurations existantes pour la zone de lancement BI façon Fiori.

Paramètre	Description
`app.name`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name=BI launch pad`
`app.name.short`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name.short=BI launch pad`
`app.url.name`	Spécifie le nom d'URL de l'application, précédé par le caractère « / ». Par défaut : `app.url.name=/BILaunchpad`
`authentication.default`	Spécifie la méthode d'authentification par défaut utilisée pour authentifier les utilisateurs dans l'application. Vous pouvez utiliser l'une des méthodes suivantes pour ce paramètre :

<table>
<tr><th>Paramètre</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Authentification</th><th>Valeur de paramètre</th></tr>
<tr><td>Enterprise</td><td>secEnterprise</td></tr>
<tr><td>LDAP</td><td>secLDAP</td></tr>
<tr><td>Windows AD</td><td>secWinAD</td></tr>
<tr><td>SAP</td><td>secSAPR3</td></tr>
<tr><td>PeopleSoft</td><td>secpsenterprise</td></tr>
<tr><td>JD Edwards</td><td>secPSE1</td></tr>
<tr><td>Siebel</td><td>secSiebel7</td></tr>
<tr><td>Oracles EBS</td><td>secOraApps</td></tr>
</table>
Par défaut :
authentication.default=secEnterprise
</td></tr>
<tr><td>authentication.visible</td><td>Spécifie si les utilisateurs se connectant à la zone de lancement BI façon Fiori ont la possibilité de visualiser et de modifier la méthode d'authentification. Par défaut : authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>Indique la visibilité de la liste de types d'authentification disponibles dans l'écran de connexion. Voici la liste de types d'authentification disponibles : Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7. Dans la liste, vous pouvez choisir d'activer ou de désactiver les types d'authentification en les ajoutant ou en les retirant de Authentication.VisibleList. Par défaut : Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>Indique la visibilité des champs Système SAP et du Client SAP lorsque vous sélectionnez le type d'authentification "SAP". Par défaut : sap.system.client.visible=true. Lorsque la propriété sap.system.client.visible est définie sur sap.system.client.visible=false, vous pouvez spécifier les valeurs des champs Système SAP et Client SAP dans le fichier des propriétés à l'aide des paramètres authentication.sapSystem= et authentication.sapClient= respectivement.</td></tr>
<tr><td>cms.default</td><td>Spécifie le nom de CMS par défaut. Par défaut : cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>Spécifie si les utilisateurs se connectant à la zone de lancement BI façon Fiori ont la possibilité de visualiser et de modifier le nom du CMS. Par défaut : cms.visible=true</td></tr>
</table>

Paramètre	Description
`dialogue.prompt.enabled`	Spécifie si les utilisateurs doivent recevoir une invite lorsqu'ils quittent une page d'entrée dans une boîte de dialogue. Par défaut : `dialogue.prompt.enabled=false`
`logontoken.enabled`	Spécifie si la création d'un jeton doit ou non être activée pour la session après la connexion d'un utilisateur à la zone de lancement BI. Le jeton sera stocké dans un cookie. Par défaut : `logontoken.enabled=false`
`SMTPFrom`	Active ou désactive le champ *De* lors de la planification d'un objet vers une destination. Par défaut : `SMTPFrom=true` Lorsque la valeur est définie sur `false`, le champ *De* n'est pas affiché et le système tente d'extraire la valeur d'e-mail *De* dans l'ordre suivant : 1. D'abord à partir du rapport par défaut pour un objet rapport. 2. Ensuite, à partir de l'adresse électronique dans le profil de l'utilisateur connecté. 3. Pour terminer, à partir du Job Server par défaut.
`url.exit`	Spécifie vers quelle URL les utilisateurs doivent être redirigés une fois leur session de zone de lancement BI façon Fiori terminée. Ce paramètre s'applique uniquement aux utilisateurs s'étant connectés à l'application par le biais d'un processus de vérification externe.
`disable.locale.preference`	Active ou désactive la visualisation et, par conséquent, la modification par l'utilisateur des préférences de paramètres régionaux pour la zone de lancement BI façon Fiori. Par défaut : `disable.locale.preference=false`
`extlogon.allow.logoff`	Active ou désactive automatiquement la déconnexion des sessions utilisateur une fois que les utilisateurs ont fermé leur session de zone de lancement BI façon Fiori. Attribuez la valeur false à ce paramètre si vous voulez que les sessions utilisateur ne se terminent pas lorsque les utilisateurs se déconnectent de la zone de lancement BI. Par défaut : `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Spécifie si l'intégration d'autres pages à cette application (sous forme de cadre) sans transmettre de jeton d'intégration valide est autorisée ou non. Par défaut : `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Spécifie une liste séparée par des virgules des types de connexion unique à activer et l'ordre dans lequel elles sont exécutées. Une liste vide indique que l'ordre hérité doit être utilisé. Si la liste est spécifiée, les options d'héritage sont ignorées.

Paramètre	Description
	Options valides : `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` et `siteminder`. Pour ne spécifier aucune liste, saisissez : `none`
`allowed.cms`	Afin de garantir une connexion sécurisée et d'empêcher la falsification des requêtes côté serveur, vous pouvez créer une liste blanche des noms ou adresses IP de CMS valides, avec les numéros de port correspondants. Vous êtes connecté à l'application uniquement si la valeur saisie pendant la connexion correspond exactement à la valeur dans la liste blanche. Entrez la liste des noms ou adresses IP de CMS avec le numéro de port dans la propriété allowed.cms. Par exemple, `allowed.cms =<cms name or IP>:<port number>.` Si vous disposez de plusieurs CMS, saisissez les valeurs en les séparant au moyen d'une virgule (,), comme indiqué ci-dessous : `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Remarque** • Pour vous connecter à l'aide du nom ou de l'adresse IP du CMS, ajoutez ces valeurs dans la propriété `allowed.cms`. • Le numéro de port est facultatif dans l'écran de connexion, c'est pourquoi vous pouvez l'omettre de la liste blanche. Vous serez alors connecté au port par défaut. Cependant, si le numéro de port est inclus dans la liste blanche, mais n'est pas saisi à la connexion, celle-ci échoue. L'utilisation d'une liste blanche n'est pas requise dans les scénarios suivants : • Si la valeur `cms.visible` est définie sur false et qu'un CMS est défini pour `cms.default`. • Si le CMS réside dans un cluster et que vous vous connectez avec le nom du cluster. Si vous tentez de vous connecter à un cluster spécifique (CMS), le nom de CMS doit être spécifié dans la propriété `allowed.cms`.

Paramètre	Description
	• Si la connexion s'effectue via la fonction de connexion unique.
upload.file.maxsize.inMB=0	Taille maximale du fichier pour le chargement de documents locaux en mégaoctets ; il doit s'agir d'un nombre entier, par exemple : 10, etc.
upload.file.allowed.formats=	Cette propriété permet de contrôler les différents types de fichiers autorisés pour le chargement de documents locaux. Pour accéder à la liste des formats de fichiers pris en charge, consultez le note SAP 2296060. Si vous définissez plusieurs formats, séparez chaque format de fichier suivi d'une virgule, par exemple txt,doc,xls.
app.custom.banner.message	Indique le message sous forme de bannière dans la zone de lancement BI.
logon.webssoauthnetication.framework=Aucun	Cette propriété est utilisée pour activer le workflow d'authentification SSO Web. Les valeurs possibles sont Aucun, OpenId et SAML.
openid.restful.url=	Cette propriété est utilisée pour définir l'URL Restful fournie dans la CMC. Par exemple : `http://<hostname>:<portNo>/biprws`

18.4.1.4 Propriétés OpenDocument

Le tableau suivant répertorie les paramètres contenus dans le fichier `opendocument.properties` par défaut pour le fichier war BOE. Pour remplacer des paramètres, créez un fichier dans : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Paramètre	Description
`app.name`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name=SAP BusinessObjects OpenDocument`
`app.name.short`	Spécifie le nom d'affichage de l'application. Le nom apparaît sur la page de titre de l'application Web et sur l'écran de connexion. Par défaut : `app.name.short=OpenDocument`
`authentication.default`	Spécifie la méthode d'authentification par défaut utilisée pour authentifier les utilisateurs dans l'application. Vous pouvez utiliser l'une des méthodes suivantes pour ce paramètre :

<table>
<tr><th>Paramètre</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Authentification</th><th>Valeur de paramètre</th></tr>
<tr><td>Enterprise</td><td>secEnterprise</td></tr>
<tr><td>LDAP</td><td>secLDAP</td></tr>
<tr><td>Windows AD</td><td>secWinAD</td></tr>
<tr><td>SAP</td><td>secSAPR3</td></tr>
<tr><td>PeopleSoft</td><td>secpsenterprise</td></tr>
<tr><td>JD Edwards</td><td>secPSE1</td></tr>
<tr><td>Siebel</td><td>secSiebel7</td></tr>
<tr><td>Oracles EBS</td><td>secOraApps</td></tr>
</table>
Par défaut : <code>authentication.default=secEnterprise</code></td></tr>
<tr><td>authentication.visible</td><td>Spécifie si les utilisateurs se connectant à OpenDocument ont la possibilité de visualiser et modifier la méthode d'authentification. Par défaut : <code>authentication.visible=false</code></td></tr>
<tr><td>Authentication.VisibleList</td><td>Indique la visibilité de la liste de types d'authentification disponibles dans l'écran de connexion. Voici la liste de types d'authentification disponibles : <code>Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</code>. Dans la liste, vous pouvez choisir d'activer ou de désactiver les types d'authentification en les ajoutant ou en les retirant de <code>Authentication.VisibleList</code>. Par défaut : <code>Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</code></td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>Indique la visibilité des champs Système SAP et du Client SAP lorsque vous sélectionnez le type d'authentification "SAP". Par défaut : <code>sap.system.client.visible=true</code>. Lorsque la propriété <code>sap.system.client.visible</code> est définie sur <code>sap.system.client.visible=false</code>, vous pouvez spécifier les valeurs des champs Système SAP et Client SAP dans le fichier des propriétés à l'aide des paramètres <code>authentication.sapSystem=</code> et <code>authentication.sapClient=</code> respectivement.</td></tr>
<tr><td>cms.default</td><td>Spécifie le nom de CMS par défaut. Par défaut : <code>cms.default=[name of host machine]</code></td></tr>
<tr><td>cms.visible</td><td>Spécifie si les utilisateurs se connectant à la OpenDocument ont la possibilité de visualiser et modifier le nom du CMS. Par défaut : <code>cms.visible=true</code></td></tr>
</table>

Paramètre	Description
`logontoken.enabled`	Spécifie si la création de jeton doit ou non être activée pour la session après la connexion d'un utilisateur à OpenDocument. Le jeton sera stocké dans un cookie. Par défaut : `logontoken.enabled=false`
`extlogon.allow.logoff`	Active ou désactive automatiquement la déconnexion des sessions utilisateur une fois que les utilisateurs ont fermé leur session OpenDocument. Attribuez-y la valeur false si vous voulez que les sessions utilisateur ne se terminent pas lorsque les utilisateurs se déconnectent d'OpenDocument. Par défaut : `extlogon.allow.logoff=true`
`SAPLogonToken.enabled`	Spécifie si l'authentification des jetons de connexion SAP de service Web RESTful auprès de la plateforme de BI doit ou non être permise. Le jeton de connexion SAP est spécifié par la valeur X-SAP-LogonToken dans l'en-tête de requête après une connexion réussie à l'URL de service Web RESTful. Par défaut : `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Spécifie si les autres pages sont autorisées à être intégrées à cette application (sous forme de cadre) sans transmettre de jeton d'intégration valide. Par défaut : `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Spécifie une liste séparée par des virgules des types de connexion unique à activer et l'ordre dans lequel elles sont exécutées. Une liste vide indique que l'ordre hérité doit être utilisé. Si la liste est spécifiée, les options d'héritage sont ignorées. Options valides : `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO` et `siteminder`. Si vous n'en voulez aucune, spécifiez : `none`
`allowed.cms`	Afin de garantir une connexion sécurisée et d'empêcher la falsification des requêtes côté serveur, vous pouvez créer une liste blanche des noms ou adresses IP de CMS valides, avec les numéros de port correspondants. Vous êtes connecté à l'application uniquement si la valeur saisie pendant la connexion correspond exactement à la valeur dans la liste blanche. Entrez la liste des noms ou adresses IP de CMS avec le numéro de port dans la propriété allowed.cms. Par exemple, `allowed.cms =<cms name or IP>:<port number>.` Si vous disposez de plusieurs CMS, entrez les valeurs en les séparant au moyen d'une virgule (,),

Paramètre	Description
	comme indiqué ci-dessous : `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Remarque** • Pour vous connecter à l'aide du nom ou de l'adresse IP du CMS, ajoutez ces valeurs dans la propriété `allowed.cms`. • Le numéro de port est facultatif dans l'écran de connexion, c'est pourquoi vous pouvez l'omettre de la liste blanche. Vous serez alors connecté au port par défaut. Cependant, si le numéro de port est inclus dans la liste blanche, mais n'est pas saisi à la connexion, celle-ci échoue. L'utilisation d'une liste blanche n'est pas requise dans les scénarios suivants : • Si la valeur `cms.visible` est définie sur false et qu'un CMS est défini pour `cms.default`. • Si le CMS réside dans un cluster et que vous vous connectez avec le nom du cluster. Si vous tentez de vous connecter à un cluster spécifique (CMS), le nom de CMS doit être spécifié dans la propriété `allowed.cms`. • Si la connexion s'effectue via la fonction de connexion unique.

18.4.1.5 Propriétés de la CMC

Le tableau suivant répertorie les paramètres inclus dans le fichier `cmc.properties` par défaut pour BOE.war. Pour remplacer des paramètres, créez un fichier dans : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Paramètre	Description
`app.url.name`	Spécifie le nom d'URL de l'application, précédé par le caractère« / »". Par défaut : `app.url.name=/CMC`
`authentication.default`	Spécifie la méthode d'authentification par défaut utilisée pour authentifier les utilisateurs dans l'application. Vous pouvez utiliser l'une des méthodes suivantes pour ce paramètre :

Paramètre	Description
	<table><tr><th>Authentification</th><th>Valeur de paramètre</th></tr><tr><td>Enterprise</td><td>secEnterprise</td></tr><tr><td>LDAP</td><td>secLDAP</td></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr><tr><td>JD Edwards</td><td>secPSE1</td></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table> Par défaut : `authentication.default=secEnterprise`
`authentication.visible`	Spécifie si les utilisateurs se connectant à la CMC ont la possibilité de visualiser et modifier la méthode d'authentification. Par défaut : `authentication.visible=false`
`Authentication.VisibleList`	Indique la visibilité de la liste de types d'authentification disponibles dans l'écran de connexion. Voici la liste de types d'authentification disponibles : `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. Dans la liste, vous pouvez choisir d'activer ou de désactiver les types d'authentification en les ajoutant ou en les retirant de `Authentication.VisibleList`. Par défaut : `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
`authentication.sapSystem`
`authentication.sapClient`
	Indique la visibilité des champs *Système SAP* et du *Client SAP* lorsque vous sélectionnez le type d'authentification "SAP". Par défaut : `sap.system.client.visible=true`. Lorsque la propriété `sap.system.client.visible` est définie sur `sap.system.client.visible=false`, vous pouvez spécifier les valeurs des champs Système SAP et Client SAP dans le fichier des propriétés à l'aide des paramètres `authentication.sapSystem=` et `authentication.sapClient=` respectivement.

`cms.default`	Spécifie le nom de CMS par défaut. Par défaut : `cms.default=[name of host machine]`
`cms.visible`	Spécifie si les utilisateurs se connectant à la CMC ont la possibilité de visualiser et de modifier le nom du CMS. Par défaut : `cms.visible=true`

Paramètre	Description
`dialogue.prompt.enabled`	Spécifie si les utilisateurs doivent recevoir une invite lorsqu'ils quittent une page d'entrée dans une boîte de dialogue. Par défaut : `dialogue.prompt.enabled=false`
`logontoken.enabled`	Spécifie si la création de jeton doit ou non être activée pour la session après la connexion d'un utilisateur à la CMC. Le jeton sera stocké dans un cookie. Par défaut : `logontoken.enabled=false`
`SMTPFrom`	Active ou désactive le champ *De* lors de la planification d'un objet vers une destination. Par défaut : `SMTPFrom=true` Lorsque la valeur est définie sur `false`, le champ *De* n'est pas affiché et le système tente d'extraire la valeur d'e-mail *De* dans l'ordre suivant : 1. D'abord à partir du rapport par défaut pour un objet rapport. 2. Ensuite, à partir de l'adresse électronique dans le profil de l'utilisateur connecté. 3. Pour terminer, à partir du Job Server par défaut.
`ulr.exit`	Spécifie vers quelle URL rediriger les utilisateurs une fois leur session CMC terminée. Ce paramètre s'applique uniquement aux utilisateurs s'étant connectés à l'application par le biais d'un processus de vérification externe.
`allowed.cms`	Afin de garantir une connexion sécurisée et d'empêcher la falsification des requêtes côté serveur, vous pouvez créer une liste blanche des noms ou adresses IP de CMS valides, avec les numéros de port correspondants. Vous êtes connecté à l'application uniquement si la valeur saisie pendant la connexion correspond exactement à la valeur dans la liste blanche. Entrez la liste des noms ou adresses IP de CMS avec le numéro de port dans la propriété allowed.cms. Par exemple, `allowed.cms =<cms name or IP>:<port number>.` Si vous disposez de plusieurs CMS, entrez les valeurs en les séparant au moyen d'une virgule (,), comme indiqué ci-dessous : `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Remarque** • Pour vous connecter à l'aide du nom ou de l'adresse IP du CMS, ajoutez ces valeurs dans la propriété `allowed.cms`.

Paramètre	Description
	> • Le numéro de port est facultatif dans l'écran de connexion, c'est pourquoi vous pouvez l'omettre de la liste blanche. Vous serez alors connecté au port par défaut. Cependant, si le numéro de port est inclus dans la liste blanche, mais n'est pas saisi à la connexion, celle-ci échoue. L'utilisation d'une liste blanche n'est pas requise dans les scénarios suivants : • Si la valeur `cms.visible` est définie sur false et qu'un CMS est défini pour `cms.default`. • Si le CMS réside dans un cluster et que vous vous connectez avec le nom du cluster. Si vous tentez de vous connecter à un cluster spécifique (CMS), le nom de CMS doit être spécifié dans la propriété `allowed.cms`. • Si la connexion s'effectue via la fonction de connexion unique.

18.5 Personnalisation des points d'entrée de connexion de la zone de lancement BI et OpenDocument

Vous pouvez personnaliser la page de connexion pour les applications Web de la zone de lancement BI et OpenDocument. Par exemple, vous pouvez personnaliser la page de connexion pour utiliser un logo d'entité ou une feuille de style d'entreprise, ou vous pouvez créer une page de connexion personnalisée activant l'authentification sécurisée.

Pour personnaliser la page de connexion, modifiez le fichier `custom.jsp` stocké dans les zones des applications de zone de lancement BI et OpenDocument de l'application Web `BOE.war`, puis redéployez l'application Web `BOE.war` sur votre système de la plateforme de BI. Les utilisateurs accèdent au point d'entrée de connexion personnalisé en naviguant vers une URL unique.

Pour utiliser ces exemples, vous devez être familier du déploiement d'applications Web de la plateforme de BI. Pour en savoir plus, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

18.5.1 Emplacements des fichiers Zone de lancement BI et OpenDocument

Les applications Web Zone de lancement BI et OpenDocument sont livrées dans le fichier d'archives Web `BOE.war`. L'emplacement du fichier d'archive `BOE.war` est définie dans le fichier `BOE.properties`.

Le fichier `BOE.properties` se trouve ici sur les systèmes Windows :

- `<REP_INSTALL_BOE>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

Le fichier `BOE.properties` se trouve ici sur les systèmes UNIX :

- `<REP_INSTALL_BOE>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

Les tableaux suivants définissent l'emplacement des fichiers communs dans le fichier d'archive Web `BOE.war`pour les applications Zone de lancement BI et OpenDocument.

Emplacements des fichiers de la zone de lancement BI

> **Remarque**
>
> L'application Web Zone de lancement BI était anciennement connue sous le nom d'InfoView.

Type de fichier	Emplacement
Script de connexion personnalisé	`WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
Répertoire pour d'autres fichiers	`WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`
URL de connexion personnalisée	`http://<nom_de_serveur>:<port>/BOE/BI/custom.jsp`

Emplacements des fichiers OpenDocument

Type de fichier	Emplacement
Script de connexion personnalisé	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`
Répertoire pour d'autres fichiers	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
URL de connexion personnalisée	`http://<nom_de_serveur>:<port>/BOE/OpenDocument/opendoc/custom.jsp`

18.5.2 Pour définir une page de connexion personnalisée

Vous pouvez personnaliser le point d'entrée vers la page de connexion de la plateforme de BI. Par exemple, vous pouvez créer une page de connexion personnalisée affichant un logo d'entité et utilisant une feuille de style d'entreprise.

Modifiez le fichier `custom.jsp` pour personnaliser l'expérience de connexion de vos utilisateurs, puis placez les fichiers de prise en charge dans le dossier `noCacheCustomResources`.

Cet exemple indique comment créer une page de connexion personnalisée redirigeant l'utilisateur vers une page de connexion standard.

1. Créez un fichier contenant votre code de connexion personnalisé et enregistrez-le sous `custom.js` dans le dossier `noCacheCustomResources`.

   Cet exemple définit une fonction qui redirige l'utilisateur vers la page de connexion standard, `logon.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. Modifiez le fichier `custom.jsp` pour personnaliser la page de connexion.

   Cet exemple affiche un message de bienvenue et un lien hypertexte appelant la méthode `load` définie dans le fichier `custom.js`.

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
   <%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
   <html>
     <head> <title>Welcome</title>
     </head>
     <body>
       <script type=  "text/javascript" src=  "noCacheCustomResources/
   custom.js"></script>
       <p>Welcome to ABC corporation.</p>
       <a href= "javascript:load()">Enter</a>
     </body>
   </html>
   ```

3. Redéployez l'application Web `BOE.war` et redémarrez le serveur Web.

18.5.3 Pour ajouter l'authentification sécurisée à la connexion

Pour activer l'authentification sécurisée, définissez l'utilisateur sécurisé en tant qu'attribut de session dans le fichier `custom.jsp` et modifiez les paramètres d'authentification dans une copie du fichier `global.properties`. Les valeurs de la copie personnalisée du fichier `global.properties` écrasent les valeurs par défaut.

> **Remarque**
>
> L'authentification sécurisée ne doit pas être activée sans HTTPS pour des raisons de sécurité. Si vous avez activé l'authentification sécurisée sans HTTPS, celle-ci est considérée comme une violation de la sécurité car l'URL est exposée à des utilisateurs non autorisés. Pour éviter une violation de la sécurité, les informations de l'utilisateur peuvent être validées avec un certificat valide. Pour en savoir plus, voir la note SAP 1388240.

1. Modifiez le fichier `custom.jsp` pour définir un attribut de session définissant l'utilisateur sécurisé.

   ```
   request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
   ```

2. Créez une copie personnalisée du fichier `global.properties` en copiant `WEB-INF\config\default\global.properties` sur `WEB-INF\config\custom\global.properties`.
3. Modifiez `WEB-INF\config\custom\global.properties` pour activer la connexion unique.

   ```
   sso.enabled=true
   ```

4. Modifiez `WEB-INF\config\custom\global.properties` pour définir les paramètres d'authentification sécurisée, y compris la variable de session utilisateur sécurisé et le secret partagé.

   Remplacez `"..."` par le secret partagé de votre système.

   ```
   trusted.auth.user.param=TrustedUserAttribute
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.shared.secret="..."
   ```

   Pour en savoir plus, voir la rubrique associée sur la configuration de l'authentification sécurisée pour les applications Web.
5. Redéployez votre application Web et redémarrez le serveur Web.
6. Dans la CMC, activez l'authentification sécurisée.

   Dans l'onglet *Authentification*, cliquez deux fois sur *Enterprise*, puis cochez la case *L'authentification sécurisée est activée*.

Informations associées

Activation de l'authentification sécurisée [page 265]
Pour configurer l'authentification sécurisée pour l'application Web [page 272]

18.6 Personnalisation des interfaces utilisateur d'application

Certaines interfaces utilisateur d'application peuvent être personnalisées au moyen de la CMC.

Dans la Central Management Console, vous pouvez personnaliser l'apparence de certaines applications. Vous pouvez par exemple activer et désactiver des éléments d'interface utilisateur.

18.6.1 Web Intelligence

18.6.1.1 Personnalisation des éléments d'interface Web Intelligence par groupe d'utilisateurs ou dossiers

Via la personnalisation, vous pouvez masquer plusieurs éléments d'interface afin de simplifier l'interaction des utilisateurs finaux avec l'application, en fonction des groupes d'utilisateurs et des dossiers contenant les documents Web Intelligence. Vous pouvez masquer les types de source de données, activer/désactiver le mode Édition, désactiver la fonctionnalité d'actualisation automatique et bien plus encore.

Par défaut, chaque élément d'interface est activé. Si vous souhaitez les masquer, vous pouvez le faire dans la Central Management Console. Le tableau ci-dessous répertorie les éléments de l'interface utilisateur que vous pouvez masquer.

Liste des fonctionnalités	Description
Mode	Masque les modes accessibles pour l'utilisateur via le bouton de liste déroulante. • Lecture Pour masquer le mode Lecture dans le bouton de liste déroulante. • Conception Pour masquer les modes Conception et Structure dans le bouton de liste déroulante. • Données Pour masquer le mode Données dans le bouton de liste déroulante. Si tous les modes sont désactivés, les documents peuvent uniquement être ouverts en mode Lecture.
Emplacement	Masque toute une catégorie de sources de données. Les catégories que vous pouvez désactiver sont les suivantes : • Référentiel de plate-forme BI • Local (disponible uniquement dans Rich Client) • Services Web • Google Drive • Microsoft OneDrive
Source de données	En mode Conception, vous pouvez restreindre les sources de données disponibles dans les boîtes de dialogue *Sélectionner une source de données* et *Modifier la source*. Les sources de données que vous pouvez désactiver sont les suivantes : • Univers • Documents Web Intelligence • Fichiers Excel • Fichiers texte • SAP BW • Vues SAP HANA • Requêtes SQL à la carte • OData • Feuille de calcul Google
Requête	• Actualisation En mode Lecture, masque la section *Données* de la barre d'outils. En mode Conception, masque le menu déroulant *Actualisation*, la commande *Tout actualiser*, le bouton *Exécuter* et son menu déroulant dans l'Éditeur de requête. • Actualisation avancée En mode Conception, masque la commande *Actualisation avancée* dans le menu déroulant *Actualisation*. • Actualisation automatique Masque l'option *Actualisation automatique* en mode Présentation. • Modifier la source En mode Conception, masque la possibilité de modifier les sources de données du document.
Données	En mode Données, masque les fonctionnalités Combiner des cubes.

Liste des fonctionnalités	Description
Analyse	• Exploration En mode Lecture et Conception, masque la case à cocher *Exploration* dans la section Analyser de la barre d'outils, Filtres d'exploration dans la *Barre de filtre*. En outre, dans le rapport, les valeurs pouvant être explorées ne sont pas affichées sous forme de liens hypertexte et les actions et icônes d'exploration disponibles pour ces valeurs sont masquées. En mode Conception, masque les filtres d'exploration dans le panneau *Générer*, sous *Filtres de données*. • Suivi des modifications apportées aux données En mode Lecture et Conception, masque *Suivre les modifications apportées aux données* et *Afficher les modifications* dans la barre d'outils.
Documents	• *Nouveau*, *Ouvrir*, *Enregistrer*, *Favoris*, *Mode Présentation* Masque les boutons correspondants dans la barre d'outils. • Commentaires En mode Lecture et Conception, masque l'onglet *Commentaires* du panneau latéral et la commande *Commentaires* dans le menu contextuel. • Éléments partagés En mode Conception, masque l'onglet *Éléments partagés* du panneau latéral et la commande *Éléments partagés* dans la section *Insérer* de la barre d'outils.
Exporter vers	Dans tous les modes, masque la possibilité d'exporter des rapports et des cubes de documents vers : • Excel • PDF • HTML • TXT • CSV
Générer un lien	En mode Conception, masque la possibilité de créer un lien OpenDocument et de générer des liens OData pour les requêtes et les éléments individuels de rapport dans les menus contextuels.
Planifier et publier	Masque la possibilité de planifier et de publier des documents au format TXT, XLS, PDF, HTML, MHTML et CSV.

18.6.1.1.1 Interface de personnalisation

Vous pouvez sélectionner des dossiers individuels afin que les documents qu'ils contiennent bénéficient automatiquement de la personnalisation. Il vous suffit de sélectionner un ou plusieurs dossiers dans la zone *Dossiers personnalisés* et de passer à l'onglet *Fonctionnalités* pour lancer la personnalisation. Par défaut, la personnalisation s'applique à chaque document du dossier que vous avez sélectionné.

L'onglet *Fonctionnalités* répertorie toutes les fonctionnalités que vous pouvez activer ou désactiver. Utilisez les cases à cocher dédiées pour les activer ou les désactiver.

18.6.1.1.2 Règles de personnalisation

Les règles suivantes servent à définir les personnalisations à appliquer à un utilisateur :

- Si l'utilisateur appartient à différents groupes, seule la personnalisation définie sur le groupe dont l'ID est inférieur s'applique. La personnalisation définie pour les autres groupes contenant l'utilisateur ne s'applique pas.
- Dans le cas d'une structure de dossiers imbriquée, le dossier parent immédiat du document ajouté à la liste des dossiers personnalisés définit les personnalisations concernant les éléments d'interface utilisateur, fonctionnalités et extensions.
- La personnalisation définie pour Dossiers par défaut s'applique aux documents stockés dans Dossiers personnels et Boîtes de réception ainsi qu'aux documents pour lesquels le dossier parent n'est pas personnalisé.
- La personnalisation définie pour les éléments d'interface utilisateur a priorité sur la personnalisation définie pour les fonctionnalités car celles-ci ne sont qu'un raccourci pour activer tous les éléments d'interface utilisateur.
- Scénario : Lorsque les éléments de personnalisation sont affichés sous forme d'arborescence et que vous désactivez un nœud dans un système. Ici, si vous effectuez une montée de version de ce système avec une version plus récente du produit ayant de nouveaux éléments dans les nœuds, ces éléments sont activés par défaut même si le nœud supérieur est désactivé.

18.6.1.1.3 Pour personnaliser l'apparence de l'interface Web Intelligence

Vous pouvez personnaliser l'apparence de l'interface utilisateur de Web Intelligence en masquant des éléments, des sous-éléments et des fonctionnalités de menu pour un groupe d'utilisateurs sélectionné.

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Dans la liste *Organiser*, sélectionnez *Utilisateurs et groupes*.
3. Dans la liste *Hiérarchie de groupe*, sélectionnez un groupe d'utilisateurs.
4. Dans la liste *Actions*, sélectionnez *Personnalisation*.
5. Dans la section *Dossiers personnalisés*, effectuez l'une des opérations suivantes :

Option	Description
Pour définir une personnalisation par défaut	1. Sélectionnez *Dossiers par défaut* dans la zone *Dossiers personnalisés*.
Pour ajouter des dossiers de documents pour lesquels vous souhaitez appliquer la personnalisation pour les groupes d'utilisateurs sélectionnés	1. Cliquez sur *Ajouter un dossier*. 2. Sélectionnez les dossiers. Les dossiers sont affichés dans la zone *Dossiers personnalisés*.
Pour éviter de redéfinir la même personnalisation pour d'autres dossiers	1. Dans la zone des *Dossiers personnalisés*, sélectionnez le dossier à partir duquel vous souhaitez copier la personnalisation.

Option	Description
	2. Dans la liste déroulante, cliquez sur *Copier la personnalisation*. 3. Sélectionnez le dossier pour lequel vous souhaitez définir la personnalisation. 4. Cliquez sur *Coller la personnalisation*. 5. Passez à l'étape 7.
Pour supprimer la personnalisation pour un dossier spécifique	1. Dans la zone *Dossiers personnalisés*, sélectionnez le dossier. 2. Dans la liste déroulante, cliquez sur *Supprimer le dossier*. 3. Passez à l'étape 7. **Remarque** Vous ne pouvez pas supprimer les *dossiers par défaut*.

6. Sélectionnez ou désélectionnez des éléments dans l'onglet *Fonctionnalités* pour les afficher ou les masquer dans Web Intelligence.

   Si vous désélectionnez tous les enfants d'un élément parent, l'élément parent est également désélectionné et masqué dans Web Intelligence. Pour en savoir plus, consultez Personnalisation des éléments d'interface Web Intelligence par groupe d'utilisateurs ou dossiers [page 792].
7. Cliquez sur *Enregistrer et fermer*.

Une fois que vous enregistrez la personnalisation, tous les utilisateurs du groupe sélectionné verront ces modifications la prochaine fois qu'ils se connecteront à la zone de lancement BI et ouvriront Web Intelligence.

> **Remarque**
>
> Il est conseillé de vous connecter à la zone de lancement BI en tant qu'utilisateur du groupe que vous venez de personnaliser, de lancer Web Intelligence et de vérifier si l'interface correspond à vos paramètres de personnalisation.

18.6.1.2 Alignement de contenu Web Intelligence

Choisir la façon dont le contenu de document sera aligné (de gauche à droite ou de droite à gauche) lorsque les utilisateurs créeront des documents Web Intelligence.

En ce qui concerne l'interface Rich Client, l'alignement de contenu est déterminé par les paramètres régionaux définis dans les préférences de la zone de lancement BI :

- Le système utilise un alignement de droite à gauche uniquement lorsque les paramètres régionaux de visualisation préférés et paramètres régionaux de produit sont définis sur des langues de droite à gauche.
- Dans d'autres cas, l'alignement de contenu est de gauche à droite.

> **Remarque**
>
> Pour en savoir plus sur la définition des paramètres régionaux, voir le *Guide de l'utilisateur de la zone de lancement BI*.

> **Remarque**
>
> L'alignement de contenu s'applique uniquement à la création de documents et n'affecte pas les documents existants.

18.6.1.3 Activation des points d'extension d'interface utilisateur Web Intelligence pour des groupes d'utilisateurs spécifiques

Vous pouvez configurer les droits Web Intelligence de manière à permettre à des groupes d'utilisateurs sélectionnés d'accéder à des extensions d'interface personnalisées. Reportez-vous au guide *SAP BusinessObjects BI Developer's Guide for Web Intelligence and the BI Semantic Layer* pour en savoir plus sur les groupes d'extensions et les appels d'API des services Web REST disponibles.

18.6.1.3.1 Pour activer les points d'extension de l'interface utilisateur Web Intelligence

- Vous avez créé et déployé l'extension appropriée dans votre installation. Déployez une extension pour chaque fonctionnalité d'extension (par exemple, bouton Personnalisé ou Enregistrer au format HTML).
- Vous avez ajouté l'extension à la liste des URL approuvées. Si ce n'est pas le cas, consultez la section Ajout d'URL approuvées à la liste des URL autorisées [page 733].

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Dans la liste *Organiser*, sélectionnez *Utilisateurs et groupes*.
3. Dans la liste *Hiérarchie de groupe*, sélectionnez un groupe d'utilisateurs.
4. Dans la liste *Actions*, sélectionnez *Personnalisation*
5. Cliquez sur l'onglet *Extensions* et effectuez une des opérations suivantes :

Option	Description
Pour ajouter une extension OSGI déployée sur la plateforme de BI et son serveur d'applications	Sélectionnez les extensions personnalisées que vous souhaitez voir utilisées par vos utilisateurs.
Pour ajouter une extension non OSGI déployée sur le serveur d'applications de la plateforme de BI ou un serveur d'applications externe	1. Cliquez sur *Ajouter*. 2. Saisissez l'URL d'extension. Il s'agit de l'URL du fichier JSON. **Remarque** Remplacez les espaces vides de l'URL par **%20**.

Option	Description

	Exemples :
	• Serveur d'applications Apache Tomcat :
	`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`
	• Serveurs d'applications externe :
	`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`
	3. Sélectionnez *Définir les informations du proxy si nécessaire* par votre serveur d'applications et saisissez le nom du serveur et le numéro du port.
	4. Sélectionnez soit *Aucune authentification* soit *Authentification de base* si requis par votre serveur d'applications et saisissez le nom d'utilisateur et le mot de passe.
	5. Cliquez sur *OK* et sélectionnez l'extension
	6. Cliquez sur *Enregistrer*.

Pour modifier les informations d'une extension	Cliquez sur *Modifier*.
Pour supprimer une extension de la CMC	Cliquez sur *Supprimer*.

6. Cliquez sur *Enregistrer et fermer*.

Les extensions activées sont accessibles au groupe d'utilisateurs sélectionné lors de l'ouverture d'un document situé dans le dossier sélectionné. Les points d'extension sont disponibles pour tous les clients d'application Web Intelligence : Web, applet Java et Rich Client.

18.6.2 Zone de lancement BI

18.6.2.1 Activer le nettoyage des valeurs d'invites dans la boîte de dialogue Planifier

Lors de la planification d'un document Web Intelligence basé sur une requête BEx contenant des invites SAP BW, les utilisateurs de la zone de lancement BI peuvent effacer une valeur d'invite afin qu'elle soit obtenue par la variable de la source de données SAP BW lors de l'exécution du document ou la corriger avant l'exécution du travail de planification.

La procédure ci-dessous permet d'afficher deux cases d'option dans l'interface utilisateur :

- *Utiliser la valeur dynamique* : laissez le processus de source de données SAP BW traiter la valeur.
- *Utiliser la valeur constante* : saisissez une valeur fixe.

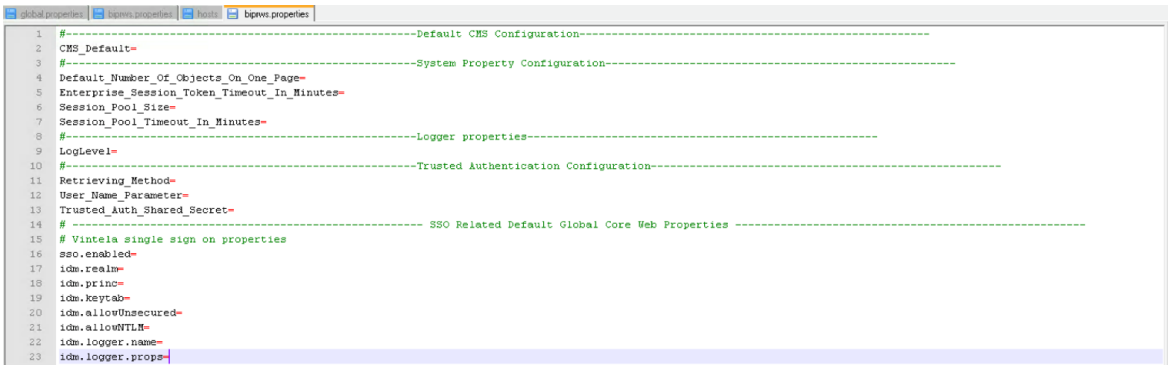
1. Exécutez l'une des actions suivantes dans le dossier `<RepInstall>\<ServeurAppWeb>\webapps\BOE\WEB-INF\config\custom` :
   - Si un fichier `AnalyticalReporting.properties` se trouve dans le dossier, ouvrez le fichier dans un éditeur de texte.
   - Si aucun fichier `AnalyticalReporting.properties` n'existe dans le dossier, créez un fichier avec ce nom de fichier et ouvrez-le dans un éditeur de texte.

2. Exécutez l'une des actions suivantes dans le fichier `AnalyticalReporting.properties` :
   - Si le fichier existe déjà, localisez l'emplacement de la propriété `bex.dynamic_variable.schedule` dans le fichier et assurez-vous que sa valeur est définie sur `true`.
   - Si vous avez créé le fichier `AnalyticalReporting.properties`, ajoutez `bex.dynamic_variable.schedule=true` à la fin du fichier.
3. Enregistrez et fermez le fichier, puis redémarrez le serveur d'applications Web.

18.7 Configuration des services Web RESTful de la plateforme de BI sur le serveur Web

Pour personnaliser la configuration des services Web RESTful, suivez les étapes ci-dessous :

1. Copiez le fichier : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\default\biprws.properties` vers `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` et ouvrez-le pour le modifier.
   Modifiez les paramètres selon vos besoins.



   Vous trouverez ci-dessous un tableau décrivant les propriétés indiquées dans la capture d'écran.

Propriété	Description	Valeur par défaut

`CMS_Default`	L'utilisateur peut fournir le nom du CMS et son numéro de port ou le nom du cluster.
	Exemple :
	`CMS_HOST_NAME:CMS_PORT_NUMBER`
	Ou
	`@CMS_CLUSTER_NAME`
		0

Propriété	Description	Valeur par défaut
`Default_Number_Of _Objects_On _One_Page`	Le nombre d'entrées qui seront répertoriées par page. Vous pouvez remplacer ce paramètre par `&pageSize=<m>` dans le SDK des services Web RESTful.	50
`Enterprise_Session_ Token_Timeout_In_Minutes)`	Le délai d'expiration de validité d'un jeton de connexion. Une fois ce délai passé, vous devez générer un nouveau jeton de connexion.	60
`Session_Pool_Size`	Le nombre de sessions en mémoire cache qui peuvent être stockées à un moment donné. Le groupe de sessions place en mémoire cache les sessions du service Web RESTful afin qu'elles puissent être réutilisées lorsqu'un utilisateur envoie une autre requête qui utilise le même jeton de connexion dans l'en-tête HTTP de la requête.	1000
`Session_Pool_Timeout_In_M inutes`	Le délai, en minutes, à partir duquel les sessions en mémoire cache expirent.	2
`LogLevel`	Permet la connexion et définit le niveau de gravité et de détail sur *Aucun* (uniquement les événements essentiels journalisés), *Faible* (démarrage, fermeture, messages de requête de début et de fin), *Moyen* (messages d'erreur, d'avertissement et la plupart des messages d'état) ou *Élevé* (Rien d'exclus). À des fins de débogage uniquement. Augmentation possible de la consommation de l'unité centrale, affectant sa performance). Les choix de menu disponibles sont : • `Unspecified` • `None` • `Low` • `Medium` • `High`	Non spécifié

Propriété	Description	Valeur par défaut
Log_Location	L'emplacement du fichier journal qui enregistre les journaux d'utilisation de l'ordinateur où la plateforme de BI est hébergée. **Remarque** • Un nouveau dossier est créé si vous indiquez le chemin d'accès à un dossier qui n'existe pas. • L'emplacement du fichier journal est défini sur l'emplacement par défaut si aucun emplacement n'est spécifié dans le fichier biprws.properties.	Non spécifié
`Retrieving_Method`	Le menu qui spécifie la méthode de requête qui doit être utilisée pour extraire les jetons de connexion à l'authentification sécurisée lors de l'utilisation de l'API du service Web RESTful /logon/trusted. • `HTTP_HEADER` est utilisé pour les requêtes GET avec l'entête de requête accept=application/xml (ou application/json). • `QUERY_STRING` est utilisé pour ajouter un nom de connexion à la fin d'une requête URL à l'aide de l'API du service Web RESTful, par exemple /logon/trusted/?user=johndoe. • `COOKIE` est utilisé lorsque le nom de connexion est extrait d'un cookie d'un navigateur Web. Le domaine, le nom, la valeur et le chemin doivent être stockés dans le cookie.	`HTTP_HEADER`
`User_Name_Parameter`	L'étiquette utilisée pour identifier l'utilisateur sécurisé pour extraire un jeton de connexion.	`X-SAP-TRUSTEDUSER`

Propriété	Description	Valeur par défaut
`Trusted_Auth_Shared_Secret`	La valeur de chaîne générée en suivant les étapes mentionnées dans la sectionGénération de la valeur d'un secret partagé [page 417].	Non spécifié
`Basic_Auth_Supported`	Active l'authentification de base sur le serveur Web Tomcat. Les valeurs possibles sont : `True` ou `False`.	Non spécifié
`Basic_Auth_Type`	Définit l'authentification sur `secEnterprise`, `secLDAP`, `secSAPR3` ou `secWinAD` pour une prise en charge de l'authentification de base.	`secEnterprise`

2. Redémarrez Tomcat.

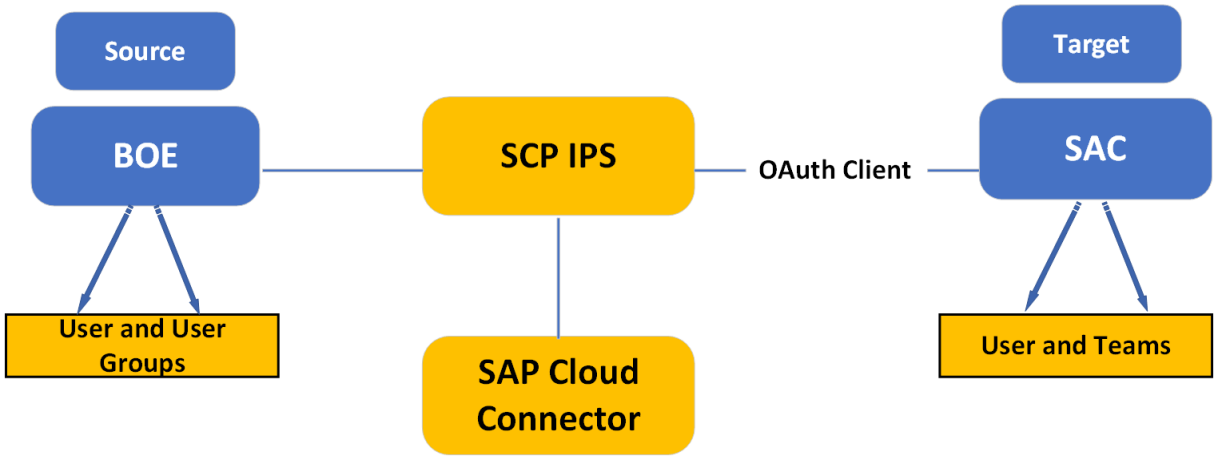
18.8 Gestion hybride des utilisateurs

À l'heure actuelle, SAP suit une stratégie privilégiant le Cloud ("Cloud First"), et les clients aussi se tournent davantage vers des solutions hybrides leur permettant de gérer les actifs entre l'environnement sur site et le Cloud. Il est donc impératif que dans la plateforme SAP BusinessObjects BI Platform, nous fournissions des services offrant cette possibilité.

Pour ce faire, nous exposons des API de mise en service des utilisateurs basées sur SCIM (System for Cross-Domain Identity Management) (en interne), qui peuvent être utilisées par le service SAP Cloud Platform Identity Provisioning (SCP IPS) pour mettre en service les utilisateurs Enterprise de la plateforme de BI dans tout autre système SCIM à l'aide d'Identity Provisioning Service (IPS) (notamment SAP Analytics Cloud).

À l'aide de SCP IPS et de la plateforme SAP BusinessObjects BI 4.2 SP06 ou version supérieure, les utilisateurs Enterprise de la plateforme de BI peuvent désormais être mis en service dans tout système SCIM cible pris en charge.

L'illustration suivante décrit le scénario hybride et explique comment activer les services entre l'environnement sur site et le Cloud.



18.9 Mise en service de vos utilisateurs sur site dans SAP Analytics Cloud

Afin de mettre en service des entités (utilisateurs, groupes, rôles) d'un système à un autre dans votre entreprise, vous devez au préalable ajouter et configurer ces systèmes comme systèmes source et cible dans l'interface utilisateur Identity Provisioning.

Vous pouvez mettre en service vos utilisateurs (BOE) sur site dans SAP Analytics Cloud via le service SAP Cloud Platform Identity Provisioning Service (SCP IPS) en quelques étapes simples.

1. Établissement de la connexion entre le système sur site et le Cloud
2. Création de références de connexion au client OAuth dans SAP Analytics Cloud
3. Configuration du système source
4. Configuration du système cible
5. Mise en service de vos utilisateurs et groupes d'utilisateurs pour SAP Analytics Cloud
6. Visualisation des utilisateurs et groupes d'utilisateurs mis en service

18.9.1 Établissement de la connexion entre le système sur site et le Cloud

Vous pouvez établir une connexion entre le système sur site et le Cloud (Identity Provisioning System) à l'aide du connecteur SAP Cloud (Système IPS).

Le connecteur Cloud est installé.

1. Lancez la page d'administration du connecteur SAP Cloud et connectez-vous sur : `https://<HCC HOST>:8443`.

   > **Remarque**
   >
   > Remplacez `<HCC HOST>` par le nom d'hôte du système dans lequel le connecteur Cloud est installé.

2.
3. Dans le panneau de navigation, sélectionnez *Connecteur*, puis cliquez sur l'icône + (*Ajouter un sous-compte*).

   La boîte de dialogue *Ajouter un sous-compte* apparaît.
4. Saisissez les informations suivantes pour votre compte IPS :

   > **Remarque**
   >
   > L'autorisation *Gestion des connexions sur site* est requise pour l'utilisateur du sous-compte dans IPS. L'*Hôte de la région* et le *Nom du sous-compte* sont disponibles dans la section *Support - Informations sur le compte* dans IPS.

   a. *Hôte de la région* : sélectionnez l'hôte de votre région dans la liste.
   b. *Nom du sous-compte* : ajoutez le nom de votre compte. Par exemple, dd00bb33.
   c. (Facultatif) *Nom d'affichage* : ajoutez un nom pour le compte.
   d. *Utilisateur du sous-compte* : ajoutez le nom d'utilisateur (S-User) de votre sous-compte.
   e. *Mot de passe* : ajoutez le mot de passe pour votre S-User.
   f. *ID de l'emplacement* : Laissez cette zone vide pour utiliser l'emplacement par défaut.
   g. (Facultatif) *Description* : ajoutez une description du connecteur Cloud.
5. Cliquez sur *Enregistrer*.
6. Dans le panneau de navigation, sous *Nom d'affichage*, sélectionnez *Cloud > Sur site*.

   Nom d'affichage est le nom du client du connecteur Cloud.
7. Sous l'onglet *Contrôle d'accès*, cliquez sur l'icône + (Ajouter).

   La boîte de dialogue *Modifier le mappage de système* apparaît.
8. Ajoutez les informations de mappage de système demandées pour votre système de plateforme de BI, le serveur d'applications Web (par exemple, Tomcat) hébergeant des biprws :
   a. *Type de backend* : sélectionnez Autre système SAP dans la liste déroulante.
   b. *Protocole* : sélectionnez HTTP dans la liste déroulante.
   c. (Facultatif) *Hôte virtuel* : l'hôte virtuel et le port par défaut correspondent à l'hôte et au port internes. Vous pouvez renommer l'hôte et le port pour éviter d'exposer le nom d'hôte et le port internes.
   d. (Facultatif) *Port virtuel* : il s'agit du numéro de port utilisé par l'hôte virtuel.
   e. *Hôte interne* : Il s'agit du nom d'hôte du serveur d'application Web (par exemple, Tomcat) qui héberge le service Web Restful (biprws).
   f. *Port interne* : il s'agit du numéro de port utilisé par l'hôte interne (port dans lequel les services Web RESTful de la plateforme de BI sont déployés, par exemple, biprws).
   g. *SAProuter* : laissez ce champ vide.
   h. *Type principal* : sélectionnez l'option Aucun dans la liste déroulante.
   i. *Nom du partenaire SNC* : laissez ce champ vide.
   j. (Facultatif) *Description* : ajoutez une description du système.
9. Cochez la case *Vérifier l'hôte interne*, puis cliquez sur *Enregistrer*.
10. Sélectionnez le système que vous avez ajouté à la liste *Mappage virtuel au système interne*.
11. Dans la zone *Ressources accessibles*, cliquez sur l'icône + (Ajouter).

    La boîte de dialogue *Ajouter une ressource* apparaît.
12. Ajoutez les informations suivantes concernant la ressource pour votre compte :

a. *Chemin URL* : /biprws/sbop/internal/v2/scim.
b. *Activé* : assurez-vous que la case est cochée.
c. *Méthode d'accès* : cochez la case d'option *Chemin et tous les sous-chemins*.
d. (Facultatif) *Description* : ajoutez une description de votre ressource.

13. Cliquez sur *Enregistrer*.

> **Remarque**
>
> L'état en regard de l'hôte virtuel doit apparaître en vert.

18.10 Création des références de connexion du client OAuth dans SAP Analytics Cloud

Pour créer les références de connexion du client OAuth dans SAP Analytics Cloud, suivez les étapes indiquées ci-dessous :

1. Connectez-vous à SAP Analytics Cloud.
2. Dans le menu principal, accédez à *Système > Administration > Intégration de l'application*.
3. Cliquez sur *Nouveau client OAuth*.
4. Choisissez-lui un nom.
5. Sélectionnez *Accès aux API* comme *Objectif*.
6. Sélectionnez *Attribution de privilèges d'accès aux utilisateurs* sous Accès.
7. Cliquez sur *Ajouter*.

   Dans cette liste de *Clients configurés*, sélectionnez le client que vous venez d'ajouter.

> **Remarque**
>
> Cliquez sur l'icône ✎ (Modifier) pour afficher l'ID et la clé secrète (mot de passe) du client OAuth généré. Ces références de connexion sont nécessaires lors de la configuration du système cible.
>
> L'ID du client OAuth correspond à votre nom d'utilisateur figurant dans les détails de configuration du système cible dans SCP IPS, et la clé secrète correspond à votre mot de passe.

18.11 Configuration du système source

Vous devez configurer les détails du système source à partir duquel vous souhaitez mettre en service des utilisateurs et groupes d'utilisateurs dans le service SAP Cloud Platform Identity Provisioning (SCP IPS).

1. Connectez-vous à SCP IPS.
2. Depuis la page d'accueil, sélectionnez la vignette *Systèmes source*.
3. Cliquez sur l'icône + (Ajouter) située en bas du panneau de gauche.

4. Dans la zone de liste déroulante *Type*, sélectionnez le type de système que vous souhaitez utiliser.
5. Ajoutez un nom pour votre système. (Veillez à ne pas créer un doublon en inscrivant le nom d'un autre système).
6. (Facultatif) Saisissez une description pour votre système pour pouvoir le distinguer facilement dans la liste par la suite.
7. Cliquez sur *Enregistrer*.

   Le nouveau système apparaît dans le panneau latéral gauche.

   Mise en garde : Si vous n'enregistrez pas votre système à ce stade, les transformations et propriétés par défaut ne s'afficheront pas.
8. Cliquez à présent sur l'icône ✎ (Modifier) pour voir les transformations et ajouter des propriétés de configuration.
9. Ajoutez les informations suivantes :
   a. *Authentification* : AuthentificationBase.
   b. *Hôte* : <nom d'hôte et port BOE>.
   c. *ips.delta.read* : activé.
   d. *ips.full.read.force.count* : 2.
   e. *Ips.trace.failed.entity.content* : vrai.
   f. *Mot de passe* : <mot de passe de l'utilisateur administrateur BOE>.
   g. *Type de proxy* : sur site.
   h. *scim.group.filter* : <ID de groupe d'utilisateurs ou CUID>.

      Par exemple, `scim.group.filter: groupId eq "4214"`.
   i. *scim.user.filter* : <ID utilisateur ou CUID>.

      Par exemple, `scim.filter.filter: userId in "8077"` ou `scim.user.filter: userCuid in "AQ.rQ1V1FR9JmQoQa0xYfII"`.
   j. *Type* : HTTP.
   k. *URL* : http://nom d'hôte : port/biprws/sbop/internal/v2/scim.
   l. *Utilisateur* : administrateur.

   > **Remarque**
   > - Vous pouvez fournir les détails concernant le système sur site à partir de zéro ou en important un fichier existant avec les informations de configuration.
   > - Vous pouvez définir certaines restrictions ou conditions autour du système source via des transformations.
   > - Lorsque vous sélectionnez une destination de connectivité, elle doit être conforme au type de système correspondant. La destination doit spécifier tous les paramètres de connexion requis pour votre scénario de mise en service d'identités.
   > - Le nom d'hôte/port indiqué dans le champ URL doit correspondre au nom d'hôte/port virtuel indiqué dans le connecteur Cloud.
10. Si vous ignorez le champ *Nom de destination*, vous pouvez ouvrir l'onglet *Propriétés* pour saisir toutes les propriétés de connexion et de configuration requises pour votre scénario de mise en service.
11. Vous pouvez modifier votre transformation système par défaut (si nécessaire).
12. Enregistrez vos modifications.

> **Remarque**
>
> À la fin de l'URL Identity Provisioning, une chaîne séparée par des tirets apparaît. Il s'agit de l'ID unique généré automatiquement pour le système nouvellement créé.

18.12 Configuration du système cible

Avant de commencer, assurez-vous d'avoir créé les références de connexion du client OAuth dans SAP Analytics Cloud.

1. Cliquez sur l'onglet *Système cible* sur la page d'accueil.
2. Dans l'onglet *Détails*, saisissez le nom du système SAP Analytics Cloud, l'URL SAP Analytics Cloud et le ou les systèmes source.

   > **Remarque**
   >
   > Les systèmes sources déjà configurés apparaissent ici par défaut.

3. Cliquez sur l'onglet *Propriétés*.
4. Ajoutez les informations suivantes :
   a. *Authentification* : AuthentificationBase.
   b. *csrf.token.path* : api/v1/scim/Users?count=1.
   c. *ips.trace.failed.entity.content* : True.
   d. *URL OAuth2TokenService* : <URLJetonClientOAuth>.
   e. *Mot de passe* : <Clé secrète générée lors de la configuration du client OAuth>.
   f. *Type de proxy* : Internet.
   g. *scim.api.csrf.protection* : activé.
   h. *Type* : HTTP.
   i. *URL* : URL SAP Analytics Cloud.
   j. *Utilisateur* : <ID du Client OAuth>.

18.13 Mise en service de vos utilisateurs et groupes d'utilisateurs pour SAP Analytics Cloud

Une fois que vous avez configuré les systèmes source et cible à l'aide du service SAP Cloud Platform Identity Provisioning, vous pouvez les mettre en service depuis l'onglet *Travaux* dans la fenêtre *Détails du système source*.

Les adresses e-mail des utilisateurs de la plateforme de BI qui seront mis en service doivent être configurées.

1. Cliquez sur la vignette *Système source*.
2. Cliquez sur *Travaux*.

3. Sous *Travaux*, pour *Type de travail* : *travail de lecture*, sélectionnez l'action *Exécuter maintenant*.

> **Remarque**
>
> Si vous avez modifié les utilisateurs ou groupes d'utilisateurs dans BOE, sélectionnez *Travail de resynchronisation* pour vous assurer que les modifications sont mises à jour dans SAP Analytics Cloud.

4. Pour afficher l'avancement, sélectionnez *Journaux des travaux* dans le panneau de gauche et affichez le *Statut* des travaux déclenchés.
5. Pour afficher les détails d'exécution du travail, cliquez sur la ligne correspondante.

   La fenêtre *Détails d'exécution du travail* s'ouvre avec le statut des actions.

18.14 Visualisation d'utilisateurs mis en service dans SAP Analytics Cloud

1. Accédez au menu principal > *Sécurité* > *Équipes*.
2. Allez à la page *Équipes*.
3. Sélectionnez votre groupe d'utilisateurs BOE.
4. Cliquez sur *Membres de l'équipe* pour afficher la liste des utilisateurs qui ont été mis en service dans SAP Analytics Cloud à partir de BOE.

> **Remarque**
>
> Vous pouvez également visualiser la liste des utilisateurs dans le menu *Utilisateurs* sous *Sécurité*.

18.15 Modèles d'exemple

Vous pouvez utiliser les modèles suivants pour mettre en service un utilisateur, ou encore un ou plusieurs groupes d'utilisateurs.

Exemple de configuration du système source

```
{ "connectorTypeString": "SCIM", "accessMode": "READ",
"alias": "SBOP_10.47.228.194",
"relatedSystems": [
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SBOP_43",
"state": "ENABLED",
"transformation": {
"user": {
```

```
"condition": "($.memberOf contains '7741') || ($.memberOf contains '7962') ||
($.id contains '8077') || ($.id contains '8081')",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
},
"group": {
"condition": "$.id contains '7741' || $.id contains '7962'",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "Administrator",
"ips.full.read.force.count": "2",
"Authentication": "BasicAuthentication",
"host": "adept6991435:6400",
"scim.group.filter": "groupId eq \"7741,7962\" or groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\"",
"ProxyType": "OnPremise",
"ips.delta.read": "enabled",
"ips.trace.failed.entity.content": "true",
"URL": "http://adept6991435:6405/biprws/sbop/internal/v2/scim",
"Password": "Password1",
"scim.user.filter": "groupId eq \"7741\" and groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\" and userId in \"8077\" or
userCuid in \"AQ.rQ1V1FR9JmQoQa0xYfII\""
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

Exemple de transformation

```
{
"connectorTypeString": "SAP_ANALYTICS_CLOUD",
"accessMode": "WRITE",
"destinationName": " ",
"alias": "https://idcsac.jp1.sapanalytics.cloud",
"relatedSystems": [
"SBOP_43"
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SAC-Machine",
"state": "ENABLED",
"transformation": {
"user": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"sourceVariable": "entityIdTargetSystem",
"targetPath": "$.id"
},
{
"sourcePath": "$.userName",
"targetPath": "$.userName"
},
{
"sourcePath": "$.name",
"targetPath": "$.name"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.active",
"optional": true,
"targetPath": "$.active"
},
{
"sourcePath": "$.emails",
"preserveArrayWithSingleElement": true,
"targetPath": "$.emails"
},
{
"condition": "$.emails[0].length() > 0",
"constant": true,
"targetPath": "$.emails[0].primary"
},
{
"constant": [
"PROFILE:sap.epm:BI_Admin"
],
"preserveArrayWithSingleElement": true,
"targetPath": "$.roles"
},
{
```

```
"sourcePath": "$.groups",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.groups"
},
{
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
"optional": true,
"targetPath": "$['urn:scim:schemas:extension:enterprise:1.0']['manager']
['managerId']",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
},
"group": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"condition": "$.displayName EMPTY false",
"sourcePath": "$.displayName",
"targetPath": "$.id"
},
{
"condition": "$.id EMPTY false",
"sourcePath": "$.id",
"targetPath": "$.id"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.roles",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.members[*].value",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.members[?(@.value)]",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "<exampleusername>",
"Authentication": "BasicAuthentication",
"OAuth2TokenServiceURL": "https://oauthasservices-
gf097393f.jp1.hana.ondemand.com/oauth2/api/v1/token",
```

```
"csrf.token.path": "/api/v1/scim/Users?count=1",
"ProxyType": "Internet",
"ips.trace.failed.entity.content": "true",
"URL": "https://idcsac.jp1.sapanalytics.cloud",
"scim.api.csrf.protection": "enabled",
"Password": "<examplepassword>"
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

19 Gestion des connexions et des univers

19.1 Gestion des connexions

Une connexion est un ensemble nommé de paramètres qui définit comment une ou plusieurs applications SAP BusinessObjects peuvent accéder aux bases de données relationnelle ou OLAP. Les détails de connexion, tels que le nom du serveur, la base de données, le nom d'utilisateur et le mot de passe, peuvent être stockés de manière sécurisée dans le dossier Connexions du référentiel de la plateforme de BI.

Les concepteurs définissent des univers basés sur des connexions. Les utilisateurs d'applications de requête, analyse et reporting accèdent à la base de données via l'univers sans avoir à connaître les structures de données sous-jacentes de la base de données.

Vous pouvez créer des connexions à l'aide des applications suivantes :

- Outil de conception d'univers : les connexions sont stockées dans le référentiel.
- Outil de conception d'information : les connexions peuvent être créées localement, puis publiées dans le référentiel, ou créées et modifiées directement dans le référentiel.

> ⓘ Remarque
>
> Pour en savoir plus sur la gestion des connexions aux sources de données OLAP, voir le *Guide d'administration de SAP BusinessObjects Analysis, édition pour OLAP*.

Vous pouvez accorder aux utilisateurs le droit de créer, modifier et supprimer des connexions.

Vous pouvez accorder aux utilisateurs l'accès aux connexions d'univers et le droit de créer et d'afficher des documents qui utilisent des univers et des connexions.

Informations associées

Gestion des paramètres de sécurité des objets dans la CMC [page 137]
Droits de connexion [page 1166]

19.1.1 Pour supprimer une connexion d'univers

> → Conseil
>
> Il est également possible de supprimer des connexions dans l'outil de conception d'univers et l'outil de conception d'information.

1. Dans la zone *Connexions*, sélectionnez une connexion d'univers dans la liste.

2. Cliquez sur *Gérer* > *Supprimer*.

19.2 Gestion des univers

Un univers est un ensemble organisé d'objets de métadonnées permettant aux utilisateurs d'analyser les données d'entreprise et de les consigner dans des rapports dans un langage non technique. Ces objets incluent les dimensions, indicateurs, hiérarchies, attributs, calculs prédéfinis, fonctions et requêtes. La couche d'objets de métadonnées repose sur un schéma de base de données relationnelle ou sur un cube OLAP, de sorte que les objets sont directement mappés aux structures de base de données. Un univers inclut des connexions aux sources de données. Ainsi, les utilisateurs d'outils de requête et d'analyse peuvent se connecter à un univers, exécuter des requêtes et créer des rapports en utilisant les objets de l'univers sans avoir à connaître les structures de données sous-jacentes de la base de données.

Vous pouvez créer des univers à l'aide des outils suivants :

- L'outil de conception d'univers. Les univers créés à l'aide de cet outil peuvent être différenciés par l'extension .unv et sont donc appelés univers .unv. Les univers .unv sont définis sur une connexion sécurisée et stockés dans le dossier Univers du référentiel.
- L'outil de conception d'information. Les univers créés à l'aide de cet outil sont basés sur la nouvelle couche sémantique. Ils sont différenciés par l'extension .unx et sont donc appelés univers .unx. Les univers .unx sont créés localement et publiés dans le dossier Univers du référentiel. Les concepteurs peuvent définir une sécurité au niveau de l'objet à l'aide de l'éditeur de sécurité de l'outil de conception d'information.

Vous pouvez accorder aux utilisateurs des droits d'application et des droits d'univers pour leur permettre de créer, de modifier et de supprimer des univers, ainsi que de créer une sécurité sur les univers.

Vous pouvez accorder aux utilisateurs des droits d'univers pour leur permettre de créer et d'afficher des documents qui utilisent des univers.

Informations associées

Gestion des paramètres de sécurité des objets dans la CMC [page 137]
Outil de conception d'univers [page 1171]
Droits d'univers (.unv) [page 1162]
Outil de conception d'information [page 1172]
Droits d'univers (.unx) [page 1164]

19.2.1 Pour supprimer des univers

> → Conseil
>
> Il est également possible de supprimer des univers dans l'outil de conception d'information..

1. Dans la zone *Univers* de la CMC, sélectionnez un univers dans la liste.
2. Cliquez sur *Gérer* > *Supprimer* >.
3. Lorsque le système vous invite à confirmer votre choix, cliquez sur *OK*.

20 Studio d'administration BI

Studio d'administration BI est une application de la CMC qui combine la surveillance, les alertes et le Cockpit d'administration, auparavant nommé Cockpit de l'administrateur BI.

L'application se compose de deux onglets *Tableau de bord* et *Applications*.

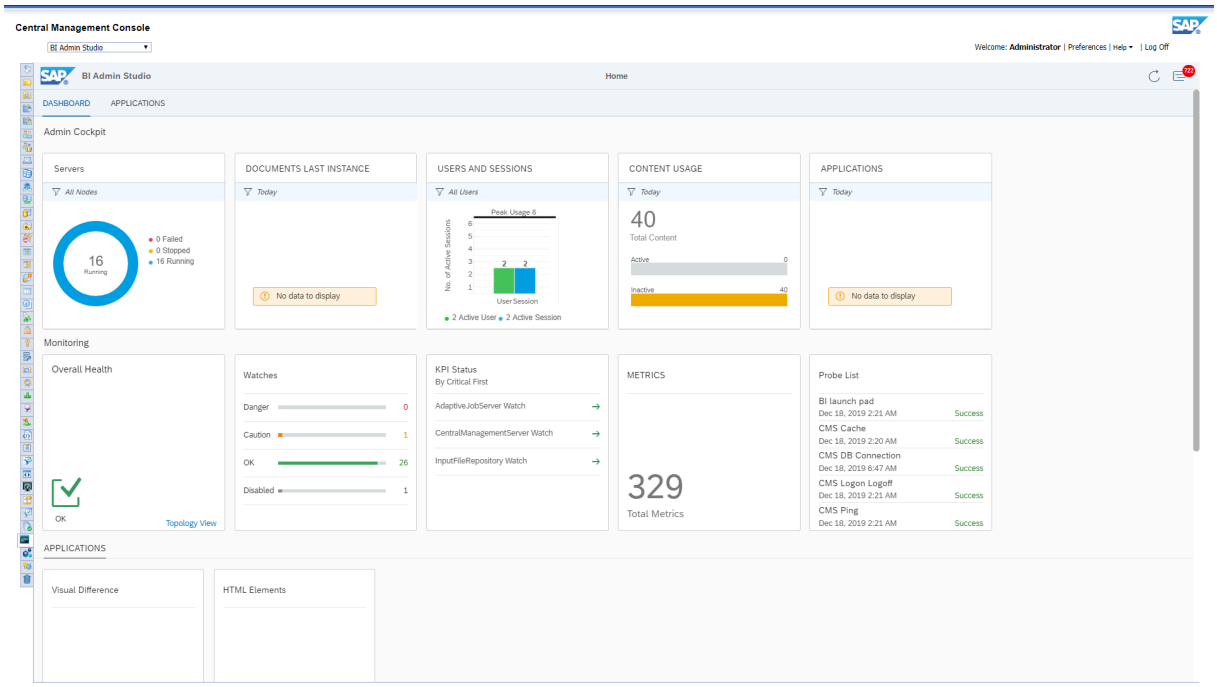


Tableau de bord

L'onglet *Tableau de bord* fournit une vue unique des tableaux de bord disponibles dans *Cockpit d'administration* et *Surveillance*. Vous pouvez cliquer sur chaque tableau de bord pour obtenir des informations détaillées. Par exemple, vous pouvez sélectionner le tableau de bord *Serveurs* pour obtenir la liste des serveurs avec un *Statut En cours d'exécution*, *Arrêté* et *Échec*, ainsi que les détails tels que *Nom du serveur*, *PID* et *Type*. Pour plus d'informations sur le Cockpit d'administration, voir Cockpit d'administration [page 817], et pour en savoir plus sur la surveillance, voir Surveillance [page 821].

Applications

Vous pouvez accéder à *Différence visuelle* et à *Éléments HTML autorisés* depuis l'onglet *Applications*. Pour en savoir plus sur la *Différence visuelle*, voir Différence visuelle [page 846], et pour en savoir plus sur les *Éléments HTML*, voir Autorisation des éléments HTML [page 848].

Alertes

Vous pouvez sélectionner pour accéder au volet de notification relatif aux alertes. Depuis le volet de notification, vous pouvez sélectionner l'option *Vers la page des alertes* pour en savoir plus sur les alertes que vous avez créées.

20.1 Cockpit d'administration

Le Cockpit d'administration BI est une nouvelle application ajoutée à la CMC. Elle permet à l'administrateur de recueillir des données concernant l'environnement BI. Cela signifie dériver les informations décisionnelles (business intelligence) au sein des données vers votre environnement d'informations décisionnelles. Vous pouvez obtenir des informations sur les serveurs, les travaux planifiés, les utilisateurs et les sessions, l'utilisation du contenu et les applications grâce au Cockpit d'administration BI.

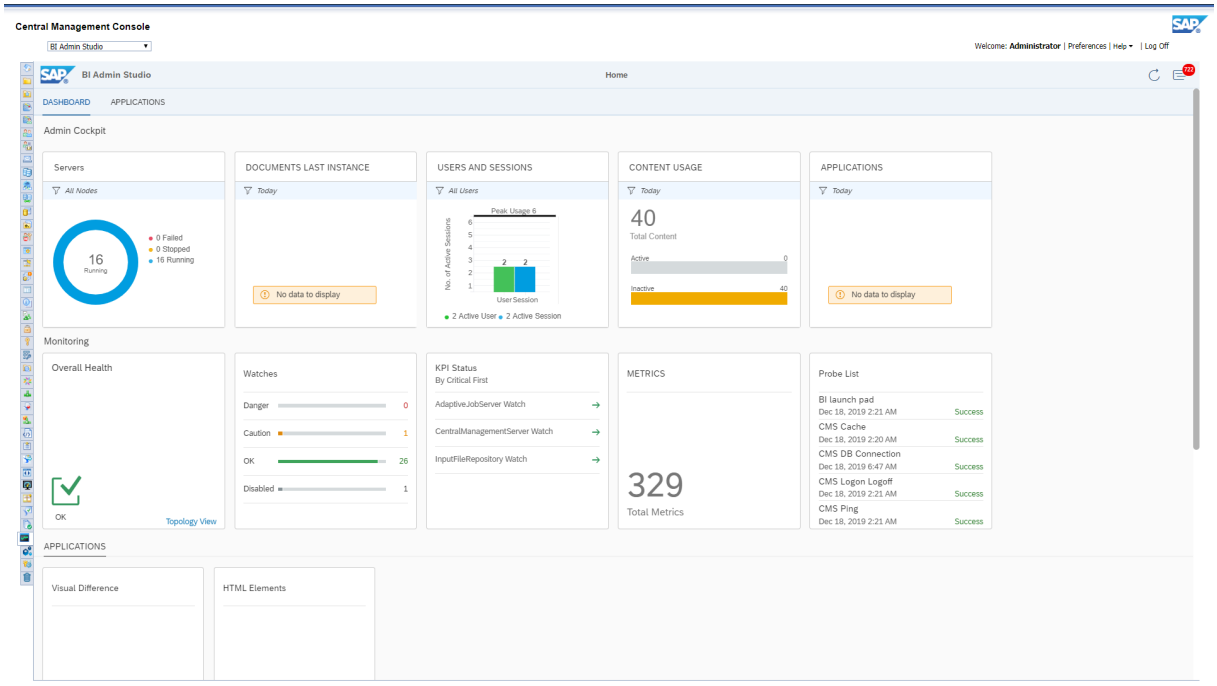
> **Remarque**
>
> Les conditions suivantes sont nécessaires pour garantir l'utilisation réussie du Cockpit d'administration BI :
>
> - Le service de surveillance doit être activé.
> - L'audit et l'événement correspondant doivent être activés pour que les bonnes données soient récupérées.
> - Le service Web RESTful de la plateforme de BI doit être accessible aux clients.
> - WACS doit fonctionner, à moins que le service Web RESTful soit déployé sur Tomcat.
> - Si vous configurez SSL pour la CMC, assurez-vous également de configurer SSL pour WACS, sauf si le service Web RESTful est déployé sur Tomcat.
> - L'accès multi-domaines doit être activé.
> - Les utilisateurs doivent appartenir au groupe Administrateurs ou à tout sous-groupe de celui-ci pour accéder au Cockpit d'administration BI.

20.1.1 Cockpit d'administration

Le Cockpit d'administration vous fournit une analyse exhaustive des données liées aux composants suivants, sous forme illustrée :

- Serveurs
- Dernière instance des documents
- Utilisateurs et sessions
- Utilisation du contenu
- Application

> **Remarque**
>
> La base de données d'audit doit être activée afin de pouvoir afficher l'analyse de l'*Utilisation du contenu* et des *Applications*.



Vous pouvez actualiser les données apparaissant dans chaque page du Cockpit d'administration en cliquant sur dans le coin supérieur droit de la page d'accueil.

20.1.2 BI et Serveurs

Le Cockpit d'administration vous permet d'obtenir des données en temps réel concernant le statut et les détails de tous les serveurs dans votre environnement BI.

La page d'accueil vous fournit les détails suivants :

- Nombre total de serveurs
- Nombre de serveurs comportant des erreurs
- Nombre de serveurs arrêtés

Vous pouvez filtrer des données qui s'affichent sur la vignette *Serveurs* en sélectionnant le cluster de serveurs voulu.

Lorsque vous cliquez sur la vignette *Serveurs*, vous êtes dirigé vers une page Serveurs qui contient les détails du nombre total de serveurs, les serveurs sur lesquels une erreur s'est produite et les serveurs arrêtés. La page Serveurs vous fournit également le *Statut*, le *Nom de serveur*, le *PID* (identificateur de procédure), le *Type*, l'*État* et l'*Heure de la dernière modification* de chaque serveur sur lequel une erreur s'est produite.

Dans la page *Serveurs*, vous pouvez filtrer les données en fonction de clusters de serveurs spécifiques en sélectionnant le cluster voulu.

Pour obtenir plus de détails sur le serveur sur lequel une erreur s'est produite, sélectionnez la ligne correspondante. Vous serez dirigé vers une nouvelle page qui détaille les motifs de l'erreur. Vous pouvez relancer le serveur sur lequel une erreur s'est produite depuis la page en sélectionnant *DÉMARRER*.

20.1.3 BI sur des instances de document

Vous pouvez utiliser le Cockpit d'administration pour obtenir des données concernant le statut et les détails de toutes les instances de documents planifiés dans votre environnement BI.

La page d'accueil vous donne les informations suivantes :

- Nombre total des dernières instances de chaque document planifié.
- Nombre des dernières instances en cours d'exécution de chaque document planifié.
- Nombre des dernières instances ayant engendré une erreur de chaque document planifié.
- Nombre des dernières instances en suspens de chaque document planifié.

Dans la vignette *Dernière instance des documents*, il est possible de filtrer les données pour une plage de périodes spécifique en sélectionnant la plage souhaitée dans le menu déroulant. Les plages de périodes disponibles sont :

- Aujourd'hui
- 7 derniers jours
- 30 derniers jours
- Trimestre
- Année

Lorsque vous cliquez sur la vignette *Dernière instance des documents*, vous êtes dirigé sur la page Dernières instances qui détaille le nombre total de dernières instances de chaque document planifié, ventilé par état : En cours d'exécution, Erreur et En suspens. L'onglet *Statistiques* fournit des détails que vous pouvez afficher dans les sections *Documents avec le plus d'instances* et *Instances avec exécution la plus longue*. La page Instances des documents vous fournit également le *Nom de l'instance*, le *Statut*, le *Type*, le *Propriétaire* et l'*Heure de fin* de chaque statut Erreur.

Vous pouvez exporter les données figurant sur la page *Dernières instances* sous la forme d'un fichier CSV en cliquant sur le bouton Exporter le lien. Vous pouvez également exporter les instances sélectionnées en cochant leur case, puis en choisissant *Exporter la sélection* dans la liste déroulante Exporter.

Pour obtenir plus de détails sur le serveur sur lequel une instance ayant engendré une erreur, sélectionnez la ligne correspondante. Vous pouvez relancer le travail depuis la page en sélectionnant *EXÉCUTER*.

Dans l'onglet des statistiques, le nouveau filtre de diagramme est activé, il permet de filtrer et afficher les 5, 10, 15 et 20 premiers documents.

20.1.4 Utilisateurs et sessions dans BI

Le Cockpit d'administration vous permet d'obtenir des données concernant les utilisateurs et les sessions dans votre environnement BI.

Par exemple, la page d'accueil vous fournit les détails suivants :

- Nombre d'utilisateurs actifs
- Nombre de sessions actives

Dans la vignette *Utilisateurs et sessions*, vous pouvez filtrer les données pour :

- Tous les utilisateurs
- Les utilisateurs nommés
- Les utilisateurs simultanés

En cliquant sur la vignette *Utilisateurs et sessions*, vous êtes dirigés vers une page Utilisateurs et sessions qui comporte les détails de tous les utilisateurs, des utilisateurs principaux et des statistiques. L'onglet Statistiques fournit des détails sur les utilisateurs les plus actifs et les plus inactifs.

La page Utilisateurs et sessions fournit également le *Nom d'utilisateur*, le *Total des sessions*, l'*Heure de la dernière connexion* et la *Plus longue session en cours d'exécution*.

Pour obtenir plus de détails sur un utilisateur particulier, sélectionnez la ligne correspondante. Vous serez dirigé vers une nouvelle page qui détaille les principales sessions de cet utilisateur. Vous pouvez interrompre toute session de cet utilisateur particulier depuis la page en sélectionnant la session voulue, puis *TERMINER LA SESSION*.

20.1.5 BI et Utilisation du contenu

Le Cockpit d'administration vous permet d'obtenir des données concernant l'utilisation du contenu dans votre environnement BI.

Par exemple, la page d'accueil vous fournit les détails suivants :

- Nombre de documents actifs
- Nombre de documents inactifs

Dans la vignette *Utilisation du contenu*, il est possible de filtrer les données pour une plage de périodes spécifique en sélectionnant la plage souhaitée dans le menu déroulant.

> **Remarque**
>
> Si vous avez supprimé du contenu actif et que vous filtrez des données pour une plage temporelle spécifique, l'élément supprimé apparaîtra toujours dans la liste du contenu actif s'il était actif au cours de la plage temporelle sélectionnée.

Les plages de périodes disponibles sont :

- Aujourd'hui
- 7 derniers jours
- 30 derniers jours
- Trimestre
- Année

Lorsque vous cliquez sur la vignette *Utilisation du contenu*, vous êtes dirigé vers une page Utilisation du contenu qui contient les détails du Contenu actif, du Contenu inactif ainsi que des statistiques. L'onglet Statistiques vous fournit des détails concernant les Boîtes de réception contenant le plus de Contenu inactif, les Univers avec le plus de contenu et les Dossiers avec le plus de contenu.

Vous pouvez exporter les données figurant sur la page *Utilisation du contenu* dans un fichier csv en sélectionnant le bouton du lien d'exportation. Vous pouvez également choisir d'exporter les travaux sélectionnés en cochant la case correspondante puis en choisissant *Exporter les objets sélectionnés* dans la liste déroulante d'exportation.

La page Utilisation du contenu vous fournit également le *Nom du contenu*, le *Type*, et l'*Heure d'exécution*.

Dans l'onglet des statistiques, le nouveau filtre de diagramme est activé, il permet de filtrer et afficher les 5, 10, 15 et 20 premiers documents.

20.1.6 BI et Applications

Le Cockpit d'administration vous permet d'obtenir des données concernant le nombre d'applications, triées par nom d'application dans votre environnement BI.

Dans la vignette *Application*, il est possible de filtrer les données pour une plage de périodes spécifique en sélectionnant la plage souhaitée dans le menu déroulant. Les plages de périodes disponibles sont :

- Aujourd'hui
- 7 derniers jours
- 30 derniers jours
- Trimestre
- Année

Lorsque vous cliquez sur la vignette *Applications*, vous êtes dirigé vers la page Applications qui contient les détails liés à *Toutes les applications* et aux *Top Applications*.

L'onglet *Top Applications* dresse une liste des 5 applications contenant le plus grand nombre de documents pour la plage de période sélectionnée. La page Applications vous fournit également le *Nom de l'application*, le *Nb. d'utilisateurs*, et le *Nb. d'artefacts*.

20.2 Surveillance

L'application de surveillance permet de capturer les métriques historiques et d'exécution des serveurs de la plateforme de BI pour le reporting et la notification. L'application de surveillance aide les administrateurs

système à identifier si une application fonctionne normalement et si les temps de réponse sont ceux escomptés. En fournissant des métriques d'activité clés, l'application de surveillance offre une meilleure perspective sur la plateforme de BI.

La surveillance permet d'effectuer ces tâches :

- Consulter les performances de chaque serveur : cela est possible grâce aux veilles, qui indiquent l'état de chaque serveur sous forme de feux de signalisation. L'administrateur système peut définir des seuils pour ces veilles et recevoir des alertes en cas de violation de ces seuils, et prendre une mesure en cas d'échec ou de panne.
- Visualiser les indicateurs de performance clés système importants : cela est utile lors de la surveillance d'activités et de ressources. Ces indicateurs de performance s'affichent dans la page du tableau de bord de l'application de surveillance.
- Visualiser l'intégralité du déploiement de la plateforme de BI (au format graphique et tabulaire) en fonction des groupes de serveurs, des catégories de services et des nœuds Enterprise.
- Visualiser les échecs récents sur l'écran de tableau de bord.
- Vérifier la disponibilité du système et le temps de réponse : à l'aide des tests, vous pouvez simuler des workflows pour vérifier si les serveurs et services du déploiement de la plateforme de BI fonctionnent comme escompté. En analysant le temps d'aller et retour de ces tests à des intervalles réguliers, l'administrateur système peut évaluer le schéma d'utilisation du système.
- Analyser la charge maximum et la période maximum du CMS : cela aide l'administrateur système à déterminer si davantage de licences ou ressources système sont nécessaires.
- Effectuer l'intégration à d'autres applications d'entreprise : l'application de surveillance de la plateforme de BI peut être intégrée à d'autres applications d'entreprise telles que SAP Solution Manager et IBM Tivoli Monitoring.
- Effectuez le suivi de la valeur de métrique du *Niveau d'audit* sous *Central Management Server* lorsque l'option *Définir les événements* est *désactivée* (valeur de métrique 1). Vous pouvez créer ici une liste de veilles lorsque la valeur de métrique est 1.Une alerte test est alors envoyée dans la liste de veilles avec une alerte par courrier électronique.

Pour en savoir plus sur l'utilisation de l'application de surveillance, notamment sur les tests et veilles, voir l'*Aide en ligne de la CMC de la plateforme SAP BusinessObjects Business Intelligence*.

Informations associées

A propos de l'annexe Métriques du serveur [page 1212]

20.2.1 Terminologie de la surveillance

La liste suivante fournit la terminologie relative à l'application de surveillance :

Tendance

Pour enregistrer ou afficher des données historiques afin de rechercher des tendances.

Tableau de bord

La page Tableau de bord offre une vue centralisée pour que l'administrateur système surveille les performances de tous les serveurs. Elle présente des informations en temps réel relatives aux indicateurs de performance clés, aux alertes récentes et aux veilles du système, ainsi que les graphiques correspondants basés sur l'état des veilles.

Veille

Les veilles indiquent le statut en temps réel et les tendances historiques des serveurs et des workflows dans l'environnement de la plateforme de BI. Les utilisateurs peuvent associer des seuils et des alertes aux veilles. Vous pouvez créer une veille à l'aide des données des tests, des serveurs, de SAPOSCOL ou des métriques dérivées.

Métrique dérivée

Les métriques dérivées sont des métriques que vous créez en combinant deux métriques existantes ou plus dans une équation mathématique. Vous pouvez créer une métrique en fonction des besoins de l'utilisateur, puis créer une veille qui utilise cette métrique.

Métrique topologique

Les métriques topologiques fournissent l'état net de chaque catégorie de service sur la plateforme de BI. Par exemple, le service Crystal Reports donne l'état combiné de toutes les veilles associées aux serveurs Crystal Reports.

Etat

Valeurs de l'état :

- "0" - "DANGER"
- "1" - "ORANGE"
- "2" - "VERT"

KPI

Les KPI (indicateurs de performance clés) sont des métriques standard de la plateforme de BI. Ils fournissent des informations sur les planifications et les sessions de connexion. Par exemple, un nombre élevé de *TravauxEnCours* indique de bonnes performances des serveurs. Par contre, un nombre élevé de *TravauxEnSuspens* indique de mauvaises performances et une grande charge système.

Test

Les tests surveillent différents services et simulent les différentes fonctionnalités des composants de la plateforme de BI. En planifiant des tests pour qu'ils s'exécutent à des intervalles spécifiés, l'administrateur système peut suivre la disponibilité et les performances des services clés fournis par la plateforme de BI. Ces données peuvent également être utilisées pour la planification de la capacité.

Feu de signalisation

Un feu de signalisation est une icône qui affiche la couleur verte, orange ou rouge pour indiquer l'état d'une veille à un moment donné. Les utilisateurs peuvent choisir de définir deux ou trois états pour une veille.

Graphique de tendances

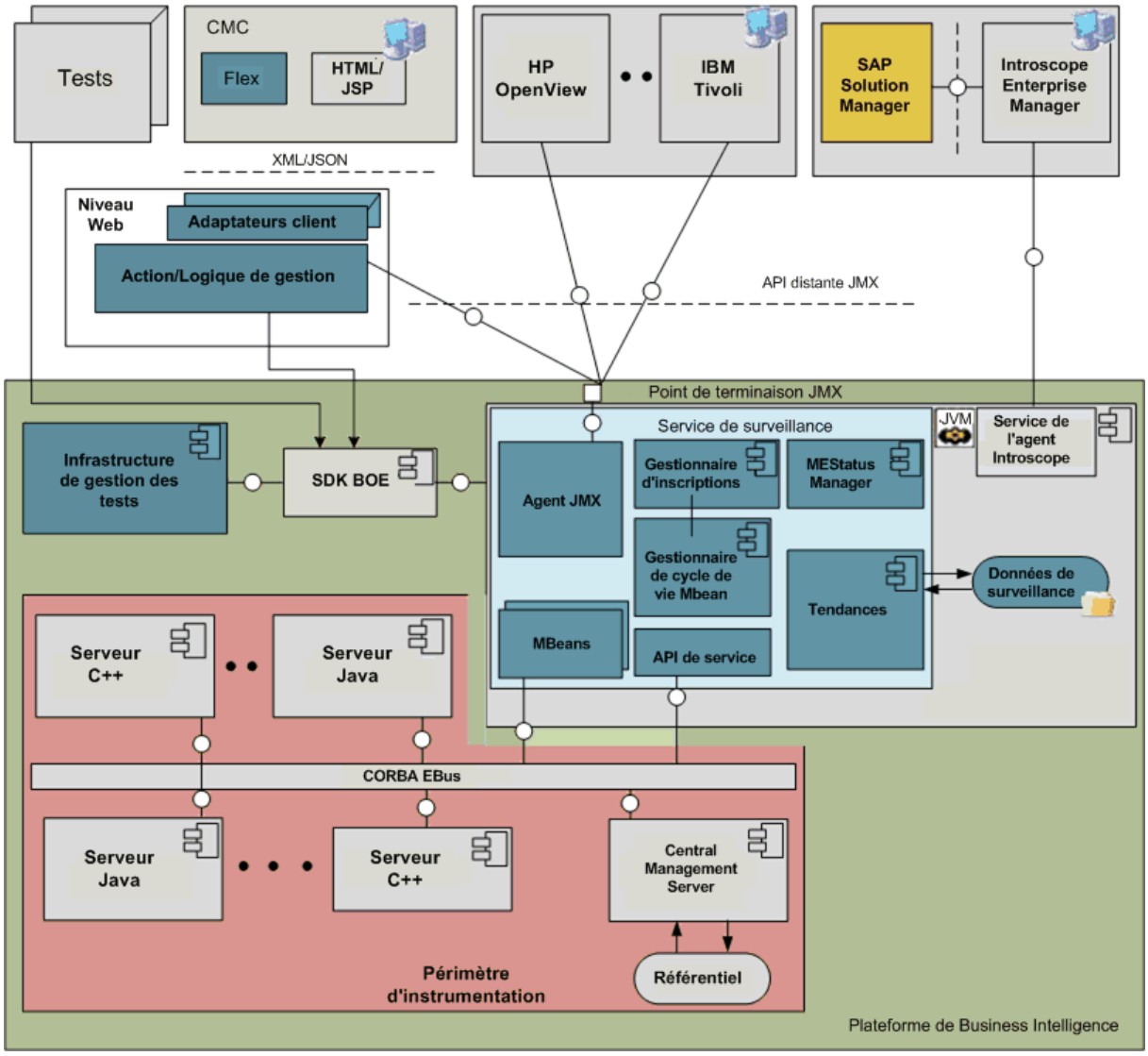
Le graphique de tendances est une représentation graphique de données de métriques historiques générées par les tests et les serveurs. Il aide l'administrateur système à surveiller le système à différents intervalles de temps et à évaluer le schéma d'utilisation système.

Alerte

Une alerte est une notification générée par l'application de surveillance lorsqu'est franchie une valeur de seuil définie par l'utilisateur pour différentes métriques appliquées à une veille. Vous pouvez choisir de recevoir des alertes par courrier électronique ou sur la page *Tableau de bord*.

20.2.1.1 Architecture

Cette section fournit une présentation de niveau supérieur de l'architecture de surveillance et explique brièvement les rôles joués par les composants. L'architecture de surveillance est représentée graphiquement ci-dessous :



Les composants de niveau supérieur de l'architecture sont répertoriés ci-dessous :

- Le serveur de traitement adaptatif (APS)
- L'agent ou serveur Java Management Extensions (JMX)
- MBeans
- Clients JMX
- Les consoles de gestion
- Base de données des tendances

Le service de surveillance est hébergé sur le serveur de traitement adaptatif. L'application est basée sur la technologie JMX.

Le service de surveillance fournit les services principaux disponibles dans l'application de surveillance. Le service de surveillance fournit les services suivants :

- Fournit le service d'agent JMX.
- Crée des MBeans de manière dynamique pour les serveurs SAP BusinessObjects.

- Fournit une gestion du cycle de vie pour les MBeans.
- Fournit un mécanisme d'enregistrement des nouveaux tests.
- Permet aux utilisateurs de créer des conditions de seuil complexes à l'aide des métriques des serveurs.
- Fournit un mécanisme de notification de seuil et envoie des alertes.
- Stocke les données historiques.

Le service de planification de métrique qui est hébergé sur l'Adaptive Job Server gère l'exécution et la planification des métriques. L'Adaptive Job Server doit donc être en cours d'exécution pour que les métriques s'exécutent.

L'application de surveillance expose également un point de terminaison d'URL JMX ou RMI (Remote Method Invocation). D'autres applications d'entreprise telles qu'IBM Tivoli Monitoring peuvent se connecter à l'application de surveillance et accéder aux métriques de la plateforme de BI en utilisant une API JMX distante. L'application de surveillance utilise la base de données du magasin de données d'audit pour le stockage de données historiques à des fins d'établissement de tendances. Pour en savoir plus sur le schéma de base de données des tendances, voir Schéma de la base de données des tendances [page 1248].

20.2.2 Configuration de la prise en charge de la base de données pour la surveillance

Cette section décrit comment configurer la surveillance et établir des rapports sur les données de surveillance.

> **Remarque**
>
> Seules les veilles dont le paramètre *Ecrire dans la base de données des tendances* est sélectionné écrivent des informations de surveillance dans la base de données des tendances.

Il existe deux options de base de données pour enregistrer les informations de surveillance : enregistrer les informations à l'aide du magasin de données d'audit ou toute autre base de données prise en charge par la plateforme via le pilote JDBC.

> **Remarque**
>
> La base de données Apache Derby est obsolète dans la version BI 4.3. Pour plus d'informations sur la migration et la sauvegarde des données, voir la Note SAP 2912759.

Vous pouvez utiliser le magasin de données d'audit par défaut, souvent appelé base de données d'audit. Il s'agit de la base de données relationnelle où le CMS stocke les données d'audit. Vous pouvez utiliser le magasin de données d'audit inclus dans la plateforme de BI ou toute autre base de données prise en charge que vous avez configurée comme base de données d'audit.

Les autres bases de données prises en charge sont les suivantes :

- DB2
- SQL Server
- My SQL
- Oracle
- Base de données SAP HANA

- SQL Anywhere
- Sybase

L'utilisation de la base de données d'audit permet aux utilisateurs d'établir des rapports à partir des données d'audit jointes aux informations de surveillance. La capture des données dans une base de données relationnelle offre la possibilité de sauvegarde et de restauration ainsi que la disponibilité en temps réel des données.

Informations associées

Configuration pour utiliser la base de données d'audit [page 827]

20.2.2.1 Configuration pour utiliser la base de données d'audit

Afin d'utiliser la base de données d'audit pour les données de surveillance, vous devez exécuter les étapes de configuration suivantes :

- Avant BI 4.3, si la base de données des tendances Derby renfermait des données, vous deviez la faire migrer vers la base de données d'audit, puis configurer la plateforme de BI pour enregistrer les informations de surveillance dans la base de données d'audit. Voici les étapes générales à suivre. Pour en savoir plus, consultez les rubriques associées.
  1. Faites migrer la base de données Derby.
  2. Configurez les fichiers SBO et ajoutez des noms d'alias.
  3. Basculez vers la base de données d'audit.
  4. Redémarrez le serveur de traitement adaptatif qui héberge le service de surveillance.
  5. Sur le tableau de bord de surveillance, vérifiez que tout fonctionne comme prévu. Vérifiez que ces tables de surveillance ont été créées dans la base de données :

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- Si la base de données des tendances ne renferme pas de données, c'est-à-dire si l'installation est nouvelle, vous n'avez pas besoin de la faire migrer. Il suffit de configurer la plateforme de BI pour enregistrer les informations de surveillance dans la base de données d'audit. Voici les étapes générales à suivre. Pour en savoir plus, consultez les rubriques associées.
  1. Vérifiez que la base de données d'audit fonctionne et que l'audit fonctionne correctement.
  2. Créez les tables de surveillance dans le magasin de données d'audit.
  3. Configurez les fichiers SBO et ajoutez des noms d'alias.
  4. Basculez vers la base de données d'audit.
  5. Redémarrez le serveur de traitement adaptatif qui héberge le service de surveillance.
  6. Sur le tableau de bord de surveillance, vérifiez que tout fonctionne comme prévu. Vérifiez que ces tables de surveillance ont été créées dans la base de données :

MOT_MES_DETAILS
MOT_MES_METRICS
MOT_TREND_DATA
MOT_TREND_DETAILS

> **Remarque**
>
> Si vous enregistrez les données de surveillance dans la base de données d'audit et que vous désirez établir des rapports à partir de ces données, vous devrez développer un univers personnalisé.

Informations associées

Configuration de fichiers SBO [page 829]
Ajout de noms d'alias dans le fichier SBO [page 832]
Pour basculer vers la base de données d'audit [page 832]
Pour créer les tables de surveillance dans le magasin de données d'audit [page 828]

20.2.2.1.1 Pour créer les tables de surveillance dans le magasin de données d'audit

Suivez cette procédure pour préparer la base de données d'audit cible :

1. Après l'installation de la plateforme de BI, les fichiers DDL associés à toutes les bases de données d'audit du CMS prises en charge sont accessibles à l'emplacement suivant : `<Rép_Install>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. Vous trouverez sept fichiers différents (extension .sql) portant le nom des bases de données respectives. Par exemple : `Oracle.sql` pour Oracle, `Sybase ASE.sql` pour la base de données Sybase ASE, etc.
2. Accédez à la base de données cible (dans ce cas, la base de données cible est celle où l'audit du CMS a été configuré) et exécutez le fichier .sql. Les quatre tables de surveillance suivantes sont créées : `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS` et `MOT_MES_METRICS`. Les index nécessaires sont aussi créés avec les tables.

Si toutes les tables sont créées avec les types de données corrects mentionnés dans le fichier .sql, le schéma de base de données requis pour l'application de surveillance est créé.

20.2.2.1.2 Pour restaurer le contenu dans la base de données cible

Les étapes suivantes doivent être effectuées afin de restaurer le contenu dans la base de données cible :

1. Activez l'insertion d'identités.

   Les tables de l'application de surveillance contiennent un certain nombre de colonnes IDENTITY. Ce sont des colonnes qui génèrent automatiquement leurs valeurs. Certaines bases de données (comme MS SQL

Server et Sybase ASE) n'autorisent pas l'insertion explicite de valeurs dans ces colonnes. Au cours de la migration des données, même ces valeurs des colonnes d'identité doivent être migrées. Les utilisateurs doivent donc activer l'insertion explicite de ces valeurs à l'aide de la commande SQL suivante : `SET IDENTITY_INSERT <NOM DE TABLE> ON`.

2. Importez le fichier de vidage CSV dans la table cible.

   Tous les logiciels fournis par les clients de base de données donnent aux utilisateurs la possibilité d'importer les données à partir de fichiers CSV dans la table en utilisant une option de menu ou une commande. L'utilisateur doit recourir à cette option pour importer les données du fichier CSV dans la table correspondante. Importez les fichiers de données dans les nouvelles tables dans l'ordre suivant :

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`

3. Désactivez l'insertion d'identités.

   Une fois les données importées, l'utilisateur doit désactiver l'insertion d'identités dans la table à l'aide de la commande SQL suivante : `SET IDENTITY_INSERT <NOM DE TABLE> OFF`.

   Les utilisateurs doivent désactiver l'insertion d'identités dans une table après l'importation de données afin d'activer l'insertion d'identités dans la table suivante. En effet, l'opération d'insertion d'identités ne peut être activée que dans une table à la fois.

L'activation ou désactivation de l'insertion d'identités s'applique uniquement aux bases de données MS SQL Server et Sybase ASE. Cela n'est pas obligatoire pour les autres bases de données comme Oracle, MaxDb, DB2, MySQL ou SQL Anywhere. Vous pouvez importer les données directement dans les tables.

20.2.2.1.3 Configuration de fichiers SBO

En interne, l'application de surveillance utilise les bibliothèques du serveur de connexion ; or la configuration SBO est nécessaire pour que le serveur de connexion établisse la connexion avec le pilote de base de données. Vous devez spécifier le pilote de base de données et son emplacement dans le fichier SBO pour établir cette connexion.

> **ⓘ Remarque**
>
> L'application de surveillance correspond à un nom de connexion d'audit et utilise JDBC si `<NomHôte>.<NumPort>.<NomBdd>` est utilisé, sinon elle utilise ODBC. Les fichiers SBO du serveur de connexion doivent être configurés en conséquence pour que l'application de surveillance puisse se connecter à la base de données d'audit.

> **ⓘ Remarque**
>
> Pour les bases de données Oracle, seules les connexions JDBC sont prises en charge.

Exemple

- Si le champ Nom de la connexion configuré dans la page Audit de la CMC est `<NomHôte>.<NumPort>.<NomBdd>`, le pilote JAR doit être configuré dans : `dataAccess\connectionServer\jdbc\<TypeBDD>.sbo`.
- Si le champ Nom de la connexion configuré dans la page Audit de la CMC est un DNS ODBC, le pilote doit être configuré dans : `<Rép_Install>\dataAccess\connectionServer\odbc\<TypeBDD>.sbo`.
- Si la base de données utilisée pour l'audit est SAP HANA, le fichier où le pilote doit être configuré est : `<Rép_Install>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Si la base de données utilisée pour l'audit est MS SQL Server, le fichier où le pilote doit être configuré est : `<Rép_Install>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Si la base de données utilisée pour l'audit est un serveur DB2, le serveur de connexion ne contient pas de fichier `db2iseries.sbo` de prise en charge.
  Par défaut, l'application de monitorage utilise le mode de connexion ODBC pour se connecter à la base de données d'audit DB2. Pour utiliser ce mode, vous devez ajouter le DSN système (pour le serveur DB2) à l'ordinateur sur lequel l'application de surveillance est exécutée et le configurer. Pour en savoir plus sur la manière d'ajouter la connexion ODBC pour DB2 et de la configurer, référez-vous aux liens suivants :
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

> **Remarque**
>
> Si vous ne configurez pas le DSN système pour DB2, les tendances de surveillance échouent.

Configuration de fichiers SBO

En général, les bibliothèques ODBC sont déjà configurées dans les fichiers SBO et vous n'avez qu'à ajouter les noms d'alias. Si ce n'est pas le cas, suivez ces exemples pour effectuer la configuration dans le fichier SBO :

Exemple

- Si la version de base de données utilisée pour l'audit est SAP HANA, la configuration dans le fichier SBO doit être :

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
```

```
</DataBase>
```

- Si la version de base de données utilisée pour l'audit est MS SQL Server 2008, la configuration dans le fichier SBO doit être :

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D">Si la version de base de données utilisée pour l'audit est MySQL 5, le fichier SBO doit comporter l'entrée :

```
<DataBase Active="Yes" Name="MySQL 5">
    <JDBCDriver>
        <ClassPath>
            <Path>C:\mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- Si la version de base de données utilisée pour l'audit est Oracle, la configuration dans le fichier SBO doit être :

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>

<Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib\ojdbc6.jar</Path>
             </ClassPath>
                <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

Pour en savoir plus sur la configuration du pilote dans les fichiers SBO, voir le *Guide d'accès aux données*.

20.2.2.1.4 Ajout de noms d'alias dans le fichier SBO

Outre la configuration du pilote, l'utilisateur doit également ajouter un alias dans le fichier SBO, sous la version de base de données utilisée pour l'audit. Le tableau suivant répertorie les noms d'alias devant être utilisés pour des bases de données spécifiques.

Nom de base de données	Nom d'alias à utiliser dans le fichier SBO
SAP HANA	Hana
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

Vous devez utiliser les noms spécifiés parce que l'application de surveillance recherche ces noms dans le fichier SBO.

Exemple

Si la base de données utilisée pour l'audit est MS SQL Server 2008, l'alias doit être ajouté au fichier SBO comme suit :

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</
Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```

20.2.2.1.5 Pour basculer vers la base de données d'audit

Changez de base de données afin que les informations de tendances de la surveillance soient stockées dans la base de données d'audit.

1. Dans la zone *Gérer* de la page d'accueil de la CMC, cliquez sur *Applications*.

2. Cliquez sur *Studio d'administration BI*.
3. Cliquez ensuite sur *Propriétés de surveillance*.
4. Cliquez deux fois sur *Application de surveillance* pour ouvrir la page Propriétés.
5. Dans la zone *Paramètres de base de données des tendances*, sélectionnez *Utiliser la base de données d'audit*.

> **Remarque**
>
> Si vous utilisez une base de données Oracle pour l'audit, le champ *Nom de la connexion de la base de données du magasin de données d'audit* sur la page Audit de la CMC doit être spécifiée comme une connexion JDBC. Spécifiez le nom de la connexion comme suit : `<server_name>,<port>,<service_name>`.

> **Remarque**
>
> Pour garantir que les tables de surveillance sont correctement créées, attribuez les autorisations suivantes pour le compte utilisateur de la base de données :
>
> EXECUTION
> CREATION DE SEQUENCE
> CREATION DE DECLENCHEMENT

20.2.2.2 Configuration de la base de données de surveillance à l'aide de JDBC

Vous avez créé une connexion JDBC. Pour créer une connexion JDBC, suivez les étapes ci-après :

1. Placez le fichier jar du pilote JDBC pour la base de données que vous souhaitez configurer à l'emplacement suivant : `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\MON.MonitoringService\lib>`.

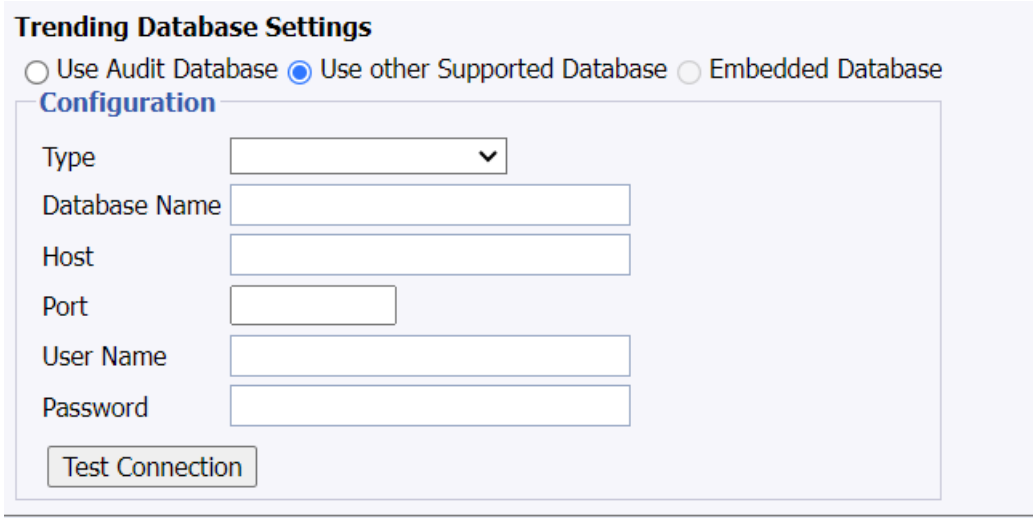
   > **Remarque**
   >
   > Dans les déploiements en cluster, vous devez copier le pilote JDBC dans le système qui héberge les services de surveillance.

2. Redémarrez le SIA.

Pour configurer une nouvelle base de données pour la Surveillance BI, suivez cette procédure :

1. Connectez-vous à la CMC.
2. Sur la page d'accueil de la CMC; sélectionnez *Applications* dans le menu déroulant.
3. Cliquez avec le bouton droit de la souris sur *Studio d'administration BI* et sélectionnez *Propriétés de surveillance*.

   La fenêtre *Propriétés de l'application de surveillance* apparaît. La case d'option *Utiliser la base de données d'audit* est cochée par défaut.
4. Cochez la case d'option *Utiliser une autre base de données prise en charge*.
5. Saisissez le *Type*, le *Nom de la base de données*, l'*Hôte*, le *Port*, le *Nom d'utilisateur* et le *Mot de passe*.



6. **Facultatif :** Ajoutez un nombre de jours après lequel la plateforme doit supprimer les données de l'historique de surveillance à l'aide de la propriété *Supprimer tout l'historique datant de plus de X jours*
7. Cliquez sur *Enregistrer et fermer*.
8. Redémarrez le serveur de traitement adaptatif.

   Vous pouvez valider votre connexion en sélectionnant *Tester la connexion*.

> ⓘ Remarque
>
> Vous devez redémarrer tous les serveurs APS qui hébergent le service Surveillance BI pour que les modifications prennent effet.

Vous avez correctement configuré une nouvelle base de données afin de stocker les commentaires de l'application de surveillance BI.

20.2.3 Propriétés de configuration

Cette section décrit les propriétés de l'application de surveillance et la manière de les modifier.

Pour visualiser les propriétés de configuration de l'application de surveillance :

1. Sur la page d'accueil de la CMC, cliquez sur *Application*.
2. Cliquez avec le bouton droit de la souris sur *Studio d'administration BI* et sélectionnez *Propriétés de surveillance*. Les propriétés configurables sont décrites ci-dessous.

Section	Champ	Description
	Activer l'application de surveillance	Sélectionnez cette option pour activer les fonctionnalités de surveillance. Si vous désélectionnez cette option, toutes les fonctions de surveillance à l'exception des tests seront désactivées. Le test de tendances sera également désactivé.

Section	Champ	Description
	URL du point de terminaison de l'agent JMX par défaut (IIOP)	Contient l'URL du point de terminaison de l'agent JMX par défaut qui utilise le protocole IIOP. Cette URL est générée automatiquement si vous activez la surveillance, puis que vous redémarrez le serveur. Il s'agit du protocole par défaut du service de surveillance. Ce champ est en lecture seule.
RMI	*Activer le protocole RMI pour JMX*	Par défaut, cette option est désactivée. Si vous activez cette option, vous devez fournir le numéro de port RMI. Le port sera utilisé aussi bien comme port d'enregistrement de registre RMI que de connecteur RMI. Ce port doit être accessible au service, sans quoi le service ne parviendra pas à démarrer. Après avoir fourni le numéro de port RMI, redémarrez le serveur. Une fois le serveur redémarré, l'URL du point de terminaison de l'agent JMX RMI est générée. Il s'agit d'une propriété en lecture seule contenant l'URL du point de terminaison de l'agent JMX utilisant le protocole RMI. Utilisez cette URL pour vous connecter à la surveillance à partir d'autres clients.
Métriques de l'hôte	*Activer les métriques de l'hôte*	Par défaut, cette option est désactivée. Si vous activez cette option, vous devez fournir le chemin d'accès à votre installation de binaire SAPOSCOL. Pour activer les métriques de l'hôte, il faut installer SAPOSCOL. Pour en savoir plus sur SAPOSCOL et son installation, voir « Installation de SAPOSCOL ».
Paramètres de base de données des tendances	*Utiliser la base de données d'audit*	Sélectionnez cette option pour stocker l'historique des tendances des métriques dans la base de données d'audit du magasin de données d'audit. **Remarque** Le magasin de données d'audit doit être configuré pour que cela fonctionne.
	Utiliser une autre base de données prise en charge	Sélectionnez cette option pour stocker l'historique des tendances de métriques ou veilles dans une base de données prise en charge que vous avez configurée.
	Supprimer tout l'historique datant de plus de X jours	Indique le nombre de jours pendant lesquels les données d'historique doivent être conservées.

Section	Champ	Description
Autres paramètres	*Intervalle d'actualisation de métrique (en secondes)*	L'intervalle minimum pouvant être spécifié est de 15 secondes. Cet intervalle régit les éléments suivants : • Calcul d'inscription des veilles : les règles de mise en garde et de danger sont calculées en permanence selon l'intervalle de temps spécifié. • Calcul de l'état de l'espion : l'état de l'espion est calculé en permanence selon l'intervalle de temps spécifié si le paramètre Evénement de l'espion est sélectionné avec l'option suivante : *Modifier l'état de la veille chaque fois que la règle de mise en garde ou la règle de danger donne la valeur Vrai*. • Période de tendance : le mode Historique des graphiques est enregistré en continu selon l'intervalle de temps spécifié.
	Intervalle d'actualisation automatique de l'interface utilisateur de surveillance (en secondes)	Cet intervalle est utilisé dans l'interface utilisateur de surveillance (dont le tableau de bord, la liste de veille et les tests) pour l'actualisation automatique. L'intervalle minimum est de 15 secondes. L'actualisation automatique n'affecte pas la durée du mode direct des graphiques qui est défini sur 15 secondes par défaut.
	Fréquence des rappels d'alerte (jours)	Indique le nombre de jours précédant la génération d'un rappel d'alerte.

3. Cliquez sur *Enregistrer*.

> **Remarque**
>
> Lorsque vous modifiez une de ces propriétés, sauf l'activation et la désactivation de l'application de surveillance, vous devez redémarrer les serveurs de traitement adaptatif qui hébergent les services de surveillance.

Installation de SAPOSCOL

Effectuez les opérations suivantes pour installer SAPOSCOL :

1. Téléchargez `SAPHOSTAGENT710_XX.SAR` depuis SAP Marketplace (http://service.sap.com).
2. Extrayez `SAPHOSTAGENT710_XX.SAR` en exécutant la commande `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR`.
3. Installez `saphostexec` en exécutant la commande `saphostexec.exe -install`. Lorsque saphostexec est installé en tant que service, SAPOSCOL est démarré.
4. Vérifiez le statut de SAPOSCOL en exécutant la commande `saposcol -s`.

20.2.3.1 URL du point de terminaison JMX

L'application de surveillance fournit une URL de point de terminaison JMX via laquelle d'autres clients peuvent se connecter en utilisant une API distante JMX. Par défaut, la connectivité JMX est fournie par-dessus le transport IIOP (Internet Inter-Orb Protocol) ou CORBA (Common Object Request Broker Architecture). Cette URL de connexion s'affiche dans la page de propriétés de l'application de surveillance. La possibilité de se connecter par-dessus IIOP libère des tracas relatifs aux pare-feux et de l'exposition des ports. Par défaut, les ports CORBA sont disponibles. Les fichiers jar répertoriés dans le tableau suivant sont nécessaires à la terminaison du client JMX pour être en mesure d'établir la connexion :

Fichiers JAR
`activation-1.1.jar`
`axiom-api-1.2.5.jar`
`axiom-impl-1.2.5.jar`
`axis2-adb-1.3.jar`
`axis2-kernel-1.3.jar`
`cecore.jar`
`celib.jar`
`cesession.jar`
`commons-logging-1.1.jar`
`corbaidl.jar`
`ebus405.jar`
`log4j.jar`
`logging.jar`
`monitoring-plugins.jar`
`monitoring-sdk.jar`
`stax-api-1.0.1.jar`
`wsdl4j-1.6.2.jar`
`wstx-asl-3.2.1.jar`
`XmlSchema-1.3.2.jar`
`TraceLog.jar`
`ceaspect.jar`
`aspectjrt.jar`

Une autre option consiste à se connecter par le biais du port RMI par défaut. Pour en savoir plus sur la connexion par le biais du port RMI, voir Propriétés de configuration [page 834].

20.2.3.2 Configuration SSL JMX

Vous pouvez désormais établir une communication sécurisée entre JConsole et BOE via la configuration SSL JMX.

1. Connectez-vous à la CMC.
2. Accédez à *Applications* > *Studio d'administration BI* > *Propriétés de surveillance*.
3. Sous *RMI*, activez l'option *Activer le protocole RMI pour JMX*.
4. Saisissez le numéro de port RMI.

   7777
5. Activez l'option *Activer SSL pour le protocole RMI pour JMX*.
6. Cliquez sur *Enregistrer* et *Fermer*.
7. Redémarrez le *serveur de traitement adaptatif*.

   > **Remarque**
   >
   > Le serveur hébergeant le service de surveillance est redémarré.

20.2.3.2.1 Génération du certificat

1. Ouvrez l'invite de commande en mode Administrateur ou dans une session de terminal et accédez à l'emplacement suivant :

   Windows :

   ```
   <RÉP_INSTALL>\SAP BusinessObjects Enterprise XI 4.0\ win64_x64\sapjvm\bin
   ```

   Linux/Unix :

   ```
   RÉP_INSTALL/sap_bobj/enterprise_xi40/<PLATEFORME>_x64/sapjvm/bin
   ```
2. Exécutez la commande permettant de générer un certificat : `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore`
3. Saisissez toutes les informations requises pour créer un certificat.
4. 4. Une fois l'exécution terminée, un fichier de certificat est créé en fonction du nom dans le même répertoire bin de sapjvm : `serverkeystore`.

20.2.3.2.2 Ajout d'un fichier de stockage des certificats au service de surveillance

1. Dans la CMC, accédez à *Serveurs* > *Liste des serveurs*.
2. Sélectionnez *Serveur de traitement adaptatif* (serveur hébergeant le service de surveillance).
3. Sélectionnez *Propriétés*.

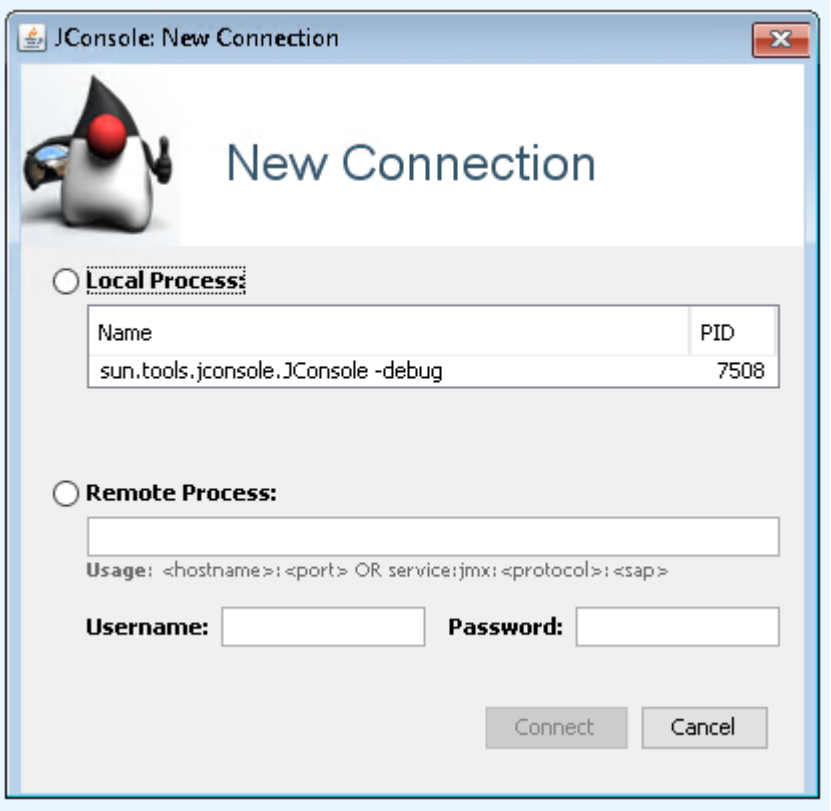
4. Accédez à la section *Configuration SSL JMX*.
5. Dans *Emplacement du fichier de stockage des certificats*, saisissez le chemin d'accès au *fichier de stockage des certificats*.
6. Saisissez les informations relatives au *mot de passe d'accès à la clé privée*.

   Mot de passe1

20.2.3.2.3 Connexion à JConsole

1. Exécutez la commande permettant de lancer `JCONSOLE.exe` dans l'invite de commande (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`)

   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:\Program Files
   (x86)\SAP BusinessObjects\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\bin\serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```
2. Une fois exécutée, la commande ci-dessus lance le visualiseur JConsole comme indiqué ci-dessous.

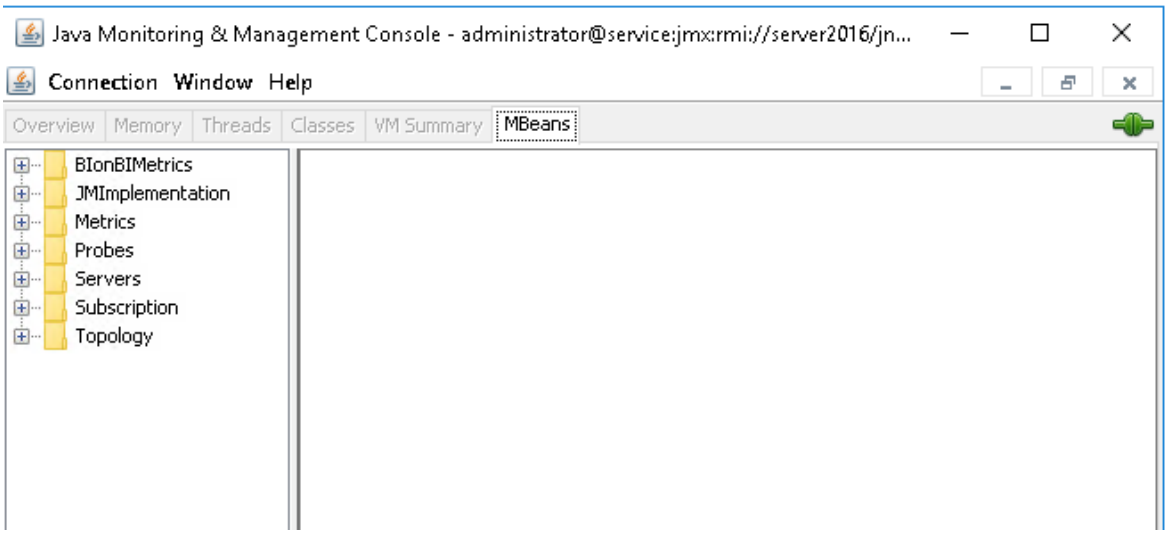


3. Cliquez sur la case d'option *Processus distant* pour activer le champ.
4. Saisissez l'*URL du point de terminaison de l'agent RMI JMX*, ainsi que le *nom d'utilisateur* et le *mot de passe* associés.

   Le format de l'*URL du point de terminaison de l'agent RMI JMX* est le suivant : `service:jmx:rmi://<HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

`service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.

5. Cliquez sur *Connexion*.
6. Le visualiseur JConsole *JAVA Monitoring & Management Console* (Console de gestion et surveillance Java) est lancé.



7. Dans le visualiseur JConsole, vous pouvez accéder à différentes sections, telles que BIonBIMetrics, Metrics, Probes, Servers et Topology pour extraire les données associées.

20.2.3.3 Authentification HTTPS pour les métriques de surveillance

L'authentification serveur HTTPS pour les métriques de surveillance est prise en charge et requiert la configuration suivante avant utilisation :

1. Importez le certificat du serveur dans le fichier de stockage sécurisé du client. Cela permet au côté client (la métrique) de vérifier l'identité du serveur. Exécutez cette commande :
   `<RACINE_INSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib>`
   `keytool -import -alias ca -keystore "<RACINE_INSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" –file ca.cer`
   `ca.cer` est le certificat auto-signé du serveur ou le certificat de l'autorité de certification (habituellement une autorité interne) ayant généré le certificat du serveur. Si le certificat du serveur est généré par une autorité de certification bien connue, il n'y a pas besoin de l'importer et cette étape peut être ignorée. En effet, le certificat du serveur sera vérifié par l'autorité de certification, dont la clé publique est déjà par défaut dans le fichier de stockage sécurisé.
2. Changez la *Base URL* dans les paramètres de métrique de la zone de lancement en `https://<URL>/BOE/BI`, où <URL> fait référence à l'hôte par le nom utilisé dans le certificat.

L'authentification client HTTPS pour les métriques de surveillance n'est pas prise en charge.

20.2.3.4 Cryptage des mots de passe pour les tests

Lors de l'utilisation de tests, pour vous assurer que les mots de passe sont cryptés, vous devez ajouter le paramètre `true` à chaque paramètre de métrique de surveillance lors de la création du test avec la ligne de commande. Pour en savoir plus et consulter un exemple de syntaxe, voir la rubrique *Gestion des tests via la ligne de commande* dans l'aide de la CMC.

20.2.4 Intégration à d'autres applications

Les solutions d'entreprise, telles qu'IBM Tivoli Monitoring, s'intègrent à l'application de surveillance en tant que clients JMX se connectant via l'URL du point de terminaison JMX. Après l'intégration, les métriques SAP BusinessObjects peuvent être visualisées à partir de l'interface utilisateur du client.

20.2.4.1 Intégration de l'application de surveillance à SAP Solution Manager

Pour intégrer l'application de surveillance à SAP Solution Manager, Wily Introscope doit être installé et en cours d'exécution sur votre système. SAP Solution Manager doit être configuré pour la station de travail Introscope. Suivez ces étapes lors de l'installation de la plateforme de BI :

1. Lors de l'étape « Configurer la connectivité à Wily Introscope Enterprise Manager », fournissez le nom d'hôte et les détails du port. Un agent Introscope sera installé à l'emplacement `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wily` lors de l'installation de la plateforme de BI.
2. Lancez la station de travail Wily Introscope et cliquez sur *Nouvel enquêteur*. Vous pouvez visualiser les métriques du serveur SAP BusinessObjects et les métriques virtuelles de test dans la section JMX de l'agent configuré.

> **Remarque**
>
> Vous pouvez configurer l'agent Wily Introscope (IS) en choisissant *CMC* > *Serveurs* > *Nœud de serveur* > *Espaces réservés*. L'hôte et le port d'IS Enterprise Manager sont également configurés pour que l'agent IS communique avec l'application de surveillance. Pour en savoir plus, voir le chapitre *Gestion des serveurs* de l'Aide de la CMC.
>
> Pour que les métriques JMX soient disponibles dans IS, assurez-vous que les services de l'agent IS et le service de surveillance sont disponibles sur l'instance du serveur de traitement adaptatif.
>
> Si vous activez l'instrumentation IS, l'instrumentation du code est activée automatiquement.

20.2.5 Prise en charge de cluster pour serveur de surveillance

L'application de surveillance prend en charge la mise en cluster, qui fournit une fonctionnalité de basculement.

Grâce à la prise en charge des clusters, un seul service est actif à tout moment tandis que les autres sont passifs. S'il existe deux services de surveillance s1 et s2 dans un environnement en cluster, un seul est disponible. Les services s1 et s2 essaient tous deux de devenir actifs, mais quand l'un des deux y parvient, l'autre devient inactif ou passif.

Le service passif contrôle périodiquement la disponibilité du service actif (toutes les minutes). Si le service actif n'est pas disponible, le service passif tente immédiatement de devenir actif.

> **Remarque**
>
> Il est recommandé d'héberger le service de surveillance sur une instance distincte de l'APS (serveur de traitement adaptatif) pour en éviter les défaillances ou de piètres performances.

20.2.6 Dépannage

Cette section fournit des solutions détaillées à un vaste éventail de problèmes pouvant survenir dans votre travail avec l'application de surveillance.

20.2.6.1 Tableau de bord

Le lien de surveillance ne s'affiche pas dans la page de la CMC

- Vérifiez si l'utilisateur dispose des droits adéquats.
- Assurez-vous que l'utilisateur est ajouté aux groupes Surveillance des utilisateurs ou Administrateur ou à tout autre groupe appartenant à ceux-ci.

Les indicateurs de performances clés ne sont pas visibles dans le tableau de bord de surveillance

- Vérifiez si les métriques requises sont visibles en choisissant *Propriétés du serveur* > *Métriques*.
- Assurez-vous que le CMS (Central Management Server) répond comme prévu.

20.2.6.2 Alertes

Impossible de recevoir des alertes sur la page Alertes

- Contrôlez si l'option *Activer Mes alertes* est sélectionnée dans les propriétés de l'application d'alertes.
- Assurez-vous d'avoir les droits d'accès adéquats pour recevoir des alertes.
- Vérifiez si les alertes récentes sont visibles sur le tableau de bord de surveillance.

> **Remarque**
>
> Vous pouvez envoyer un document Crystal Reports à l'ID de courrier électronique défini pour tester si le SMTP fonctionne comme prévu.

Réception des notifications par courrier électronique impossible

- Contrôlez si l'option *Activer l'adresse électronique* est sélectionnée dans les propriétés de l'application d'alertes.
- Vérifiez si les paramètres de l'adresse électronique destinée à recevoir les alertes sont appropriés.
- Vérifiez si le serveur SMTP fonctionne.
- Assurez-vous que l'instance de l'Adaptative Job Server est activée.
- Contrôlez les paramètres SMTP dans l'instance de l'Adaptative Job Server de destination.

20.2.6.3 Liste de veille

Impossible de recevoir des données d'historique pour la veille

- Vérifiez l'intervalle d'interrogation dans la page *Propriétés* de l'application de surveillance.
- Vérifiez le fichier de trace dans le dossier de journalisation.
- Vérifiez si l'heure système du serveur et du client est la même dans un fuseau horaire donné.

Une erreur s'est produite lors de l'extraction des données actives synchronisées

Contrôlez si l'instance du serveur de traitement adaptatif est en cours d'exécution.

L'onglet Liste de veille est désactivé.

- Vérifiez si le service de surveillance est en cours d'exécution.
- Vérifiez l'existence de messages d'erreur dans les journaux du service de surveillance.
- Vérifiez si les serveurs et leurs métriques sont visibles dans la jConsole.

20.2.6.4 Tests

Impossible de planifier des tests

- Vérifiez si l'instance de l'AdaptiveJobServer qui héberge le service de planification de la métrique est en cours d'exécution.
- Assurez-vous que le CUID du rapport utilisé pour les documents Crystal Reports et Web Intelligence est approprié.
- Assurez-vous que l'utilisateur dispose des droits d'administration ou est un membre du groupe Administrateur.
- Vérifiez si l'utilisateur dispose des droits adéquats pour ouvrir, actualiser et exporter les documents Crystal Reports ou Web Intelligence utilisés dans les tests correspondants.

Le statut de planification du test est En suspens.

- Vérifiez si l'instance ProbeSchedulingService est installée.
- Vérifiez si l'instance de l'AdaptiveJobServer qui héberge le service de planification de la métrique est en cours d'exécution.

Une erreur s'est produite lors de l'extraction des données de tendance à partir de la base de données

Vérifiez si l'instance AdaptiveProcessingServer est en cours de fonctionnement.

Echec de l'exécution de probeRun.bat

- Vérifiez si `java_home` est défini.
- Vérifiez si les bons paramètres sont entrés dans l'invite de commande.

> **Remarque**
>
> Saisissez `probeRun.bat -help` dans l'invite de commande pour vérifier si tous les paramètres sont appropriés.

20.2.6.5 Métriques

Les métriques d'hôte ne sont pas répertoriées

- Assurez-vous que SAPOSCOL est en cours d'exécution.
- Assurez-vous que l'option *Activer les métriques de l'hôte* est sélectionnée dans la page *Propriétés* de l'application de surveillance.
- Redémarrez l'instance AdaptiveProcessingServer pour rendre effectives les modifications.
- Assurez-vous que *Chemin d'accès à votre installation SAPOSCOL en binaire* est approprié.

Une erreur s'est produite lors de l'extraction du client

Vérifiez si l'instance AdaptiveProcessingServer est en cours de fonctionnement.

La valeur de métrique SAPOSCOL est zéro sur la page Métrique.

- Assurez-vous que SAPOSCOL est en cours d'exécution.
- Exécutez les commandes suivantes sur l'hôte où est installé SAPOSCOL :
  1. `saposcol -s` pour consulter le statut.
  2. `saposcol -m` pour obtenir un aperçu des données recueillies par SAPOSCOL.

20.2.6.6 Graphique

Les graphiques affichent différentes heures pour les modes direct et historique.

Assurez-vous que l'heure système du serveur et du client est la même dans un fuseau horaire donné.

20.3 Différence visuelle

La différence visuelle vous permet d'afficher les différences entre deux versions d'un fichier LCMBIAR ou d'un objet ou les deux. Vous pouvez utiliser cette fonction pour déterminer la différence entre des fichiers ou des objets afin de développer et de gérer différents types de rapports. Cette fonction fournit un statut de comparaison entre la version source et la version de destination. Par exemple, si une version précédente d'un rapport utilisateur est exacte et que la version actuelle est inexacte, vous pouvez comparer et analyser le fichier pour déterminer où réside le problème.

Page d'accueil

La page d'accueil de la fonction de différence visuelle contient les onglets et les volets suivants :

- Nouvelle comparaison - cet onglet permet de créer une comparaison entre des objets
- Recherche de comparaisons - ce champ permet de rechercher des objets déjà comparés
- Volet Comparaisons - ce volet répertorie les onglets de filtres et de différences
- Comparaisons : volet Différences - ce volet répertorie les objets comparés avec le nom de la comparaison, la date et l'heure, ainsi que le statut des différences

20.3.1 Comparaison d'objets ou de fichiers à l'aide de la différence visuelle

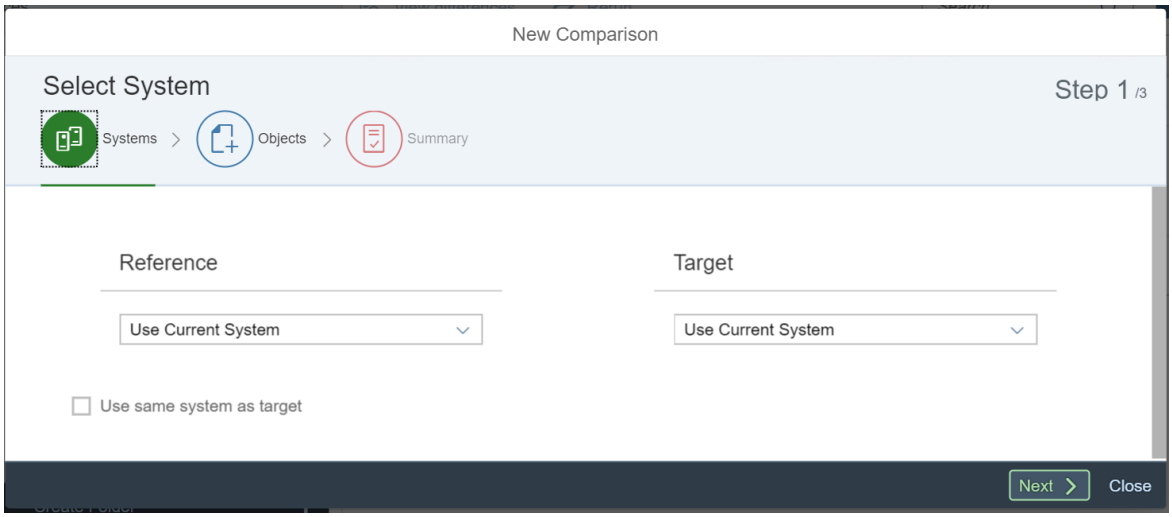
Pour comparer des fichiers à l'aide de la différence visuelle, procédez comme suit :

1. Connectez-vous à l'application CMC.
2. Sur la page d'accueil de la CMC, dans l'onglet *Gérer*, cliquez sur le lien *Différence visuelle*.
   La page Différence visuelle s'affiche. Les fichiers comparés sont stockés dans le dossier Différences ou dans un sous-dossier créé par l'utilisateur, le cas échéant.

   > **Remarque**
   >
   > Pour créer un nouveau sous-dossier, sélectionnez Create Folder +.

3. Sélectionnez + pour créer une nouvelle comparaison.

L'assistant *Nouvelle comparaison* s'affiche.



4. Sélectionnez le système de *Référence* et le système *Cible* dans la liste déroulante.

   Vous pouvez vous connecter à l'un quelconque des systèmes de référence et des systèmes cibles suivants :

   > **Remarque**
   >
   > Si un objet est ajouté dans le système de gestion des versions (VMS), vous aurez la possibilité de sélectionner des versions dans l'étape suivante.

   - CMS
   - Système de fichiers local
5. Dans l'écran *Sélection d'objets* , recherchez et sélectionnez l'objet ou un fichier dans le système de *Référence* et le système *Cible*.
6. Modifiez le *Nom de la comparaison*, si nécessaire.
7. Sélectionnez *Comparer* pour comparer les objets.

   > **Remarque**
   >
   > - Vous pouvez vérifier les différences en sélectionnant la comparaison, puis *Afficher les différences*. Les différences sont mises en surbrillance en orange et les objets manquants en rouge.
   > - Vous pouvez exécuter la comparaison à nouveau en sélectionnant la comparaison, puis *Réexécuter*

   Le processus de comparaison démarre immédiatement.

   Vous pouvez également utiliser l'option de filtre pour afficher les objets comparés par type, avec leurs différences ou leurs attributs communs.

20.3.2 Comparaison d'objets ou de fichiers à l'aide du système de gestion des versions

Dans un système de gestion des versions, vous pouvez comparer des dossiers ou des travaux de gestion des promotions à l'aide de l'option Différence visuelle.

Pour comparer les objets dans un système de gestion des versions, procédez comme suit :

1. Connectez-vous à l'application de la CMC.
2. Sur la page d'accueil de la CMC, dans l'onglet *Gérer*, cliquez sur le lien *Différence visuelle*.
   La page Différence visuelle s'affiche. Les fichiers comparés sont stockés dans le dossier Différences ou dans un sous-dossier créé par l'utilisateur, le cas échéant.

   > **Remarque**
   >
   > Pour créer un nouveau sous-dossier, cliquez sur l'icône Dossier.

3. Cliquez sur *Nouvelle comparaison*.
   L'écran *Différence visuelle - Comparaisons* s'affiche.
4. Sélectionnez *Se connecter au VMS* dans *Sélectionner un système* sous Référence.
5. Saisissez les références de connexion au VMS et cliquez sur *Connexion*.
   La boîte de dialogue *Différence visuelle - Sélection automatique du système cible* s'affiche.
6. Cliquez sur *Non* pour définir un autre système cible et sur*Oui* pour définir le système cible de la même manière que le système de référence.
7. Cliquez sur *Parcourir* pour sélectionner les objets ou les travaux que vous souhaitez comparer à la fois dans le système de référence et dans le système cible.
8. Cliquez sur *Ajouter*.
   Les objets sélectionnés pour la comparaison sont répertoriés dans le volet *Nouvelle comparaison*.
   Vous pouvez comparer les fichiers immédiatement ou reporter la comparaison à plus tard. Pour comparer les fichiers, passez à l'étape suivante.
9. Cliquez sur *Comparer* pour comparer les travaux ou les dossiers.
   Le processus de comparaison démarre immédiatement et les différences, le cas échéant, s'affichent dans le *visualiseur Différence visuelle*. Les différences sont mises en surbrillance en orange et les objets manquants en rouge.
   Vous pouvez également utiliser l'option de filtre pour afficher les objets comparés par type, avec leurs différences ou leurs attributs communs.
10. Cliquez sur *Enregistrer* pour enregistrer le rapport de différences.
11. Spécifiez l'emplacement dans lequel vous souhaitez enregistrer le rapport, puis cliquez sur *OK*.

20.4 Autorisation des éléments HTML

Pour que les utilisateurs puissent bénéficier des fonctionnalités des éléments HTML de confiance et protéger leur organisation contre tous les autres éléments, spécifiez une liste des éléments HTML autorisés.

Lorsqu'un utilisateur ouvre un document qui contient une cellule avec la propriété Lu au format HTML ou Lire comme lien hypertexte dans le visualiseur HTML Web Intelligence ou dans le visualiseur interactif, le visualiseur peut interpréter le code HTML. Ce comportement varie selon la définition du rendu de ces cellules dans les propriétés d'affichage Web Intelligence et selon les éléments HTML que vous avez autorisés.

Lorsque vous spécifiez les éléments HTML autorisés et qu'un document en mode Lecture contient un élément non autorisé, seul le texte de l'élément est conservé et non la balise ou les attributs de l'élément. Dans un document qui contient un élément autorisé et des attributs autorisés et non autorisés, seuls l'élément et les attributs autorisés sont conservés.

Pour autoriser uniquement certains éléments HTML spécifiques, dans les propriétés d'affichage Web Intelligence pour JavaScript, sélectionnez *Activer uniquement les éléments HTML définis dans la page des éléments HTML éléments* et spécifiez les éléments HTML dans la page *Éléments HTML éléments*.

Par défaut, seuls les éléments HTML requis pour assurer le fonctionnement correct de Web Intelligence sont autorisés. Vous pouvez ajouter ou supprimer des éléments dans la liste par défaut.

> ⚠ Attention
>
> - Web Intelligence active le code Javascript/HTML intégré dans les cellules du document grâce à ses fonctionnalités de formule.
> Ce code peut être activé ou désactivé dans la Central Management Console. Cependant, en autorisant JavaScript, les HTML et les liens hypertexte, vous reconnaissez votre risque qu'exposition à Cross-Site Scripting. Cross-Site Scripting permet aux attaquants de modifier des sites Web ou d'exécuter du code sur d'autres systèmes. Cette vulnérabilité affecte des produits tels que les navigateurs Internet lorsqu'ils exécutent des scripts. La majorité des attaques Cross-Site Scripting résultent d'une programmation non sécurisée sur le système cible.
> - Le code peut être ajusté à l'aide d'une liste de balises et d'attributs HTML autorisés. Toutefois, SAP n'est pas responsable de la compatibilité de ce code et de ses éventuels effets secondaires. Il est possible, par exemple, que votre code nécessite quelques adaptations en raison de mises à jour du navigateur, de la prise en charge de la version Javascript ou du mode d'intégration dynamique du code dans la page Web. D'un point de vue technique, à partir de la version 4.3, l'application fonctionne comme une application monopage. Il n'existe pas de séparation technique entre le rapport et la page Web globale. Le code nécessitera peut-être des ajustements pour pouvoir s'exécuter dans ce nouveau contexte.
> - La suppression d'éléments dans la liste par défaut altère les fonctions Web Intelligence, c'est pourquoi elle est déconseillée.

Vous pouvez autoriser :

- L'élément `<a>` avec l'attribut `href` pour ajouter une référence.
- Un ensemble d'attributs pour tous les éléments dans la liste en associant l'élément * avec la liste d'attributs.
  Vous ne pouvez pas autoriser la totalité des attributs associés à un élément.
- Les éléments qui contiennent peut-être du code JavaScript, tels que `<script>`, `<onClick>` et `<onMouseEnter>`.
  Vous ne pouvez pas autoriser les mots clés JavaScript.

Exemple

Éléments HTML autorisés

Élément	Attributs
*	style, class, id
img	src

Élément	Attributs
link	ref

Le tableau ci-dessous indique le mode d'affichage des éléments HTML des documents dans Web Intelligence, suite aux autorisations.

Impact des autorisations des éléments HTML

Code HTML d'origine	Code HTML final	Explication
`<link title="SAP" ref="www.sap.com">`	`<link ref="www.sap.com">`	L'élément `<link>` et l'attribut `ref` sont autorisés, c'est pourquoi le lien s'affiche sous forme de lien actif dans le document. L'attribut `title` n'est pas autorisé, c'est pourquoi il est supprimé du document.
`<img src="datasource" id="I1">`	`<img src="datasource" id="I1">`	L'élément `<img>` et l'attribut `src` associé sont autorisés et l'attribut `id` est autorisé pour tous les éléments, c'est pourquoi le code HTML d'origine est conservé.
`<div title="datasource" id="D1">`	Supprimé	L'élément `<div>` n'est pas autorisé, c'est pourquoi l'élément ainsi que les attributs associés sont supprimés du document.
`<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>`	`...as shown in the picture below:<img src="../picture.jpg">`	L'élément `<p>` n'est pas autorisé, c'est pourquoi il est supprimé. Seul le texte inclus dans l'élément `<p>` est conservé. L'élément `<img>` et l'attribut `src` associé sont autorisés, c'est pourquoi ils sont conservés. L'attribut `alt` n'est pas autorisé, c'est pourquoi il est supprimé du document.

Pour modifier les paramètres d'affichage de Web Intelligence [page 724]Pour modifier la liste des éléments HTML autorisés [page 851]

20.4.1 Pour modifier la liste des éléments HTML autorisés

Spécifiez les éléments HTML que vous souhaitez autoriser et activez la protection contre les éléments malveillants en modifiant la liste des éléments HTML autorisés.

Web Intelligence autorise uniquement les éléments que vous définissez à la page *Éléments HTML autorisés* lorsque la propriété d'affichage du code JavaScript *Activer uniquement les éléments HTML définis dans la page des éléments HTML éléments* est active dans les propriétés Web Intelligence.

1. Accédez à CMC et sélectionnez *Studio d'administration BI*.
2. Dans la *Page d'accueil de la Central Management Console*, faites défiler jusqu'à *Éléments HTML*.
3. Modifiez la liste en procédant comme décrit dans le tableau ci-dessous :

Modification	Étapes
Pour ajouter un élément	Cliquez sur *Ajouter un nouvel élément* et saisissez l'élément et les attributs associés à autoriser. **Remarque** • Pour autoriser des attributs spécifiques pour tous les éléments HTML, entrez * comme élément et ajoutez les attributs. • Lorsque vous tentez d'ajouter un élément HTML qui figure déjà dans la liste, seuls les nouveaux attributs pour l'élément sont ajoutés à la liste.
Pour modifier un élément	Cliquez sur l'élément, puis sur *Modifier l'élément sélectionné*.
Pour supprimer un élément	Cliquez sur l'élément, puis sur *Supprimer l'élément sélectionné*.
Pour restaurer la liste par défaut des éléments HTML autorisés	Cliquez sur *Réinitialiser*. La liste par défaut contient uniquement les éléments requis pour assurer le fonctionnent correct de Web Intelligence.

21 Reporting du CMS

21.1 Reporting du CMS

Avant de commencer à utiliser le reporting sur le CMS, vous devez comprendre fondamentalement les concepts suivants :

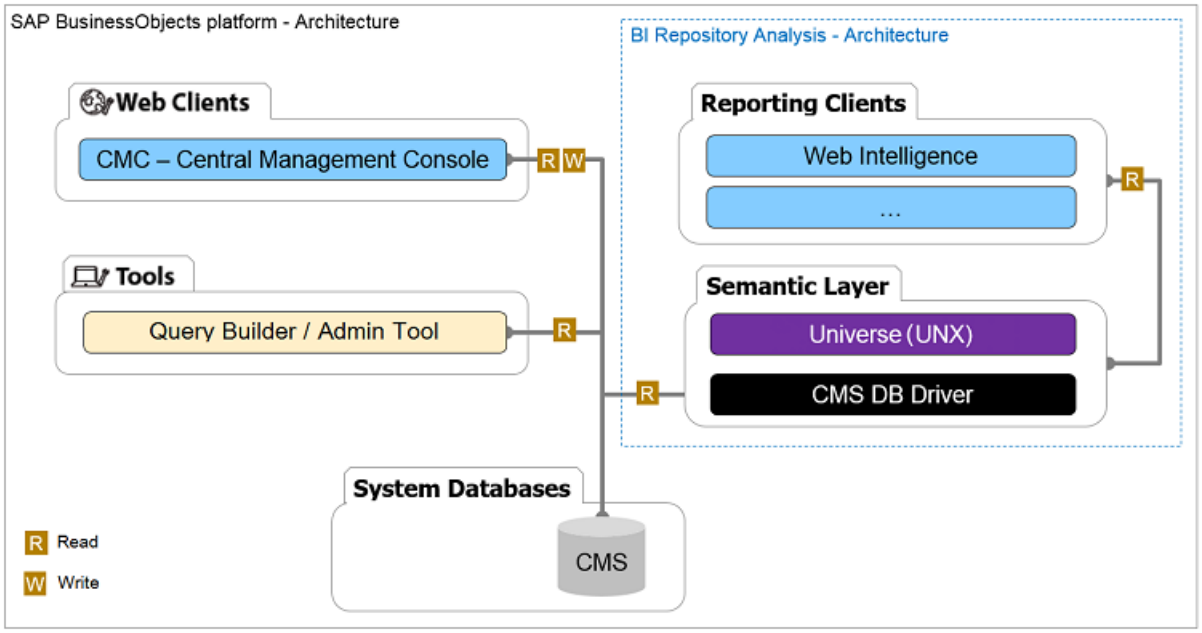
- Architecture de la plateforme SAP BusinessObjects
- Structure de la base de données système du CMS
- Propriétés et relations des InfoObjects

Informations associées

Architecture de la plateforme SAP BusinessObjects [page 852]
Structure de la base de données système du CMS [page 853]

21.1.1 Architecture de la plateforme SAP BusinessObjects

Ce schéma est conçu pour vous aider à comprendre l'architecture de la plateforme SAP BusinessObjects.



Le tableau suivant donne de plus amples informations sur les composants de la plateforme SAP BusinessObjects.

Composants de la plateforme SAP BusinessObjects

Composants	Description
Central Management Console (CMC)	Outil basé sur le Web que vous utilisez pour configurer les paramètres de sécurité et pour gérer les éléments suivants : • Utilisateur • Contenu • Serveur
Base de données système du CMS	Base de données qui enregistre les informations suivantes de la plateforme de BI : • Utilisateur • Serveur • Document • Configuration • Authentification La base de données système du CMS est gérée par le Central Management Server (CMS) et peut être appelée également référentiel système.
Générateur de requêtes (également appelé outil d'administration)	Outil basé sur le Web que vous utilisez pour interroger le référentiel BusinessObjects et obtenir les informations requises qui ne sont pas disponibles dans la CMC.
Analyse du référentiel BI	Cette solution utilise la couche sémantique de la plateforme de BI, l'univers (UNX) et le pilote de base de données CMS pour interroger le CMS.

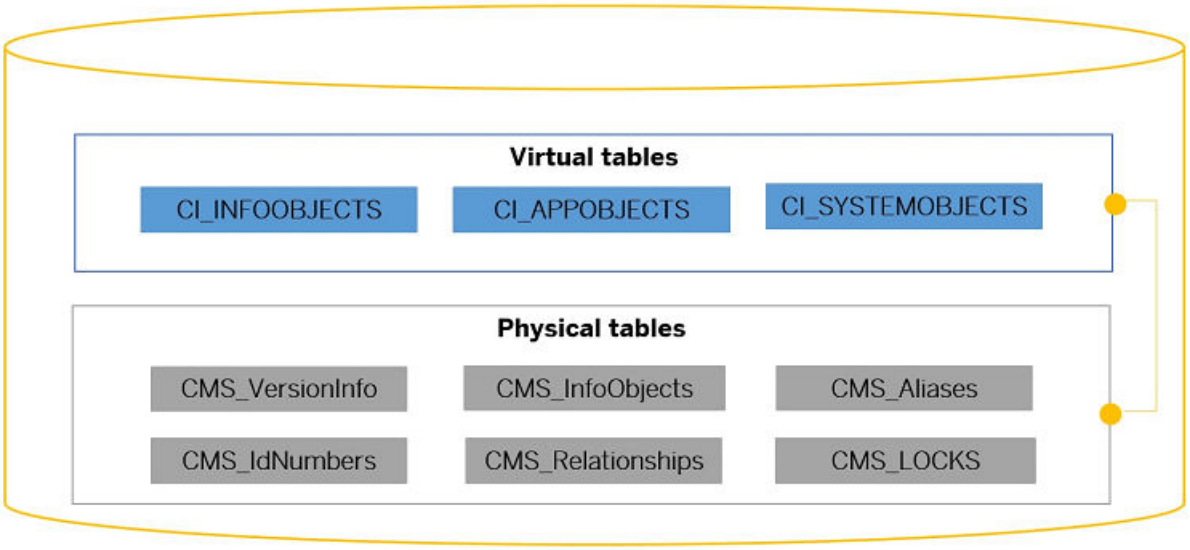
21.1.2 Structure de la base de données système du CMS

La base de données système du CMS est gérée par le Central Management Server (CMS) et peut être appelée également référentiel système. Le système CMS est une base de données qui stocke les informations de la plateforme de BI sous la forme d'InfoObjects.

La base de données système du CMS comprend deux types de tables :

- Table de base de données physique : les métadonnées du CMS sont stockées dans les tables de base de données physiques.
- Table virtuelle : le serveur CMS parcourt les InfoObjects dans les tables virtuelles.

Le schéma suivant offre un aperçu sur la structure de la base de données système du CMS.



Pour en savoir plus sur la structure de la base de données système du CMS, voir les rubriques associées.

Informations associées

Tables de base de données physiques [page 854]
Tables virtuelles [page 855]

21.1.2.1 Tables de base de données physiques

Les métadonnées du CMS sont stockées dans six tables de base de données physiques.

Tables de base de données physiques

Table physique	Description
CMS_VersionInfo	Inclut la version actuelle de BusinessObjects Enterprise (BOE)
CMS_InfoObjects	Table principale dans le référentiel système. Un InfoObject est stocké par ligne.
CMS_Aliases	Mappe le ou les alias utilisateur à l'ID utilisateur correspondant. Un utilisateur possède un alias pour chaque domaine sécurité dont il est membre. Cependant, un utilisateur ne possède qu'un seul ID utilisateur.
CMS_IdNumbers	Génère des ID d'objet et des ID de type uniques.

Table physique	Description
CMS_Relationships	Stocke les relations entre les InfoObjects.
CMS_LOCKS	Table auxiliaire de CMS_RELATIONS

21.1.2.2 Tables virtuelles

Le serveur CMS parcourt les InfoObjects dans trois tables virtuelles.

Tables virtuelles

Table virtuelle	Description
Table des InfoObjects	Inclut les InfoObjects que l'utilisateur final peut afficher, tels que : • Documents de rapport • Programmes • Raccourcis • Dossiers • Catégories • Boîtes de réception
Table d'AppObjects	Inclut les InfoObjects que les documents utilisent, tels que : • Univers • Connexions • Syntaxes des arguments
Table d'objets système	Inclut les InfoObjects que la plateforme de BI utilise pour fonctionner, tels que : • Utilisateurs • Groupes • Clés de licence

21.1.3 À propos des InfoObjects

Avant d'interroger les métadonnées des InfoObjects, vous devez comprendre clairement les concepts suivants :

- Propriétés d'InfoObject
- Relations entre les InfoObjects

Si vous comprenez la façon dont sont organisés les InfoObjects dans le référentiel CMS, vous serez en mesure de parcourir le référentiel rapidement et facilement et de résoudre les problèmes liés au référentiel CMS.

Informations associées

Propriétés d'InfoObject [page 856]
Relations entre les InfoObjects [page 856]

21.1.3.1 Propriétés d'InfoObject

Le tableau suivant énumère les principales propriétés des InfoObjects avec leur description.

Propriétés d'InfoObject

Propriétés d'InfoObject	Description
SI_NAME	Nom de l'objet
SI_KIND	Type d'objet
SI_OWNER	Nom d'utilisateur du propriétaire
SI_OWNERID	ID utilisateur du propriétaire
SI_CHILDREN	Nombre d'enfants
SI_CUID	Identifiants uniques de cluster qui identifient de façon unique un InfoObject
SI_UNIVERSE	Univers (UNV) utilisés par le document

21.1.3.2 Relations entre les InfoObjects

Les InfoObjects sont organisés selon trois hiérarchies :

- Hiérarchie de dossiers
- Hiérarchie d'utilisateur/de groupe d'utilisateurs
- Hiérarchie de serveur/de groupe de serveurs

Le CMS et les applications client utilisent la hiérarchie de dossiers pour parcourir les InfoObjects.

Pour en savoir plus sur les relations entre les InfoObjects, voir les rubriques associées.

Informations associées

Hiérarchie de dossiers [page 857]
Dossiers racine [page 857]

21.1.3.2.1 Hiérarchie de dossiers

La hiérarchie de dossiers est une liste horizontale créée à partir d'un parent d'InfoObject. Tous les InfoObjects doivent avoir un parent unique défini dans la propriété SI_PARENTID.

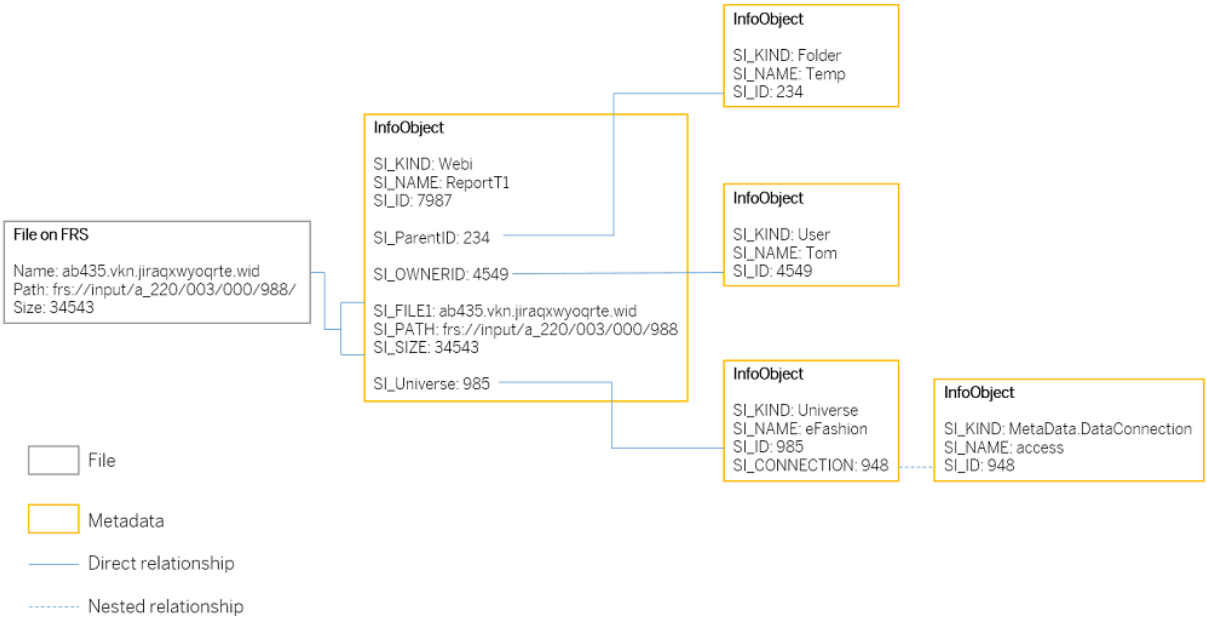
Le CMS utilise la propriété d'ID parent pour créer une hiérarchie de dossiers qui est virtuelle. En effet, la hiérarchie ne reflète pas la façon dont les InfoObjects sont stockés dans le référentiel.

21.1.3.2.2 Dossiers racine

Le dossier supérieur dans la hiérarchie du référentiel CMS désigne les dossiers de cluster du CMS. Les dossiers racine se trouvent au niveau inférieur au dossier de cluster du CMS. Les dossiers racine sont virtuels et ne correspondent à aucun élément sur le système de fichiers.

Les InfoObjects sont organisés en dossiers racine pour le CMS et les applications client, de sorte qu'ils puissent être retrouvés facilement et rapidement. Par exemple, les applications client peuvent parcourir la collection d'InfoObjects en utilisant d'abord le dossier racine des InfoObjects, puis la propriété d'ID parent et les propriétés d'ID enfant. En général, vous trouverez le même type d'InfoObject dans un dossier racine.

Le diagramme suivant vous aide à mieux comprendre les relations entre les InfoObjects.



Comme vous pouvez le voir, de par leur structure, les InfoObjects peuvent avoir une infinité de relations et de relations imbriquées.

21.2 Aperçu du reporting du CMS

En tant qu'administrateur, vous devez comprendre et optimiser l'utilisation de la plateforme Business Intelligence. Le kit d'exemples de reporting du CMS inclut le pilote de base de données du CMS, qui vous

permet de visualiser et de créer des rapports sur les objets de métadonnées de la base de données du CMS. Vous pouvez maintenant utiliser un univers et les clients du reporting natifs pour interroger les objets de métadonnées de la base de données du référentiel CMS. Ces objets de métadonnées incluent des informations sur la plateforme Business Intelligence, telles que :

- Connexions
- Documents
- Planifications
- Univers
- Utilisateurs

Vous pouvez importer l'exemple de reporting du CMS qui contient les objets prédéfinis pour vous aider à créer des rapports et des tableaux de bord en utilisant les analyses de données et les applications de reporting de SAP BusinessObjects suivantes :

- SAP BusinessObjects Web Intelligence
- SAP Crystal Reports pour Enterprise

Pour un démarrage facile et rapide du reporting sur le CMS, vous pouvez travailler avec le kit d'exemples de reporting du CMS. Voici les étapes principales pour la création d'un rapport du CMS :

- Importez l'exemple de reporting du CMS : Vous devez utiliser Gestion des promotions dans la CMC pour importer l'exemple de reporting du CMS.
- Créez un rapport du CMS : avec SAP BusinessObjects Web Intelligence, vous pouvez créer un rapport du CMS en utilisant l'exemple d'univers du CMS comme source de données.

Voir les informations associées pour une procédure de bout en bout qui vous offre une vue d'ensemble plus détaillée du processus de création.

Informations associées

Kit d'exemples de reporting du CMS
Création d'un rapport du CMS
Importation du kit d'exemples de reporting du CMS avec l'outil de gestion des promotions [page 860]

21.3 Connexion de la base de données du CMS

Utilisez un pilote de base de données du CMS pour créer une connexion sécurisée à la base de données du CMS. Vous pouvez également utiliser la connexion par défaut disponible dans l'exemple de reporting du CMS ou vous pouvez créer votre propre connexion à la base de données du CMS.

Pour établir une connexion à la base de données du CMS, vous devez utiliser une connexion relationnelle. Le tableau suivant décrit les paramètres d'une connexion relationnelle.

Paramètres pour une connexion relationnelle

Paramètre	Description
Mode d'authentification	Méthode utilisée pour authentifier les références de connexion de l'utilisateur lors de l'accès à la source de données : • *Utiliser le nom d'utilisateur, le mot de passe et l'ID système spécifiés* : utilise les paramètres *Nom d'utilisateur* et *Mot de passe* définis pour la connexion. Vous pouvez accéder à la source de données depuis un système sur site ou un système distant. **Remarque** Assurez-vous que l'utilisateur dispose des droits pour afficher le contenu de cette section. • *Utiliser le jeton de la session* : utilise la session de l'utilisateur actuel. Vous pouvez uniquement voir le contenu que vous êtes autorisé à afficher et à utiliser. Vous pouvez uniquement accéder à la source de données depuis un système sur site. **Remarque** Pour des questions de sécurité, ce mode d'authentification est l'option recommandée.
ID système	Nom du CMS si le *Mode d'authentification* est *Utiliser le nom d'utilisateur et le mot de passe spécifiés*.
Nom d'utilisateur	Nom d'utilisateur permettant d'accéder à la source de données si le *Mode d'authentification* est *Utiliser le nom d'utilisateur et le mot de passe spécifiés*.
Mot de passe	Mot de passe permettant d'accéder à la source de données si le *Mode d'authentification* est *Utiliser le nom d'utilisateur et le mot de passe spécifiés*.

21.4 Kit d'exemples de reporting du CMS

Vous devez utiliser le kit d'exemples de reporting du CMS pour démarrer la création de documents pour le reporting du CMS. Le pilote de la base de données du CMS est intégré sur la plateforme Business Intelligence et l'exemple de reporting du CMS est disponible à l'emplacement suivant :

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`.

Cet exemple comprend :

- Connexion (fichier .cns de la base de données système du CMS de la plateforme de BI)
- Univers (fichier .unx de la base de données système du CMS de la plateforme de BI)
- Exemples Web Intelligence

Vous pouvez trouver plus d'informations sur le reporting du CMS sur le réseau de la communauté SAP.

Informations associées

Importation du kit d'exemples de reporting du CMS avec l'outil de gestion des promotions [page 860]

21.4.1 Importation du kit d'exemples de reporting du CMS avec l'outil de gestion des promotions

Avant de commencer, assurez-vous d'avoir accès à l'exemple de reporting du CMS qui se trouve à l'emplacement suivant :

```
<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI
on BI
```

Vous utilisez l'outil de gestion des promotions dans la Central Management Console (CMC) pour importer l'exemple de reporting du CMS.

1. Dans la Central Management Console, cliquez sur *Gestion des promotions*.
2. Cliquez sur *Importer* > *Fichier d'importation*.
3. Sélectionnez *Système de fichiers*.
4. Cliquez sur *Choisir un fichier* pour sélectionner l'exemple.
5. Dans le volet *Nouveau travail*, sélectionnez *Connexion à un nouveau CMS* pour le champ *Destination*.
6. Saisissez les paramètres de connexion, puis cliquez sur *Connexion* > *Créer*.
7. Dans le volet *Travaux de promotion*, cliquez avec le bouton droit de la souris, puis sélectionnez *Promouvoir*.
8. Dans la boîte de dialogue *Promouvoir*, cliquez sur *Promouvoir*.

Si le *Statut de la promotion* de l'exemple de reporting du CMS est *Réussite*, vous avez correctement importé l'exemple vers votre système Business Intelligence 4.2. Pour savoir comment utiliser l'exemple d'univers pour le reporting du CMS, voir la rubrique associée.

Informations associées

Kit d'exemples de reporting du CMS [page 859]

21.4.2 Exemple d'univers du CMS

L'exemple d'univers du CMS inclut un univers prédéfini qui prend en charge des scénarios courants de reporting. Selon vos besoins d'analyse et de reporting, vous pouvez modifier et améliorer l'univers prédéfini. Vous pouvez également rechercher une liste de requêtes prédéfinies dans le volet *Requêtes*. Ces requêtes peuvent servir de tutoriels pour les fonctionnalités d'univers.

Vous trouverez les requêtes les plus utiles et leur signification dans le tableau suivant.

Requêtes utiles à exécuter sur l'univers du CMS

Requête	Description
Détail-Relation-Utilisateur-Exemple	Permet de voir à quel groupe appartient un utilisateur.
CheminDossier-Exemple (univers)	Permet de rechercher l'emplacement d'un univers.
Relations-InfoPlanifiées-Exemple	Permet de visualiser les actions planifiées par les utilisateurs.
Propriétés-QT-Exemple avec filtre (serveur)	Permet de visualiser les propriétés d'un InfoObject.

21.4.3 Extension de l'exemple d'univers du CMS

Vous pouvez créer un univers lié pour étendre l'exemple d'univers du CMS. Un univers lié est un univers .UNX qui contient un lien vers un univers de référence désigné dans le CMS.

Dans ce cas, l'exemple d'univers du CMS agit comme un univers de référence, de manière à ce que l'univers lié puisse utiliser la fondation de données et la couche de gestion de l'exemple d'univers du CMS en tant que blocs de base préfabriqués. Une fois l'univers lié créé, vous pouvez enregistrer sa fondation de données et sa couche de gestion héritées de l'exemple d'univers du CMS sous de nouveaux fichiers, afin qu'elles aient un cycle de vie indépendant de l'exemple d'univers du CMS.

Vous pouvez utiliser la connexion à la base de données du CMS de l'exemple d'univers du CMS ou une autre connexion compatible avec la base de données du CMS.

Vous pouvez ajouter des tables, créer des jointures reliant des tables de fondation de données de référence avec les nouvelles et ajouter de nouveaux composants à la couche de gestion de la même manière que pour tout autre univers. Toutes les modifications de composants de référence sont automatiquement propagées à l'univers lié lorsqu'il est vérifié dans le CMS.

21.5 Création d'un rapport sur le CMS

Avec SAP BusinessObjects Web Intelligence, vous pouvez créer un rapport du CMS en utilisant l'exemple d'univers du CMS comme source de données.

1. Ouvrez Web Intelligence et cliquez sur l'icône *Nouveau* dans la barre d'outils *Fichier*.

2. Sélectionnez l'exemple d'univers du CMS.

   Avec Web Intelligence Rich Client, cliquez sur *Sélectionner*.

   L'*Éditeur de requête* s'ouvre.
3. Sélectionnez et faites glisser dans le volet *Objets du résultat* les dimensions et les indicateurs à inclure dans la requête.
4. Sélectionnez les objets pour lesquels vous souhaitez définir des filtres de requête, puis faites-les glisser vers le volet *Filtres de la requête*. Pour créer un filtre express sur un objet, sélectionnez ce dernier dans le volet *Objets du résultat*, puis cliquez sur l'icône *Ajouter un filtre express* dans la barre d'outils *Objets du résultat*.
5. Cliquez sur *Exécuter la requête*.

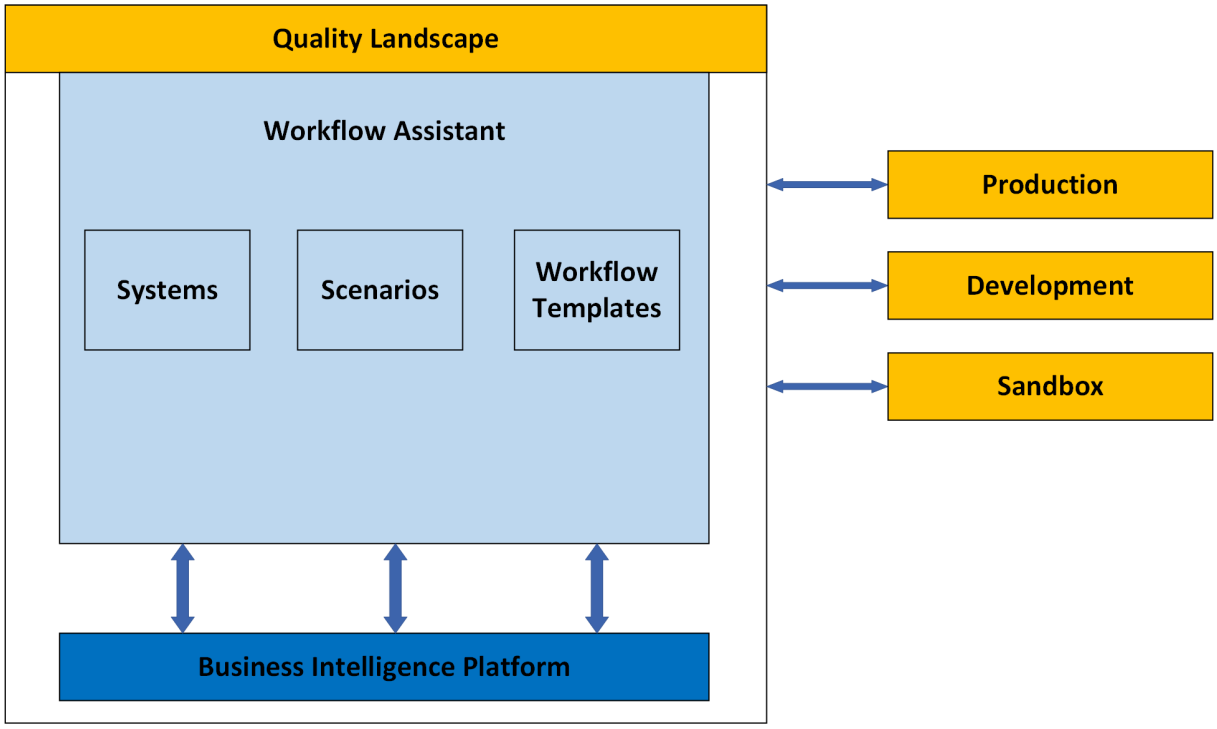
22 Assistant du workflow

La structure d'automatisation et les services d'agent ont fusionné en un service unique appelé Assistant du workflow. L'Assistant du workflow est une application de la CMC (Central Management Console) pour l'administration des systèmes BI et l'automatisation des tâches BI.

> **Remarque**
>
> La fonctionnalité Structure d'automatisation dans la console d'administration BI est désormais assurée par le biais de l'Assistant du workflow. L'URL de la console d'administration BI `(http://<NomSystème>:<N°Port>/BOE/BIAdminConsole)` et le service de file d'attente de messages sont désormais obsolètes.

L'Assistant du workflow affiche le contenu sous forme d'onglets : *Scénarios*, *Modèles de workflow* et *Systèmes*. Dans ces onglets, vous pouvez explorer en avant la section pertinente pour obtenir des informations et des fonctions plus détaillées.

L'Assistant du workflow implémente un concept basé sur les rôles pour que les utilisateurs aient uniquement accès aux onglets pour lesquels ils disposent des autorisations requises.



À propos des systèmes

Un système désigne un ou plusieurs ordinateurs BI au(x)quel(s) vous êtes autorisé à accéder. Gestion du système est une application qui vous permet d'accéder à vos infrastructures BI et de les gérer de

façon centralisée. Pour pouvoir utiliser l'Assistant du workflow, vous devez enregistrer au préalable vos infrastructures BI à l'aide de l'application Gestion du système.

À propos de l'Assistant du workflow

L'Assistant du workflow permet de simplifier les tâches BI complexes et répétitives.

> **Exemple**
>
> Imaginons que vous deviez effectuer les tâches BI suivantes dans l'ordre :
>
> 1. Connexion à la plateforme de BI.
> 2. Modification de la source de certains documents Web Intelligence de `.unv` à `.unx`.
> 3. Actualisation de ces documents Web Intelligence.
> 4. Déconnexion de la plateforme de BI.

L'effort manuel est réduit avec l'Assistant du workflow. Vous pouvez créer un scénario à l'aide de modèles de tâche et de workflow, enregistrer ce scénario, l'exécuter et en afficher les résultats.

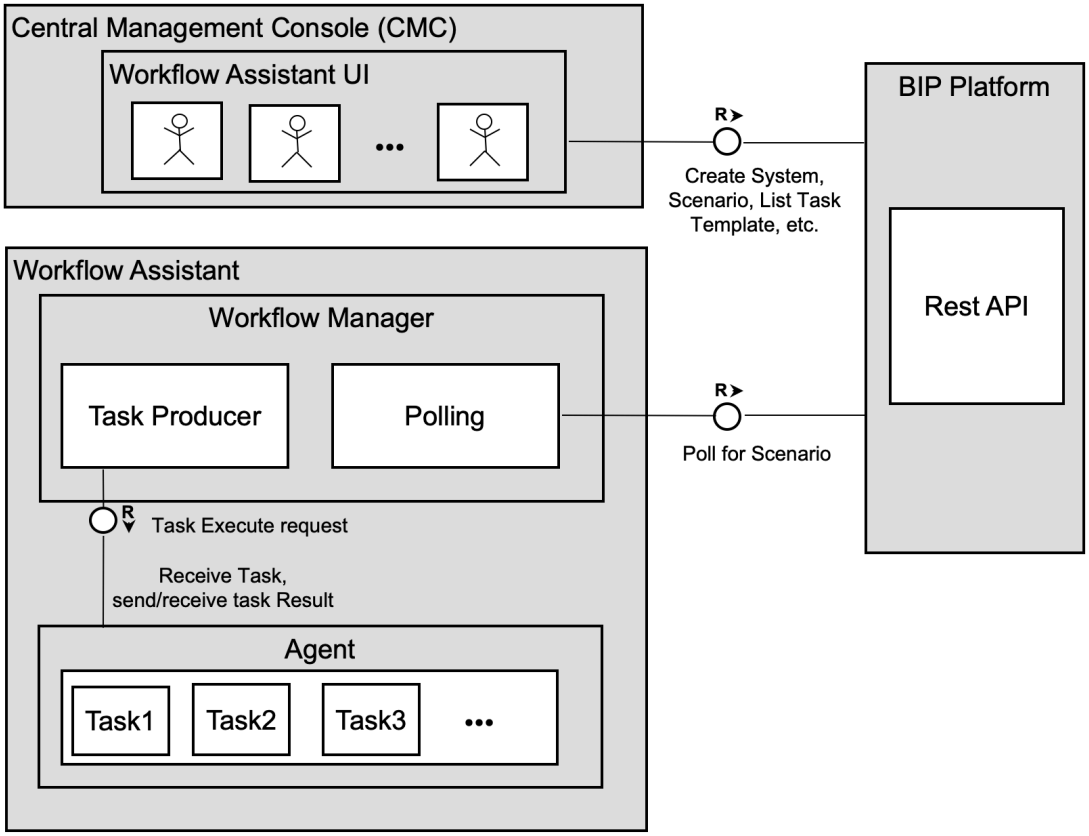
22.1 Public visé

Ce guide est destiné à certains utilisateurs de la plateforme de Business Intelligence (BI) et à certains développeurs de la plateforme de BI.

- Les utilisateurs de la plateforme de BI qui utilisent ce guide doivent disposer des droits d'accès à la CMC (Central Management Console) et à l'Assistant du workflow. Ces utilisateurs assument le rôle d'administrateurs ou d'administrateurs délégués.
- Les développeurs de la plateforme de BI qui utilisent ce guide doivent être habitués à travailler sur des SDK Java et être capables de créer des schémas JSON personnalisés à l'aide du SDK de modèle de tâche pour répondre à des besoins spécifiques.

22.2 Compréhension de l'architecture

Le diagramme ci-dessous illustre l'architecture de l'Assistant du workflow et les interconnexions entre ses composants.



Glossaire des termes utilisés dans le diagramme ci-dessus :

Terme	Définition
IU de l'Assistant du workflow	Il s'agit d'une interface utilisateur (IU) pour créer des modèles de workflow et des scénarios qui peuvent être exécutés sur un système donné.
Gestionnaire de workflow	Un gestionnaire de workflow interroge les scénarios de la plateforme, gère l'exécution des scénarios et enregistre les résultats.
Agent	Il s'agit d'un processus léger qui exécute les tâches dans les scénarios.

22.3 Glossaire

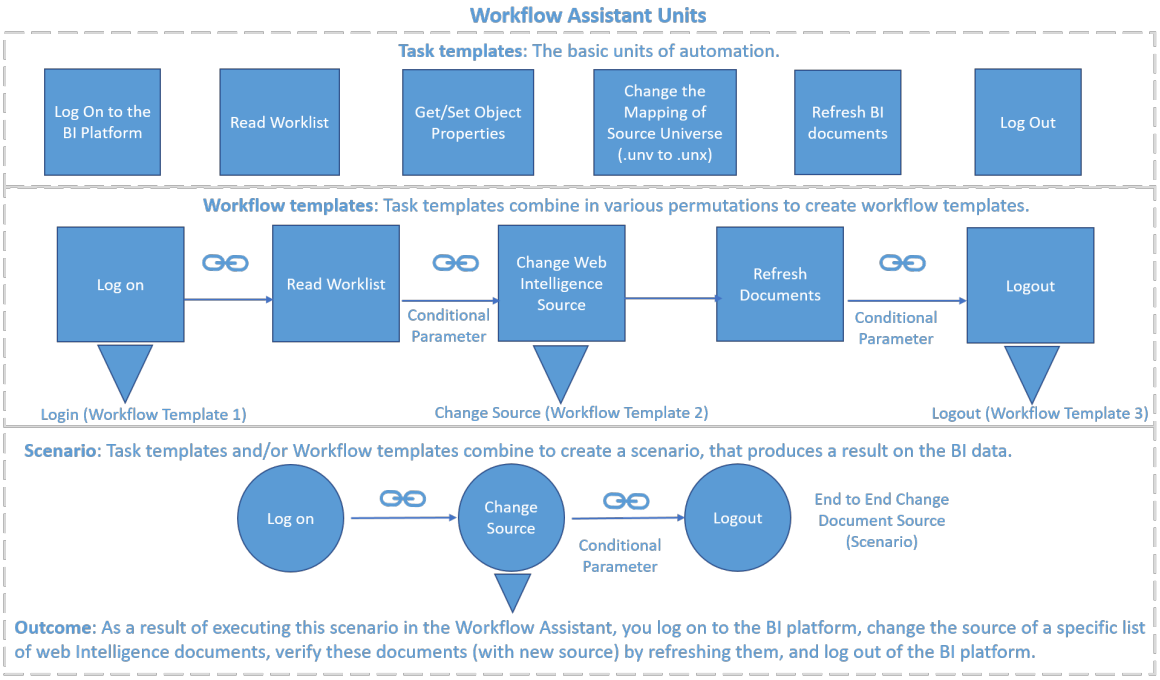
L'Assistant du workflow s'accompagne de son propre vocabulaire spécialisé.

Termes fréquemment utilisés dans l'Assistant du workflow

Terme	Définition
Modèle de tâche standard	Unité de base d'automatisation fournie par défaut dans l'application. Ces unités peuvent être utilisées dans des scénarios ou des modèles de workflow. Il peut s'agir, par exemple, d'une simple tâche, comme se connecter à la plateforme de BI, actualiser des documents BI, lire des données, modifier le mappage d'univers source des documents Web Intelligence (de `unv` à `unx`), ajouter des utilisateurs ou se déconnecter.
Modèle de tâche personnalisé	Modèle de tâche (unité de base d'automatisation) créé par les développeurs pour des besoins personnalisés. **⚠ Restriction** Vous ne pouvez pas créer de modèle de tâche personnalisé via l'IU de l'Assistant du workflow. Le SDK de modèle de tâche est requis.
Modèle de workflow	Groupe logique de modèles de tâche organisés dans la séquence requise pour atteindre le résultat d'un workflow.
Modèle de workflow standard	Modèles de workflow prédéfinis dans l'Assistant du workflow. Les administrateurs peuvent facilement utiliser des modèles de workflow standard lors de la création de scénarios pour leurs divers besoins d'automatisation BI.
Modèle de workflow personnalisé	Modèle de workflow créé par les administrateurs pour leurs besoins personnalisés. Sa création a lieu dans l'Assistant du workflow, en regroupant des modèles de tâche standard ou personnalisés.
Scénario	Entité exécutable créée à l'aide de modèles de tâche ou de modèles de workflow dans la séquence requise.

Terme	Définition
Paramètre conditionnel	La connexion entre les modèles de tâche ou les modèles de workflow, qui oriente la procédure de contrôle, repose sur l'une des conditions suivantes : • Continuer (par défaut) • En cas de réussite • En cas d'échec • En cas de réussite partielle **Remarque** Un paramètre conditionnel vous permet également d'insérer un *"Délai"* (en secondes) pour que la tâche suivante dans le scénario commence seulement un certain temps après la fin de l'exécution de la tâche précédente. **→ N'oubliez pas** L'Assistant du workflow prend en compte la valeur de paramètre conditionnelle "Continuer" uniquement si la tâche précédente s'est terminée en affichant l'un des trois états suivants : "Succès", "Réussite partielle" ou "Échec". Si la tâche précédente comporte le statut "Erreur" ou "Non exécuté", l'état du nœud suivant est automatiquement défini sur "Non exécuté".

Cette illustration vous aidera à comprendre l'interconnexion entre certains des termes susmentionnés :



22.4 À propos de l'installation et de la mise à jour

Votre accès aux fonctionnalités backend peut différer selon que vous procédez à une nouvelle installation ou que vous mettez à jour une installation existante.

Lorsque vous procédez à **une nouvelle installation** de la plateforme SAP BusinessObjects BI (installation par défaut), vous obtenez un accès complet à l'Assistant du workflow sur les ordinateurs où la plateforme de BI est installée et configurée. Cela inclut l'accès à l'application Assistant du workflow dans la CMC et aux fonctionnalités backend (service Assistant du workflow).

Cependant, lorsque vous mettez à jour la plateforme de BI version SP5 ou ultérieure vers la version 4.3, les fonctionnalités complètes de l'Assistant du workflow sont disponibles, mais vous devrez encore parcourir la note SAP mentionnée sous Restrictions. Après l'installation de la mise à jour, exécutez le workflow d'installation "Modifier" pour accéder aux services backend. Pour en savoir plus sur le workflow d'installation "Modifier", consultez le *Guide de mise à jour de Support Package* publié sur la page du portail d'aide consacrée à la plateforme SAP Business Intelligence.

> **Remarque**
>
> L'Assistant du workflow fait partie du fichier BOE.war. Après la mise à jour de la plateforme de BI version 4.2 SP4 ou antérieure vers la version 4.2 SP5 et supérieure, l'application Web est déployée uniquement si la fonctionnalité *Applications Web Java* a été sélectionnée lors de l'installation de la version existante.

> **Attention**
>
> Vous ne devez pas installer l'Assistant du workflow sur plusieurs ordinateurs au sein de systèmes, car la mise en cluster de l'Assistant du workflow n'est pas prise en charge.

L'Assistant du workflow prend désormais en charge les systèmes d'exploitation AIX et Solaris.

> **⚠ Restriction**
>
> - Pour les plateformes AIX et Solaris, lorsque vous procédez à l'installation de la version 4.3 de BI sur une version 4.2 SP05 ou ultérieure, l'Assistant du workflow est installé par défaut. Cependant, une réparation est requise pour pouvoir bénéficier des services backend.
> - Lorsque vous effectuez une mise à jour de la plateforme de BI version 4.2 SP4 ou antérieure vers la version 4.2 SP5 ou ultérieure, vous constatez que certains dossiers ne sont pas répertoriés dans l'Assistant du workflow. Pour en savoir plus, consultez la note SAP 2882649.

22.5 Configuration de l'Assistant du workflow

Lorsque vous installez l'Assistant du workflow dans le cadre de l'installation de la plateforme de BI, vous obtenez ce service par défaut dans votre configuration.

Vous pouvez ensuite configurer l'authentification sécurisée pour commencer à utiliser l'Assistant du workflow.

22.5.1 Configuration de base

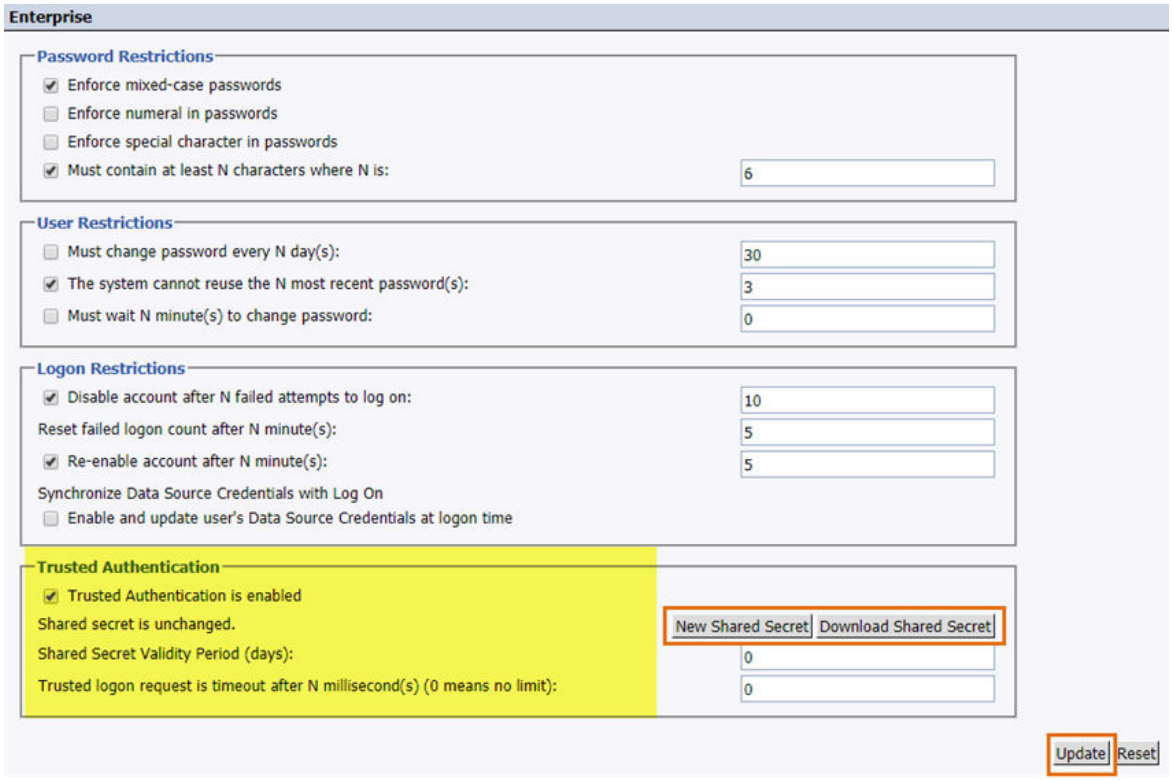
22.5.1.1 Configuration de l'authentification Enterprise pour l'Assistant du workflow

Vous avez installé l'Assistant du workflow dans le cadre de l'installation de la plateforme de BI dans votre configuration.

Pour configurer l'authentification (Enterprise) sécurisée pour l'Assistant du workflow, suivez la procédure décrite ci-dessous :

1. Connectez-vous à la CMC (Central Management Console) via la connexion au CMS du nœud principal.
2. Sélectionnez *Authentification* dans la liste déroulante, puis cliquez deux fois sur *Enterprise*.

La boîte de dialogue "Entreprise" apparaît, tel qu'illustré ci-dessous :



3. Dans la section "Authentification sécurisée", assurez-vous que l'*authentification sécurisée* est activée.
4. Cliquez sur *Nouveau secret partagé*.
   La clé secrète partagée est générée.
5. Cliquez sur *Télécharger le secret partagé*.
6. Sélectionnez *Mettre à jour*.
7. Enregistrer la clé secrète partagée générée (TrustedPrincipal.conf) :
   a. Sous Windows, `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0\win64_x64/`.
   b. Sous Linux, sous `<REPINSTALL>/sap_bobj/enterprise_xi40/linux_x64/`.
   c. Sous AIX, sous `<REPINSTALL>/sap_bobj/enterprise_xi40/aix_rs6000_64/`.
   d. Dans Solaris, sous `<REPINSTALL>/sap_bobj/enterprise_xi40/solaris_sparcv9/`.

> **Remarque**
>
> Pour en savoir plus sur la création de certificats d'authentification sécurisée avec différentes options, voir la rubrique Activation de l'authentification sécurisée [page 265].

22.5.1.2 Création d'un utilisateur par défaut pour le service backend Assistant du workflow

1. Créez un utilisateur portant le nom **UtilisateurAW** dans l'Assistant du workflow.

2. Affectez les droits appropriés en accédant au dossier `Assistant du workflow` et en accordant un contrôle total au compte **UtilisateurAW**.

   Le service backend Assistant du workflow se lance via le compte **UtilisateurAW**.

   Si le compte **UtilisateurAW** n'existe pas, l'Assistant du workflow se lance via le compte *Administrateur*.

   > ⓘ Remarque
   >
   > Le nouvel utilisateur ne doit pas obligatoirement faire partie du groupe d'utilisateurs *Administrateur*.

22.5.1.3 Lancement du service Assistant du workflow

Cette rubrique fournit des instructions pour lancer le *service Assistant du workflow*.

1. Configurez l'authentification Enterprise pour l'Assistant du workflow. Pour en savoir plus, voir Configuration de l'authentification Enterprise pour l'Assistant du workflow [page 869].
2. Pour lancer le *service Assistant du workflow* :
   a. Dans Windows, lancez *Central Configuration Manager* (CCM) et lancez le *service Assistant du workflow*.
   b. Sous Unix, accédez à `<REPINSTALL>/AdminConsole/WorkflowAssistant/startWfAssistant.sh`.

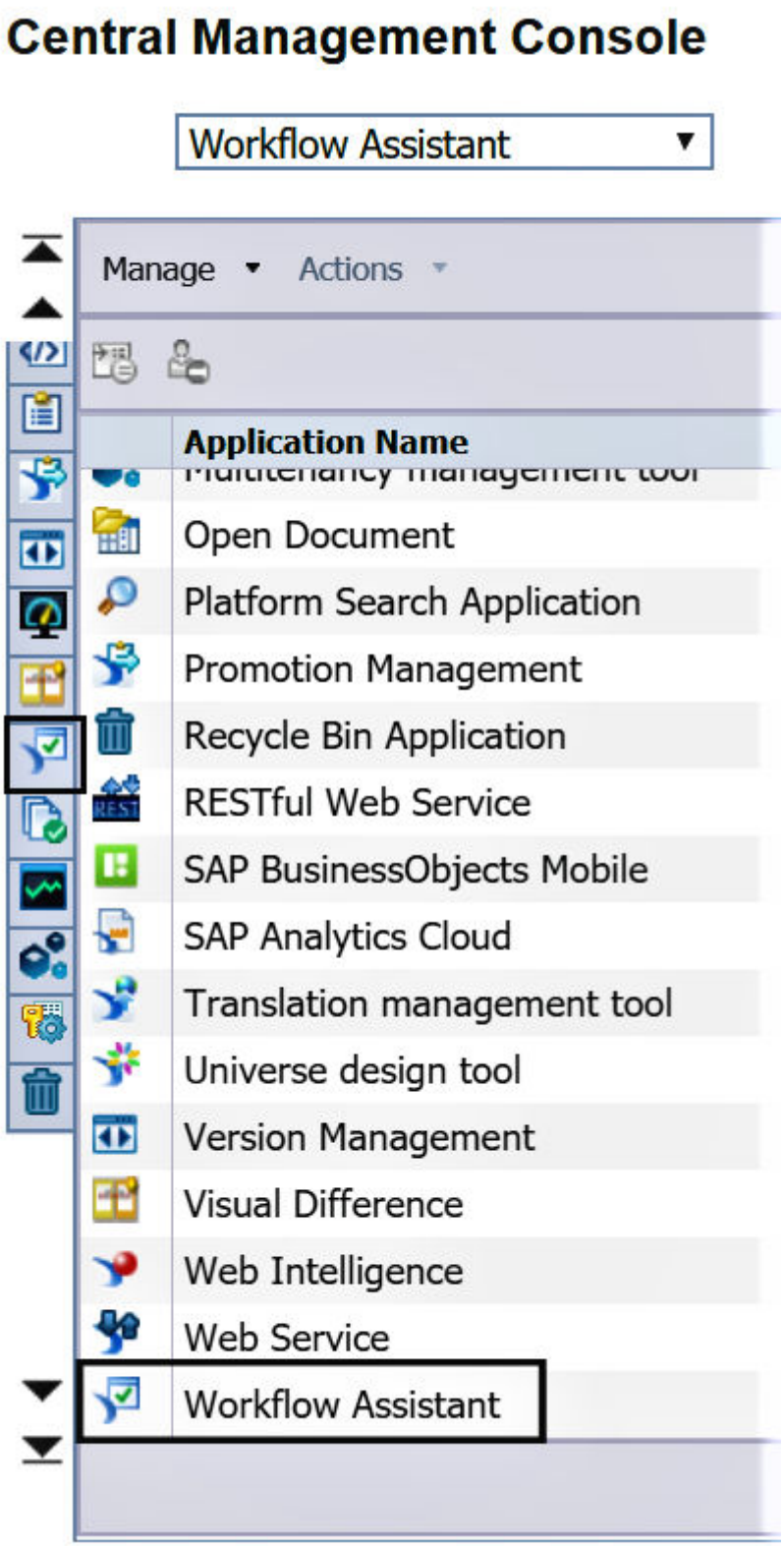
   Vous pouvez maintenant utiliser l'*Assistant du workflow* et exécuter des scénarios.

   > ⓘ Remarque
   >
   > Pour vous assurer du lancement correct de l'Assistant du workflow, consultez le contenu du fichier `message.properties` dans `<Répertoire-Install-BOE>\AdminConsole\WorkflowAssistant\service-logs` Le contenu de `message.properties` doit être le suivant :
   >
   > ```
   > STATUS_WFM=success
   >
   > MESSAGE_AGENT=Agent - Started\!\!
   >
   > STATUS_AGENT=success
   >
   > MESSAGE_WFM=Workflow Assistant - Started\!\!
   > ```

22.6 Gestion des droits d'Assistant du workflow via la Central Management Console

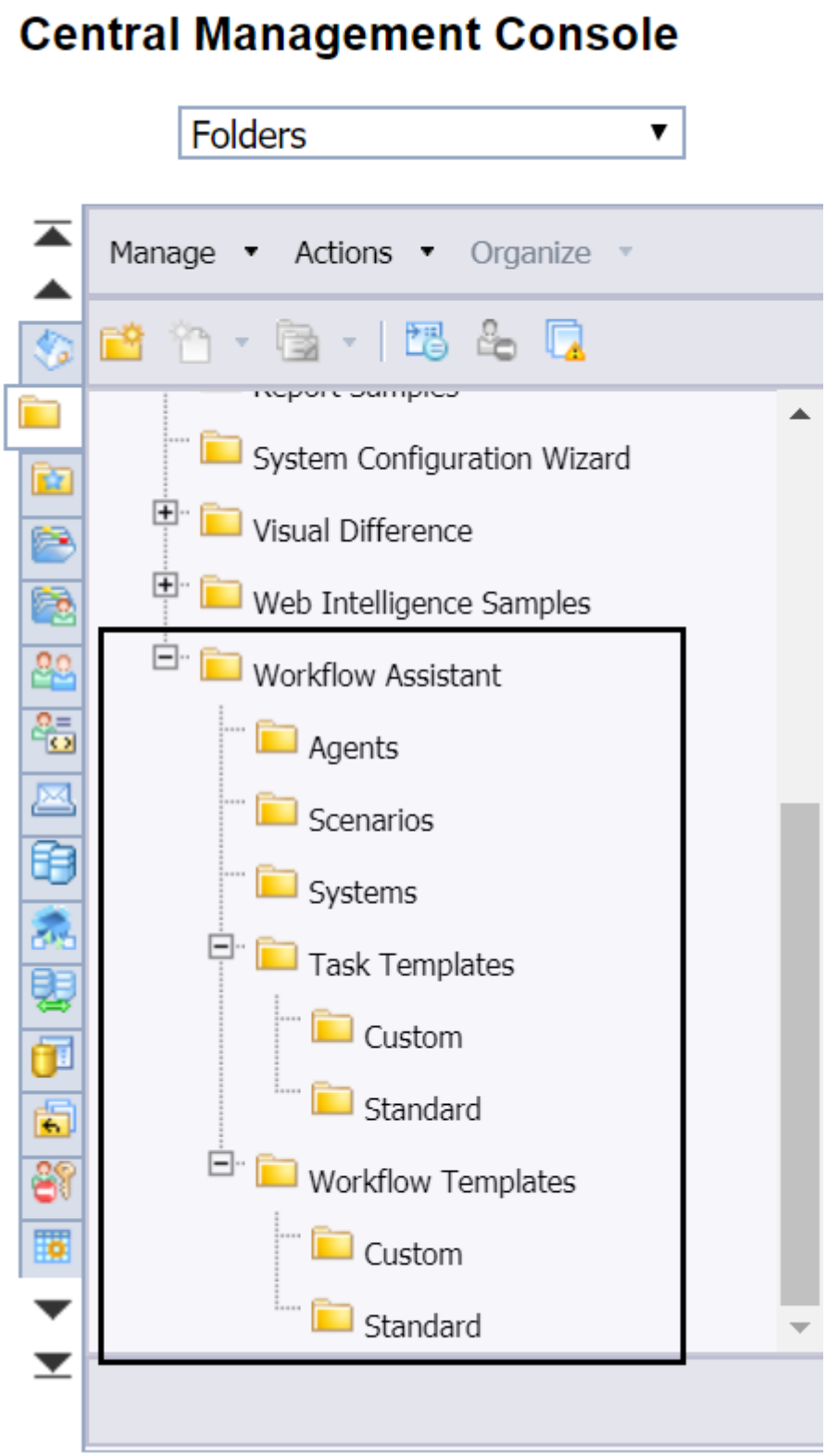
Vous gérez la sécurité relative à l'Assistant du workflow via la CMC (Central Management Console).

L'*Assistant du workflow* est répertorié sous *Applications* de la *Central Management Console*.



Dans l'Assistant du workflow, vous pouvez visualiser et gérer les droits d'accès et les paramètres généraux de sécurité pour les entités suivantes :

- Systèmes
- Scénarios
- Modèles de tâche
- Modèles de workflow



Pour en savoir plus sur la gestion des paramètres de sécurité pour les objets dans la CMC, voir la rubrique Gestion des paramètres de sécurité pour les objets dans la CMC.

> **Remarque**
>
> - Vous pouvez contrôler l'accès à une fonctionnalité dans l'Assistant du workflow (comme *Systèmes*, *Scénarios*, *Modèles de tâche* et *Modèles de workflow*) en attribuant des droits au niveau du dossier ou de l'objet à l'utilisateur, mais le manque de droits n'a aucun impact sur l'interface utilisateur. Cela signifie qu'un utilisateur doit avoir le droit *Ajouter des objets dans ce dossier* sur le dossier *Scénario* pour créer un scénario.
> - Par exemple, l'utilisateur peut voir l'option pour créer un scénario dans l'Assistant du workflow, même s'il ne dispose pas de droits sur le dossier *Scénario* dans la CMC. Si l'utilisateur essaie tout de même de créer et enregistrer un scénario dans le dossier *Scénario*, le système affiche un message d'erreur.

Gestion des droits d'application

Si vous disposez des droits appropriés spécifiques à l'application, vous pouvez refuser ou effectuer les tâches suivantes dans l'Assistant du workflow :

- Pour refuser une tâche *Créer le modèle de tâche*, accédez au dossier Modèle de tâche et refusez le droit *Ajouter les objets au dossier*.
- Pour refuser une tâche *Créer le modèle de workflow*, accédez au dossier Modèle de workflow et refusez le droit *Ajouter les objets au dossier*.
- Pour refuser une tâche *Créer le scénario*, accédez au dossier Scénario et refusez le droit *Ajouter les objets au dossier*.
- Pour refuser une tâche *Modifier le modèle de tâche*, accédez au dossier Modèle de tâche et refusez le droit *Modifier les objets*.
- Pour refuser une tâche *Modifier le modèle de tâche appartenant à l'utilisateur*, accédez au dossier Modèle de tâche et refusez le droit *Modifier les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Modifier le modèle de workflow*, accédez au dossier Modèle de workflow et refusez le droit *Modifier les objets*.
- Pour refuser une tâche *Modifier le modèle de workflow appartenant à l'utilisateur*, accédez au dossier Modèle de workflow et refusez le droit *Modifier les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Modifier le scénario*, accédez au dossier Scénario et refusez le droit *Modifier les objets*.
- Pour refuser une tâche *Modifier le scénario appartenant à l'utilisateur*, accédez au dossier Scénario et refusez le droit *Modifier les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Visualiser le modèle de tâche*, accédez au dossier Modèle de tâche et refusez le droit *Visualiser les objets*.
- Pour refuser une tâche *Visualiser le modèle de tâche appartenant à l'utilisateur*, accédez au dossier Modèle de tâche et refusez le droit *Visualiser les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Visualiser le modèle de workflow*, accédez au dossier Modèle de workflow et refusez le droit *Visualiser les objets*.
- Pour refuser une tâche *Visualiser le modèle de workflow appartenant à l'utilisateur*, accédez au dossier Modèle de workflow et refusez le droit *Visualiser les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Visualiser le scénario*, accédez au dossier Scénario et refusez le droit *Visualiser les objets*.
- Pour refuser une tâche *Visualiser le scénario appartenant à l'utilisateur*, accédez au dossier Scénario et refusez le droit *Visualiser les objets appartenant à l'utilisateur*.

- Pour refuser une tâche *Supprimer le modèle de tâche*, accédez au dossier Modèle de tâche et refusez le droit *Supprimer les objets*.
- Pour refuser une tâche *Supprimer le modèle de tâche appartenant à l'utilisateur*, accédez au dossier Modèle de tâche et refusez le droit *Supprimer les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Supprimer le modèle de workflow*, accédez au dossier Modèle de workflow et refusez le droit *Supprimer les objets*.
- Pour refuser une tâche *Supprimer le modèle de workflow appartenant à l'utilisateur*, accédez au dossier Modèle de workflow et refusez le droit *Supprimer les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Supprimer le scénario*, accédez au dossier Scénario et refusez le droit *Supprimer les objets*.
- Pour refuser une tâche *Supprimer le scénario appartenant à l'utilisateur*, accédez au dossier Scénario et refusez le droit *Supprimer les objets appartenant à l'utilisateur*.
- Pour refuser une tâche *Exécuter le scénario pour toutes les combinaisons*, accédez au scénario donné et refusez le droit *Ajouter les objets au dossier*.
- Pour refuser une tâche *Exécuter le scénario appartenant à l'utilisateur pour toutes les combinaisons*, accédez au scénario donné et refusez le droit *Ajouter des objets au dossier appartenant à l'utilisateur*.
- Pour refuser une tâche *Créer une infrastructure*, accédez au dossier Infrastructure et refusez le droit *Ajouter des objets au dossier*.
- Pour refuser une tâche *Modifier et visualiser l'infrastructure*, accédez au dossier Infrastructure et refusez les droits *Modifier les objets* et *Visualiser les objets*.
- Pour refuser une tâche *Supprimer l'infrastructure*, accédez au dossier Infrastructure et refusez le droit *Supprimer les objets*.
- Pour refuser une tâche *Ajouter des références de connexion utilisateur dans l'infrastructure*, accédez au dossier Infrastructure et refusez le droit *Ajouter les objets au dossier*.

> **ⓘ Remarque**
>
> Tous les droits susmentionnés peuvent être appliqués à chacun des modèles de tâche/modèles de workflow/scénarios.

22.7 Utilisation de l'Assistant du workflow

L'Assistant du workflow est une application dans la CMC qui permet d'automatiser vos tâches d'administration BI répétitives et complexes. Dans les sections suivantes, vous allez apprendre à automatiser les tâches d'administration BI.

22.7.1 À propos des modèles de tâche standard

Des modèles de tâche standard sont intégrés (prêts à l'emploi) dans l'Assistant du workflow. Lors de la création de scénarios ou des modèles de workflow, vous pouvez utiliser ces modèles de tâche.

Modèle de tâche standard	Description
Connexion	Crée une session avec le serveur de la plateforme de BI cible.
Actualiser les documents	Ouvre et actualise la liste des documents fournis à l'aide de l'opération `<Planifier maintenant>`. **Remarque** Pour les documents contenant des invites, les valeurs par défaut doivent être spécifiées dans les documents avant l'exécution.
Modifier la source Web Intelligence	Modifie le mappage d'univers source pour votre liste de documents, de .unv en .unx, .de unx en .unx ou de .unv en .bex.
Ajouter/Supprimer un utilisateur et un groupe d'utilisateurs	Ajoute ou supprime les utilisateurs et les groupes d'utilisateurs dans l'infrastructure BI. **Remarque** Ce modèle de tâche correspond à la `<fonctionnalité Importer>` sur la plateforme de BI. Pour en savoir plus sur la fonctionnalité Importer, voir la rubrique Pour ajouter des utilisateurs ou groupes d'utilisateurs en bloc.
Obtenir les propriétés	Renvoie les valeurs de certaines propriétés pour les InfoObjects concernés par la requête.
Définir des propriétés	Définit les valeurs de certaines propriétés pour les InfoObjects donnés dans le CMS.
Lire la réserve de travail	Lit les fichiers .CSV en tant qu'entrée et renvoie les valeurs séparées par des virgules qui peuvent être utilisées par les tâches suivantes. Utilisez ce modèle de tâche lorsqu'un grand nombre de valeurs (données en bloc) doit être utilisé par des modèles de workflow

Modèle de tâche standard	Description
	dans votre scénario et qu'il n'est pas possible de renseigner manuellement les valeurs à l'aide du panneau Entrée de l'Assistant du workflow.
Requête de réserve de travail	Lance une requête dans les tableaux du CMS et fournit la sortie au format CSV.
Enregistrer les données de sortie	Enregistre les valeurs extraites du champ *Paramètre de sortie* dans un fichier CSV du CMS.
Définir les propriétés du serveur	Définit les valeurs de certaines propriétés pour le(s) serveur(s) donné(s).
Déconnexion	Termine la session de la tâche avec le serveur de la plateforme de BI cible.

22.7.1.1 Connexion

Paramètres pour modèle de tâche Connexion

Paramètres d'entrée

Nom	Type	Description
Système	Chaîne	Nom de l'infrastructure enregistrée dans l'Assistant du workflow

22.7.1.2 Actualiser les documents

Paramètres pour Actualiser les documents

Paramètre d'entrée

Nom	Type	Description
*Documents	CSV	Identificateurs de documents (ID/CUID) pour les documents à actualiser Un utilisateur peut également sélectionner des documents dans l'Explorateur de référentiel via l'aide à la saisie. Format CSV : ID ou CUID

Paramètres de sortie

Nom	Type	Description
DocumentsActualisés	CSV	Documents qui ont été correctement actualisés. Format CSV : ID, CUID
DocumentsNonActualisés	CSV	Documents qui n'ont pas pu être actualisés. Format CSV : ID, CUID
Tout	CSV	Liste des documents traités. Format CSV : ID, CUID

22.7.1.3 Modifier la source Web Intelligence

Paramètres pour Modifier la source Web Intelligence

Paramètres d'entrée

Nom	Type	Description
*Document	CSV	Spécifiez le CUID du document Web Intelligence pour lequel vous souhaitez remplacer UNV par UNX, UNX par UNX ou UNV par BEx. Un utilisateur peut également sélectionner des documents en recourant à l'Explorateur de référentiel via l'aide à la saisie ou en mappant une sortie d'une tâche à une autre. Format CSV : ID ou CUID
*Mappage d'univers	CSV	Mappage des univers (UNV, UNX, BEx) sur la base de l'ID ou du CUID. Un utilisateur peut également mapper les univers via l'écran Mappage de l'univers dans l'aide à la saisie. Format CSV (pour UNV-UNX) : unv_cuid, unx_cuid ou unv_id, unx_id Format CSV (pour UNX-UNX) : src_cuid, dest_cuid, type Format CSV (pour UNV-BEx) : src_cuid, dest_cuid, type, technical_name
Action dans le document	Chaîne	Pour modifier la source sans enregistrer le document, affectez la valeur : "Test" Pour modifier la source et enregistrer le document, affectez la valeur : "Modifier"

Paramètres de sortie

Nom	Type	Description
Réussite	CSV	Documents pour lesquels la source a été correctement modifiée. Format CSV : ID, CUID

Nom	Type	Description
Échec	CSV	Documents pour lesquels la source n'a pas pu être modifiée. Format CSV : ID, CUID
Tout	CSV	Liste des documents entrants. Format CSV : ID, CUID

Restriction

- Seul l'élément .UNV basé sur une requête .BEx peut être remplacé par une autre requête .BEx.
- Les requêtes BEx avec des invites ne sont pas prises en charge.
- Le mappage a lieu uniquement si les objets d'univers ont un type similaire et un nom au plus proche des objets de requête BEx.
- Les objets d'univers créés avec des étiquettes ne sont pas mappés.

22.7.1.4 Ajouter/Supprimer un utilisateur et un groupe d'utilisateurs

Paramètres pour Ajouter/Supprimer un utilisateur et un groupe d'utilisateurs

Paramètres d'entrée

Nom	Type	Description

*Données	CSV	Informations spécifiques à l'utilisateur.
		
		Consultez les exemples de données CSV ci-dessous. Pour en savoir plus sur les données CSV, voir la rubrique *Pour ajouter des utilisateurs ou groupes d'utilisateurs en bloc* dans le *Guide d'administration de la plateforme de Business Intelligence*.
		
		`command,group,user,fullname,password,mail,profileName,profileValue`
		`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue`

> **Remarque**
>
> Vous pouvez également créer un fichier CSV sans en-tête CSV et l'utiliser comme entrée dans votre scénario.
>
> Le mot de passe sélectionné dans le fichier CSV doit respecter la stratégie de mot de passe.

> **→ Conseil**
>
> Vous pouvez utiliser des virgules consécutives pour ignorer un champ de saisie.

22.7.1.5 Obtenir les propriétés

Paramètres pour Obtenir les propriétés

Paramètres d'entrée

Nom	Type	Description
*InfoObject	CSV	Valeurs CSV des InfoObjects. Le préfixe 'si_' ne doit pas être spécifié pour l'utilisation des propriétés. Format CSV : ID ou CUID
*Propriété	CSV	Valeurs CSV des propriétés. Le préfixe 'si_' ne doit pas être spécifié pour l'utilisation des propriétés. Pour les InfoObjects d'un utilisateur, la propriété prise en charge est "property;data".

Paramètres de sortie

Nom	Type	Description
Réussite	CSV	Liste des InfoObjects pour lesquels la valeur de propriété a été correctement recherchée ou affectée. Format CSV : ID ou <propriété recherchée>
Échec	CSV	Liste des InfoObjects pour lesquels la valeur de propriété n'a pas pu être recherchée ou affectée. Format CSV : ID, CUID
Tout	CSV	Liste de tous les InfoObjects traités. Format CSV : ID, CUID

22.7.1.6 Définir des propriétés

Paramètres pour Définir des propriétés

Paramètres d'entrée

Nom	Type	Description
*InfoObject	CSV	Valeurs CSV des InfoObjects. Le préfixe 'si_' ne doit pas être spécifié pour l'utilisation des propriétés. Format CSV : ID ou CUID
*Propriété	CSV	Valeurs CSV des propriétés. Pour les InfoObjects d'un utilisateur, la propriété prise en charge est "property;data".

Paramètres de sortie

Nom	Type	Description
Réussite	CSV	Liste des InfoObjects pour lesquels la valeur de propriété a été correctement extraite ou définie. Format CSV : ID ou <propriété recherchée>
Échec	CSV	Liste des InfoObjects pour lesquels la valeur de propriété n'a pas pu être extraite ou définie. Format CSV : ID, CUID
Tout	CSV	Liste de tous les InfoObjects traités. Format CSV : ID, CUID

22.7.1.7 Définir les propriétés du serveur

Paramètres pour Définir les propriétés du serveur

Paramètres d'entrée

Nom	Type	Description
*Serveur	CSV	Identificateurs (ID/CUID) pour les serveurs à modifier. Un utilisateur peut également sélectionner des serveurs dans l'Explorateur de référentiel via l'aide à la saisie. Format CSV : ID ou CUID
*Propriété	CSV	Valeurs CSV avec propriété et valeur. Par exemple : `hostname;new value`. Propriétés prises en charge : hostname

Paramètres de sortie

Nom	Type	Description
Réussite	CSV	Liste des serveurs pour lesquels la valeur de propriété a été correctement définie. Format CSV : ID
Échec	CSV	Liste des serveurs pour lesquels la valeur de propriété n'a pas pu être définie. Format CSV : ID
Tout	CSV	Liste de tous les serveurs traités. Format CSV : ID

22.7.1.8 Lire la réserve de travail

Paramètres pour Lire la réserve de travail

Paramètres d'entrée

Nom	Type	Description
*Fichier	CSV	Fichier CSV avec les données requises pour la lecture. Un utilisateur peut également sélectionner un fichier CSV dans l'Explorateur de référentiel via l'aide à la saisie. Format CSV : <En-tête1>, <En-tête2>, ..<En-têteN> **Remarque** Pour en savoir plus sur les formats de données et les séparateurs dans CSV, voir Utilisation de données CSV [page 892].

Paramètres de sortie

Nom	Type	Description
Valeurs	CSV	Liste des valeurs lues à partir du fichier d'entrée, lesquelles sont renvoyées dans un format séparé par des virgules.

22.7.1.9 Enregistrement des données de sortie

Paramètres pour la tâche Enregistrer les données de sortie

Paramètres d'entrée

Nom	Type	Description
*Paramètre	CSV	Mappez les données de sortie obtenues depuis la tâche précédente.
*Nom du fichier	Chaîne	Spécifiez le nom de fichier pour enregistrer les données de sortie.
*Choisir le dossier de destination	Chaîne	Sélectionnez le dossier d'enregistrement du fichier.
*Options d'enregistrement	Chaîne	Pour écraser un fichier existant portant le même nom, sélectionnez la valeur : *Écraser*. Pour renommer un fichier existant avec le même nom complété du suffixe _1, _2, ..., sélectionnez la valeur : *Renommer*.

> ⓘ Remarque
>
> **Paramètres de sortie**
>
> Les données de sortie obtenues se présentent sous la forme d'un fichier dans le CMS. Par conséquent, aucun paramètre ne peut être utilisé.

22.7.1.10 Déconnexion

Paramètres pour la tâche Déconnexion

Paramètre d'entrée

Nom	Type	Description
SessionToken	Chaîne	Jeton de session (généré en raison de la connexion)

22.7.2 À propos des modèles de workflow standard

Des modèles de workflow standard sont intégrés (prêts à l'emploi) dans l'Assistant du workflow. Lors de la création de scénarios, vous pouvez utiliser ces modèles de workflow.

Modèles de workflow standard disponibles dans l'Assistant du workflow

Nom du modèle	Description
Connexion	Crée une session avec le serveur de la plateforme de BI cible.
Actualiser les documents	Actualise la liste spécifiée de documents Web Intelligence.
Modifier la propriété du document	Lance une requête pour déterminer le propriétaire du document et affecte le même propriétaire à un autre document.
Modifier le type de licence utilisateur	Lance une requête pour dresser la liste des utilisateurs en fonction de conditions spécifiques à l'utilisateur et modifie le type de licence.
Modifier la source Web Intelligence & vérifier les documents	Modifie le mappage d'univers source de .unv en .unx ou de .unv en .bex et valide les documents pour les documents Web Intelligence en bloc.
Ajouter/Supprimer des utilisateurs	Permet à un administrateur d'ajouter ou de supprimer des utilisateurs et des groupes.
Déconnexion	Termine la session de la tâche avec le serveur de la plateforme de BI cible.

22.7.3 À propos des modèles de tâche personnalisés

Vous pouvez utiliser les modèles de tâche standard dans l'Assistant du workflow pour concevoir des modèles de workflow et exécuter des scénarios. Si les modèles standard ne permettent pas de répondre à vos besoins, vous pouvez développer votre propre modèle de tâche et plug-in pour l'Assistant du workflow.

Créez votre propre modèle de tâche personnalisé à l'aide du SDK de modèle de tâche personnalisé qui fournit une API permettant aux développeurs d'implémenter de nouveaux modèles de tâche. Pour en savoir plus, voir Comment créer un modèle de tâche personnalisé dans la structure d'automatisation BI.

22.7.4 Gestion de modèles de workflow

Vous pouvez créer, modifier et supprimer des modèles de workflow personnalisés dans l'Assistant du workflow.

22.7.4.1 Création de modèles de workflow personnalisés

Vous créez des modèles de workflow personnalisés à l'aide de modèles de tâche standard ou personnalisés.

1. Sur la page d'accueil, sélectionnez *Assistant du workflow*.
2. Sur la page *Assistant du workflow*, sélectionnez l'onglet *Modèles de workflow*.
3. Cliquez sur l'icône + (*Ajouter*) en haut à droite des *Modèles de workflow*.
4. Dans la zone de graphiques *Créer le modèle de workflow*, cliquez sur l'icône > (*Développer*) qui figure avant les catégories *Standard* et *Personnalisé* des modèles de tâche dans le panneau de gauche.
5. Glissez et déposez les modèles de tâche requis vers la zone de graphiques située dans la partie droite de la page.
6. Renommez le modèle de tâche que vous venez de déposer dans la zone de graphiques.
7. (Facultatif) Sélectionnez l'icône (*Lier*) qui figure entre deux modèles de tâche et sélectionnez la valeur requise pour les paramètres conditionnels dans la liste qui apparaît.

   Ici, vous pouvez également insérer le `<Délai>` (en secondes).
8. (Facultatif) Définissez les valeurs des paramètres d'entrée, qui seront utilisées comme valeurs par défaut lors de l'utilisation du modèle de workflow dans un scénario.
9. Sélectionnez *Enregistrer*.
10. Dans la boîte de dialogue *Enregistrer le modèle de workflow*, saisissez un nom (obligatoire) pour votre modèle de workflow, puis ajoutez une description si nécessaire.
11. Sélectionnez *Enregistrer* dans la boîte de dialogue *Enregistrer le modèle de workflow* .

    Le nouveau modèle de workflow est alors répertorié dans la vue *Modèles de workflow* de l'Assistant du workflow.

    > **Remarque**
    >
    > Toute modification apportée aux modèles de workflow existants n'a aucune incidence sur les scénarios existants.

22.7.4.2 Modification des modèles de workflow personnalisés

Vous modifiez des modèles de workflow personnalisés dans l'Assistant du workflow.

1. Dans l'onglet *Modèles de workflow* de l'Assistant du workflow, cliquez sur (*Autres*) et sélectionnez *Modifier*.
2. Dans l'écran *Modifier le modèle de workflow*, apportez les modifications requises au modèle de workflow en ajoutant/supprimant les modèles de tâche, en modifiant les valeurs des paramètres d'entrée ou en modifiant les paramètres conditionnels entre les modèles de tâche.

3. Sélectionnez *Enregistrer sous*.
4. Dans la boîte de dialogue *Enregistrer le modèle de workflow*, modifiez le nom du modèle de workflow selon vos besoins.
5. Sélectionnez *Enregistrer*.

   Les modifications apportées au modèle de workflow sont enregistrées et vous revenez à la page d'accueil de l'Assistant du workflow.

22.7.4.3 Suppression de modèles de workflow personnalisés

Vous supprimez des modèles de workflow personnalisés dans l'Assistant du workflow.

1. Dans l'onglet *Modèles de workflow* de l'Assistant du workflow, cliquez sur ... (*Autres*) et sélectionnez *Supprimer*.
2. Sélectionnez *Supprimer* dans l'avertissement qui apparaît.

   Le modèle de workflow supprimé n'est plus répertorié dans l'onglet *Modèles de workflow* de l'Assistant du workflow.

22.7.5 Gestion de scénarios et affichage des résultats

Vous créez des scénarios en connectant des modèles de tâche et des modèles de workflow. Vous gérez les scénarios et affichez les résultats dans l'Assistant du workflow.

22.7.5.1 Création de scénarios

Cette rubrique explique comment créer des scénarios dans l'Assistant du workflow.

1. Sur la page d'accueil de la CMC, sélectionnez *Assistant du workflow*.

   Les scénarios disponibles sont répertoriés sur la page qui s'affiche.
2. Cliquez sur l'icône + (*Créer dossier ou scénario*) et sélectionnez *Scénario*.
3. Dans la page *Créer le scénario*, cliquez sur l'icône > (*Développer*) qui figure avant les catégories *Standard* et *Personnalisé* des modèles de tâche dans le panneau de gauche.

   > **Remarque**
   >
   > Vous pouvez consulter la description de la tâche en plaçant le curseur de la souris sur le nom du modèle de tâche.
4. Glisser et déposez les modèles de workflow requis vers la zone de graphiques située dans la partie droite de la page.
5. (Facultatif) Sélectionnez l'icône (*Lier*) qui figure entre deux modèles de tâche et sélectionnez la valeur requise pour les paramètres conditionnels dans la liste qui apparaît.

Ici, vous pouvez également insérer le `<Délai>` (en secondes).

6. Cliquez sur un modèle de workflow dans la zone de graphiques.

   Un panneau d'entrée apparaît sur le côté droit de la page.

7. Dans le panneau d'entrée à droite, cliquez sur > (*Développer*) pour voir les champs de paramètre d'entrée pour chaque modèle de tâche et sélectionnez les valeurs requises dans les champs.

> ⚠ Attention
>
> - Assurez-vous que les valeurs d'entrée que vous spécifiez pour les paramètres de modèle ne contiennent pas vos données personnelles et respectent les directives du Règlement général sur la protection des données (RGPD). Pour en savoir plus sur le RGPD, voir la rubrique Protection et confidentialité des données [page 181].

> ⓘ Remarque
>
> Vous pouvez obtenir davantage d'informations sur les paramètres en vous référant aux informations de paramètre. Pour en savoir plus sur les informations de paramètre, voir À propos des informations de paramètres [page 893].

8. Sélectionnez *Enregistrer*.

> → N'oubliez pas
>
> Vous devez obligatoirement spécifier des entrées pour chaque modèle de tâche dans un scénario avant de pouvoir exécuter le scénario. Cependant, vous pouvez également utiliser l'option *Exécuter avec le paramètre* pour spécifier les entrées.

9. Dans la boîte de dialogue *Enregistrer le scénario*, indiquez les informations nécessaires dans les onglets *Enregistrer le scénario* et *Notifier par courrier électronique*.
   a. Dans l'onglet *Enregistrer le scénario*, saisissez un nom (obligatoire) pour votre scénario, ajoutez une description et sélectionnez l'emplacement où sera enregistré le scénario.
   b. Dans l'onglet *Notifier par courrier électronique*, cliquez sur le bouton bascule pour l'activer.
      Les options illustrées dans l'image ci-dessous

      Only On ☐ Success ☐ Partial Success ☐ Failure

      s'affichent.
   c. Sélectionnez une ou plusieurs options. Votre sélection servira de critère pour déclencher une notification par courrier électronique.
   d. Vous pouvez *utiliser le paramètre par défaut* ou le désactiver à l'aide du bouton bascule. Ces paramètres par défaut sont définis dans la CMC. Voir le *Guide d'administration Business Intelligence* pour apprendre à définir des paramètres par défaut pour les destinations de courrier électronique.
   e. Si vous désélectionnez *Utiliser le paramètre par défaut*, renseignez les adresses électroniques dans *De, À*, *CC* (facultatif) et *CCi* (facultatif), l'*Objet* et le *Message*. Vous pouvez également ajouter des caractères génériques dans chaque champ.

10. Sélectionnez *Enregistrer* ou *Enregistrer et exécuter*.

    Le nouveau scénario est répertorié dans la vue *Scénarios* de l'*Assistant du workflow* et, en fonction des critères sélectionnés dans l'onglet *Notifier par courrier électronique*, le courrier électronique sera déclenché.

22.7.5.1.1 Indication des paramètres d'entrée

Lors de la création de modèles de workflow dans l'*Assistant du workflow*, vous pouvez ajouter des valeurs d'entrée au moment de la conception et de l'exécution. En d'autres termes, vous pouvez ajouter des valeurs d'entrée lors de la création et de l'exécution d'un scénario. Il existe deux façons d'ajouter des valeurs d'entrée à un *scénario* :

1. Aide à la saisie
2. Mappage de la sortie d'une tâche comme entrée d'une autre tâche

Aide à la saisie

Vous pouvez sélectionner un objet, comme un document ou une réserve de travail, dans l'Explorateur de référentiel avec l'*Aide à la saisie*. Par exemple, dans un scénario permettant d'actualiser le document, vous pouvez sélectionner un document en cliquant sur l'icône (*Aide à la saisie*) dans le champ *Documents*.

Mappage de la sortie d'une tâche comme entrée d'une autre tâche

Vous pouvez indiquer la sortie de la première tâche comme entrée pour la deuxième tâche lors de l'exécution d'un scénario. Saisissez @ dans un champ de saisie et vous verrez la liste des valeurs obtenues dans la première tâche.

- Une valeur d'entrée suit le format suivant : **@<ModèleWorkflow>.<ModèleTâche>.<ParamètreSortie>**.
- La liste des valeurs d'entrée affiche uniquement les valeurs compatibles obtenues dans la première tâche. Si le champ de saisie accepte le format CSV comme type de données, par exemple, les valeurs d'entrée de la tâche précédente qui sont au format CSV sont affichées.

> **Remarque**
>
> Les paramètres d'entrée prennent en charge le fichier CSV comme entrée. Pour en savoir plus, voir Utilisation de données CSV [page 892].

22.7.5.1.2 Utilisation de données CSV

La plupart des modèles de tâche standard prennent en charge les valeurs des paramètres d'entrée au format CSV. Par exemple, le modèle de tâche *Actualisation du document* prend en charge le format CSV pour le champ de saisie *Documents*. Cela signifie que vous pouvez sélectionner un fichier CSV comprenant des données au format **Nom, CUID et Statut** comme entrée pour *Documents*.

> **Remarque**
>
> Si le champ de saisie de tâche accepte le **CUID**, et que vous sélectionnez un fichier CSV qui contient d'autres paramètres y compris **CUID**, le champ de saisie n'utilise alors que les valeurs de colonne **CUID** provenant du fichier CSV. Voici ci-dessous un exemple de données CSV :
>
> Nom, CUID, Statut ;
>
> Charting, AW4AVT1AUhVAogA6P7OQv9c, Réussite ;
>
> RapportVentes, BW3AVT1AUHVAogA743QCDsD, Réussite ;
>
> Dans cet exemple, le champ de saisie utilise AW4AVT1AUhVAogA6P7OQv9c et BW3AVT1AUhVAogA743QCDsD, et ignore les autres valeurs.

Séparateur de colonnes et de lignes

Le séparateur de colonnes pris en charge est **,**. Le séparateur de lignes est **;**. Un séparateur de colonnes et de lignes sépare, dans un champ de saisie, les données au format colonne et ligne. Voici ci-dessous un exemple de données CSV :

Nom, CUID, Statut ;

Charting, AW4AVT1AUhVAogA6P7OQv9c, Réussite ;

RapportVentes, BW3AVT1AUHVAogA743QCDsD, Réussite ;

Ici, la virgule indique que **Nom, CUID et Statut** sont des colonnes, tandis que le point-virgule indique la fin de la ligne.

> **Remarque**
>
> Si un fichier CSV est une entrée pour le modèle de tâche *Lire la réserve de travail*, le séparateur de colonnes est alors **,**. Le séparateur de lignes est **;** ou une nouvelle ligne.

> **Attention**
>
> Une valeur dans les données CSV ne doit contenir ni virgule ni point-virgule.

22.7.5.1.3 À propos des informations de paramètres

Vous pouvez afficher les informations de paramètres après développement et sélection d'un paramètre dans le panneau d'entrée d'un scénario. Par exemple, dans le modèle de tâche Actualiser les documents, il existe un champ de saisie intitulé Documents. Lorsque vous sélectionnez le champ de saisie Documents, les informations de paramètres s'affichent.

Les informations de paramètres comprennent deux sections :

1. Paramètre d'entrée

2. Paramètre de sortie

Paramètre d'entrée

Le paramètre d'entrée explique le type d'entrée requis pour le champ sélectionné. Il est spécifique au champ de saisie dans le modèle de tâche.

Paramètre de sortie

Le paramètre de sortie explique les différentes sorties obtenues à partir de la tâche. Il est spécifique à l'ensemble de la tâche, et pas uniquement à un champ de saisie.

22.7.5.2 Modification des scénarios

Vous modifiez des scénarios dans l'Assistant du workflow.

1. Dans l'onglet *Scénarios* de l'Assistant du workflow, cliquez sur ⋯ (*Autres*) et sélectionnez *Modifier*.

   L'écran "Modifier le scénario" apparaît.
2. Dans l'écran *Modifier le scénario*, apportez les modifications requises au scénario en ajoutant/supprimant les modèles de tâche/modèles de workflow ou en modifiant les valeurs des paramètres d'entrée des modèles.
3. Sélectionnez *Enregistrer*.

   La boîte de dialogue "Enregistrer le scénario" apparaît.
4. Dans la boîte de dialogue *Enregistrer le scénario*, modifiez le nom du scénario selon vos besoins et sélectionnez *Enregistrer*.

   Les modifications apportées au scénario sont enregistrées et vous revenez à la page d'accueil de l'Assistant du workflow.

22.7.5.3 Suppression de scénarios

Vous supprimez des scénarios dans l'Assistant du workflow.

1. Dans l'onglet *Scénarios* de l'Assistant du workflow, cliquez sur ⋯ (*Autres*) et sélectionnez *Supprimer*.
2. Sélectionnez *Supprimer* dans l'avertissement qui apparaît.

   Le scénario supprimé n'est plus répertorié dans l'onglet *Scénarios* de l'Assistant du workflow.

22.7.5.4 Exécution de scénarios et affichage des résultats

Vous exécutez les scénarios sur les données de BI et affichez les résultats dans l'Assistant du workflow.

1. Dans la vue *Scénarios* de l'Assistant du workflow, cliquez sur ··· (*Autres*) et sélectionnez *Exécuter* ou *Exécuter avec le paramètre*.

   L'option *Exécuter avec le paramètre* ouvre une boîte de dialogue affichant tous les paramètres d'entrée du scénario et vous pouvez modifier les valeurs ou définir les valeurs manquantes.

   > ⓘ Remarque
   >
   > Les valeurs définies dans cette boîte de dialogue de paramètres ne sont pas enregistrées avec le scénario ; elles sont uniquement utilisées pour l'instance en cours d'exécution.

   Le scénario (vignette ou élément de liste) passe alors au statut En cours d'exécution ou En suspens. Une fois l'exécution terminée, le statut est mis à jour pour afficher la valeur pertinente (`<Réussite/Réussite partielle/Échec/En suspens/Erreur/Exécution avec une erreur>`).

2. Pour afficher les résultats du scénario (pendant qu'il est en cours d'exécution ou après son exécution réussie), cliquez ··· sur (*Autres*) et sélectionnez *Afficher les résultats*.

   > ⓘ Remarque
   >
   > Vous pouvez sélectionner l'option Afficher l'historique pour consulter les résultats des exécutions précédentes d'un scénario.

3. Sur la page *Résultats*, développez les résultats pour afficher les détails d'exécution et d'avancement pour chaque modèle de workflow et modèle de tâche dans le scénario. Une fois que vous avez affiché les résultats, vous pouvez revenir à l'écran principal à l'aide du bouton < (*Retour*).

   > ⓘ Remarque
   >
   > Vous pouvez sélectionner l'option Exporter pour enregistrer les résultats du scénario au format PDF.

   > ⓘ Remarque
   >
   > 1. Vous pouvez définir le temps maximal de réponse d'une tâche à un agent en ajoutant ce temps (en secondes) par rapport à la valeur de clé task_time_out dans le fichier wfmanager_conf.properties. Par défaut, la valeur de clé task_time_out est définie sur 86 400 secondes, c'est-à-dire un jour.
   >
   > 2. La valeur de clé task_time_out est définie pour tous les agents dans l'Assistant du workflow.

22.7.5.5 Arrêt de scénarios

Vous pouvez arrêter un scénario lorsque l'exécution de la tâche est toujours en cours.

Conditions prérequises :

Vous pouvez procédez aux étapes ci-dessous uniquement si un scénario est à l'état En cours d'exécution ou En suspens.

- Dans la vue Scénarios, sélectionnez *Autres* scénarios.
- Cliquez sur Arrêter.

> **Remarque**
>
> L'option Arrêter n'arrête pas le scénario immédiatement. Après votre sélection de l'option Arrêter, la tâche actuelle, en cours d'exécution, est d'abord terminée, puis le scénario est arrêté. Cela signifie que seules les tâches en suspens dans le scénario ne seront pas exécutées.

22.7.6 Explication des états des modèles de tâche, modèles de workflow et scénarios

États d'artéfact possibles (pour les modèles de tâche/modèles de workflow/scénarios) avec descriptions

État	Description
Créé (C)	Lorsqu'un artefact est créé mais n'a encore jamais été exécuté.
En suspens (P)	Lorsqu'un artefact est déclenché pour exécution et figure dans la file d'attente en attendant d'être exécuté.
En cours d'exécution (R)	Lorsqu'un artefact est en train d'être d'exécuté.
Réussite (S)	Lorsque tous les éléments traités sont correctement exécutés. Par exemple, les documents traités sont bien actualisés après la tâche Actualiser le document. **Remarque** Si le moindre modèle de workflow dans un scénario échoue pendant l'exécution, l'ensemble du scénario n'atteint pas l'état "Réussite".
Réussite partielle (PS)	Lorsque seuls quelques éléments traités sont correctement exécutés. Par exemple, lorsque quelques documents ne s'actualisent pas après la tâche Actualiser le document, l'état passe sur Réussite partielle.
Échec (F)	Lorsqu'aucun élément n'est exécuté correctement.
Erreur (E)	Lorsqu'un artéfact rencontre une erreur ou des exceptions lors de l'exécution.
Exécution avec une erreur (RE)	Lorsqu'un artefact rencontre une erreur sur le serveur, mais qu'il continue à s'exécuter.

État	Description
Non exécuté	Lorsqu'un modèle de tâche ou un modèle de workflow dans un scénario ne s'exécute pas en raison de la configuration de paramètres conditionnels. Par exemple, si l'administrateur choisit d'activer la condition `<En cas de réussite>` entre deux modèles de workflow, de telle sorte que le processus d'exécution n'atteint pas le modèle de workflow suivant en cas d'échec du modèle de workflow précédent. Dans ce cas, le modèle de workflow suivant et tous les modèles de workflow ultérieurs restent à l'état `<Non exécuté>`.

> **Remarque**
>
> Voici les légendes des tableaux :
>
> - TTS : statut du modèle de tâche
> - WFTS : statut du modèle de workflow
> - SS : statut du scénario

Matrice de statuts : statut des modèles de tâche et statut du modèle de workflow qui en résulte

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	S	S	E	NE	E (Erreur)
S	S	S	PS	NE	PS (Réussite partielle)
S	S	PS	F	NE	F (Échec)
S	PS	F	R	NE	R (En cours d'exécution)
S	E	NE	NE	NE	E (Erreur)
S	E	RE	NE	NE	RE (Exécution avec une erreur)

La matrice ci-dessous explique l'impact que le statut de chaque modèle de workflow exerce sur le statut global du scénario.

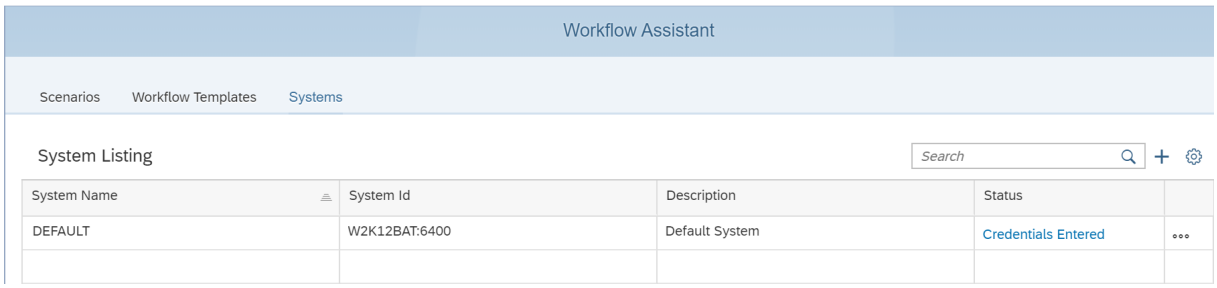
Matrice de statuts : statut des modèles de workflow et statut du scénario qui en résulte

WFTS1	WFTS2	WFTS3	WFTS4	WFTS5	SS
S	S	S	E	NE	E (Erreur)
S	S	S	PS	NE	PS (Réussite partielle)
S	S	PS	F	NE	F (Échec)
S	PS	F	R	NE	R (En cours d'exécution)
S	E	NE	NE	NE	E (Erreur)
S	E	RE	NE	NE	RE (Exécution avec une erreur)

22.7.7 Utilisation de Systèmes

L'onglet *Systèmes* permet d'enregistrer plusieurs infrastructures BI. Depuis *Systèmes*, vous pouvez accéder à vos infrastructures BI enregistrées.

Instantané de l'onglet *Systèmes*



Vous pouvez effectuer les actions suivantes dans l'onglet *Systèmes* :

- Ajouter (enregistrer) un nouveau système

  > → N'oubliez pas
  >
  > Vous devez obligatoirement enregistrer vos systèmes dans cet onglet pour pouvoir utiliser ces systèmes dans d'autres vues telles que des *Scénarios* et *Modèles de workflow*.

- Modifier (éditer ou supprimer) un système existant
- Vous connecter (ou vous déconnecter) au système en saisissant vos références de connexion (`User Name, Password, Authentication`)

  > ⓘ Remarque
  >
  > Le système sur lequel vous avez installé l'Assistant du workflow est répertorié comme système "Par défaut" dans l'onglet *Systèmes*. Cependant, pour vous connecter à cette infrastructure, vous devez saisir vos références de connexion.

- Personnaliser les colonnes affichées dans la vue Systèmes

22.7.7.1 Enregistrement d'un nouveau système BI

Pour vous connecter à votre système BI autorisé et utiliser les fonctionnalités de l'Assistant du workflow, il est nécessaire au préalable d'enregistrer (ajouter) des systèmes BI dans l'Assistant du workflow.

Pour enregistrer des systèmes, suivez la procédure décrite ci-dessous :

1. Connectez-vous à l'Assistant du workflow.
2. Sur la page *Accueil*, accédez à l'onglet *Systèmes*.

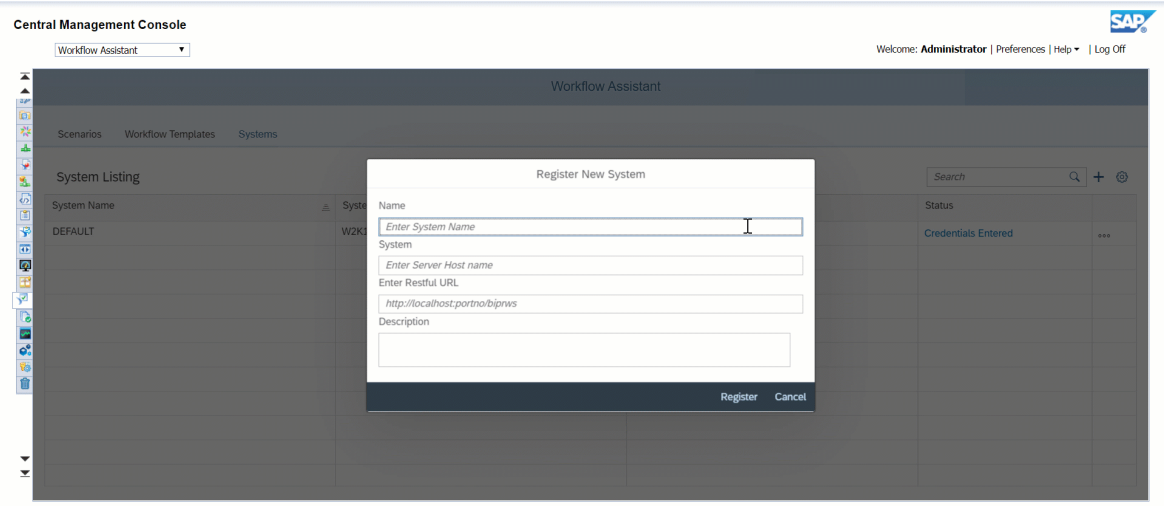
   Cette vue répertorie vos systèmes enregistrés disponibles.
3. Cliquez sur l'icône + (*Ajouter*).

   La boîte de dialogue "Enregistrer nouveau système" apparaît.

4. Pour `<Nom>`, saisissez un alias vous permettant de discerner votre système.
5. Pour `<Système>`, saisissez le nom d'hôte du serveur ou l'adresse IP qui identifie votre ordinateur ou votre cluster d'ordinateurs.
6. Pour `<URL RestFul>`, saisissez l'URL des services Web RESTful pour le serveur de la plateforme de BI. Vous pouvez également ajouter une `<Description>` pour le système.
7. Sélectionnez *Enregistrer*.

> **Remarque**
>
> Vous pouvez enregistrer un même système BI sous différents noms, mais il est recommandé de n'enregistrer un système BI qu'une seule fois dans la vue Systèmes.

Le système enregistré s'ajoute à votre liste de systèmes dans le tableau Liste de systèmes.



22.7.7.2 Modification des systèmes BI existants

La vue Systèmes vous permet de modifier vos systèmes enregistrés.

Pour modifier un système existant, suivez la procédure décrite ci-dessous :

1. Connectez-vous à l'Assistant du workflow et accédez à l'onglet *Systèmes*.
2. Dans la vue Systèmes, cliquez sur ... (*Autres*) → *Modifier* pour le système répertorié que vous souhaitez modifier.

   La boîte de dialogue *Modifier le système* apparaît.
3. Modifiez le `<nom>` (alias), le `<système>`, l'`<URL RestFul>` ou la `<description>` en fonction de vos besoins, puis sélectionnez *Terminé*.

   Les modifications sont alors reflétées dans le tableau "Liste de systèmes".

> **Remarque**
>
> Pour supprimer un système, cliquez sur (*Autres*) → *Supprimer* pour le système répertorié que vous souhaitez supprimer, puis confirmez la suppression dans la boîte de dialogue qui s'affiche.

22.7.7.3 Connexion aux systèmes BI enregistrés

Vous pouvez vous connecter à vos systèmes enregistrés à l'aide du champ `<Statut>` du tableau Liste de systèmes. Il est essentiel de se connecter au système BI pour pouvoir utiliser vos systèmes dans les scénarios de l'Assistant du workflow.

Pour vous connecter à un système BI préalablement ajouté, suivez la procédure décrite ci-dessous :

1. Connectez-vous à l'Assistant du workflow et accédez à l'onglet *Systèmes*.
2. Sélectionnez l'indicateur (*Aucune référence de connexion saisie)* sous forme de chaîne affiché dans le champ `<Statut>` des systèmes enregistrés auxquels vous n'êtes pas encore connecté.

   La boîte de dialogue "Saisir les références de connexion" apparaît.
3. Saisissez vos références de connexion au système BI (en fonction de l'autorisation accordée par l'administrateur de la plateforme) : `<Nom d'utilisateur>`, `<Mot de passe>` et `<Authentification>`. Cliquez ensuite sur *Enregistrer*.

   L'Assistant du workflow valide vos références de connexion et met à jour le `<statut>` de votre infrastructure BI en le passant sur *Références de connexion saisies* si la validation réussit. Sinon, un message d'erreur s'affiche et le `<statut>` reste inchangé.

22.7.7.4 Personnalisation de la vue Systèmes

Vous pouvez personnaliser l'apparence de la vue Liste de systèmes en modifiant la visibilité des champs (colonnes) dans la vue.

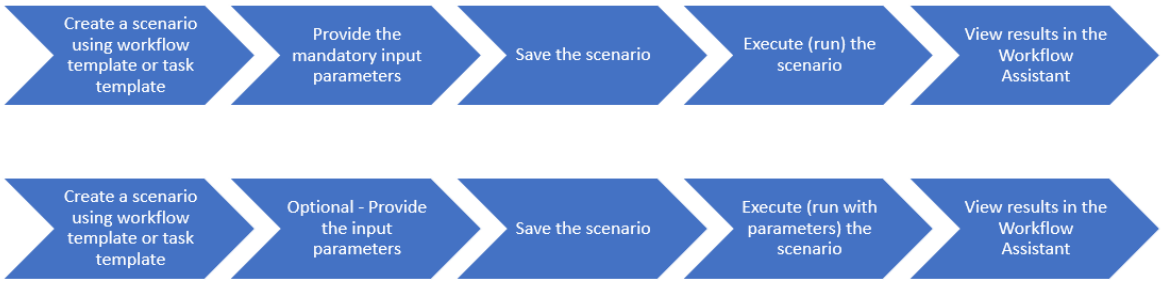
Pour masquer/afficher des colonnes spécifiques de la vue Systèmes, suivez la procédure ci-dessous :

1. Connectez-vous à l'Assistant du workflow et accédez à l'onglet *Systèmes*.
2. Cliquez sur (*Paramètres*) et désélectionnez les colonnes (en-têtes de champs) que vous souhaitez masquer dans le tableau Liste de systèmes.

   Les colonnes désélectionnées n'apparaissent plus dans le tableau Liste de systèmes.
3. Pour réinclure une colonne masquée dans la vue, cliquez sur *Paramètres* et sélectionnez à nouveau les en-têtes de champs requis.

22.7.8 Flux de processus de bout en bout de l'Assistant du workflow

Voir une représentation visuelle.



22.8 Vérification des fichiers journaux

Cette rubrique explique comment vérifier les fichiers journaux de l'Assistant du workflow.

Assistant du workflow

Pour l'Assistant du workflow, vous devez sélectionner le niveau de traçage dans le fichier *WorkflowAssistant_Trace.ini* sous `<REPINSTALL>\AdminConsole\WorkflowAssistant`. Les fichiers de trace peuvent également être configurés à l'aide d'un fichier **_Trace.ini** en définissant les variables d'environnement suivantes :

- `BO_TRACE_CONFIGDIR`, pour définir le nom du dossier des fichiers de configuration, par exemple : `C:\BOTraces\config`
- `BO_TRACE_CONFIGFILE`, pour définir le nom du fichier de configuration, par exemple : `BO_trace.ini`
- `BO_TRACE_LOGDIR`, pour définir le nom du dossier des journaux, par exemple : `C:\BOTraces`

> **Remarque**
>
> Le nom du fichier `INI` est sensible à la casse.

Créez le fichier de configuration `BO_trace.ini` comme suit :

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

Vous pouvez consultez les journaux par défaut dans `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\logging`.

23 Corbeille

23.1 Corbeille

À propos de la Corbeille

La Corbeille est une nouvelle application de la CMC. Lorsqu'un utilisateur supprime un élément du système BOE, il est déplacé dans la Corbeille, où il sera stocké temporairement jusqu'à ce que la Corbeille soit vidée. L'utilisateur peut ainsi récupérer les rapports ou dossiers supprimés par erreur et les restaurer à leurs emplacements d'origine.

L'application de la Corbeille permet à l'administrateur de :

- Initier la restauration d'un élément supprimé (tel qu'un rapport ou un dossier)
- Supprimer définitivement des éléments de la corbeille
- Effectuer un nettoyage automatique de la Corbeille

Si Corbeille est activé, vous pouvez recycler les types d'InfoObject suivants :

- Contenu de dossier personnel
- Événements
- Calendriers
- Contenu de dossier public
- Univers
- Connexions
- Catégories publiques
- Catégories personnelles
- Boîtes de réception
- Profils
- Rôles personnalisés

23.1.1 Restauration d'un élément de la corbeille

La corbeille affiche une liste d'éléments supprimés. Procédez comme suit afin de restaurer l'un des éléments :

1. Connectez-vous à la CMC.
2. Depuis le volet *Gérer* de la page d'accueil de la CMC, sélectionnez *Corbeille*.
3. Faites un clic droit sur l'élément à restaurer puis sélectionnez *Restaurer* dans le menu contextuel.

4. Cliquez sur *OK*.

   Vous pouvez accéder à l'emplacement de l'élément restauré afin de confirmer l'opération de restauration.

   > ⓘ Remarque
   >
   > Si vous restaurez un élément dans la Corbeille et qu'il existe déjà un autre élément du même nom à l'emplacement de restauration, l'élément est enregistré à l'emplacement de restauration avec le nom suivant : "<nom de l'élément> restauré(1, 2, ...)".
   >
   > Lorsque le dossier parent d'un élément dans la Corbeille est supprimé, le dossier parent est recréé là où l'élément est restauré. Toutefois, le dossier parent ne contiendra que l'élément restauré de la Corbeille.
   >
   > Vous ne pouvez ouvrir un élément ou y accéder s'il se trouve dans la Corbeille.
   >
   > Si vous supprimez un élément d'un dossier et qu'un administrateur restreint les droits de modification du dossier par la suite, vous pouvez quand même restaurer l'élément dans le dossier d'origine.

Vous avez correctement restauré un élément de la Corbeille.

23.1.2 Suppression définitive des éléments de la corbeille

En tant qu'administrateur, vous avez le droit de supprimer définitivement des éléments sélectionnés de la Corbeille ou de vider la Corbeille.

Procédez comme suit afin d'éliminer définitivement des éléments de la Corbeille :

1. Connectez-vous à la CMC.
2. Depuis le volet *Gérer* de la page d'accueil de la CMC, sélectionnez *Corbeille*.
3. Faites un clic droit sur l'élément à éliminer puis sélectionnez *Supprimer* dans le menu contextuel.
4. Cliquez sur *OK*.

Vous avez correctement éliminé un élément de la Corbeille.

23.1.3 Activation du nettoyage automatique de la Corbeille

Vous pouvez exécuter un nettoyage automatique régulier de la Corbeille.

Pour activer le nettoyage automatique de la corbeille, procédez comme suit :

1. Connectez-vous à la CMC.
2. Depuis le volet *Gérer* de la page d'accueil de la CMC, sélectionnez *Applications*.
3. Depuis la page *Applications*, sélectionnez l'application *Corbeille*.

   La boîte de dialogue *Propriétés* : *Corbeille* s'affiche.
4. Cochez la case et spécifiez (en jours) à quel intervalle le système peut lancer le nettoyage automatique d'un élément supprimé.
5. Cliquez sur *Enregistrer et fermer*.

Vous avez correctement activé le nettoyage automatique de la Corbeille.

24 Audit

24.1 Présentation

L'audit vous permet de conserver un enregistrement des événements significatifs sur les serveurs et applications, ce qui vous donne une idée des informations consultées, du type d'accès, des modifications et de la personne qui exécute ces opérations. Ces informations sont enregistrées dans une base de données appelée le Magasin de données d'audit. Une fois les données enregistrées dans le magasin de données d'audit, vous pouvez concevoir des rapports personnalisés selon vos besoins. Vous pouvez rechercher des exemples d'univers et de rapports dans SAP Communityhttp://community.sap.com/.

Dans ce chapitre, un auditeur est un système responsable de l'enregistrement ou du stockage des informations sur un événement et un candidat à l'audit est un système quelconque responsable de l'exécution d'un événement auditable. Dans certains cas, un seul et même système peut exécuter les deux fonctions.

Fonctionnement de l'audit

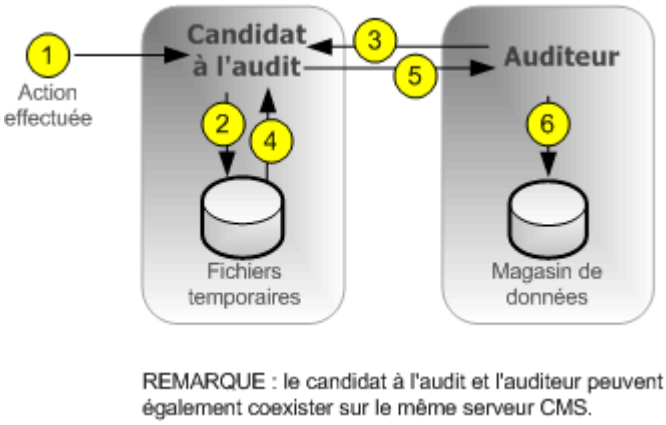
Le CMS (Central Management Server) joue le rôle d'auditeur système, tandis que chaque serveur ou application qui déclenche un événement pouvant être audité joue le rôle de candidat à l'audit. Lorsqu'un événement audité est déclenché, le candidat à l'audit génère un enregistrement et le stocke dans un fichier temporaire local. À intervalles réguliers, le CMS communique avec le candidat à l'audit pour demander ces enregistrements et écrit les données dans le magasin de données d'audit.

Le CMS contrôle également la synchronisation des événements d'audit se produisant sur différents ordinateurs. Chaque candidat à l'audit fournit un horodatage pour les événements d'audit qu'il consigne. Pour garantir la cohérence des horodatages des événements sur différents serveurs, le CMS diffuse périodiquement son heure système aux candidats à l'audit. Les candidats à l'audit comparent ensuite cette heure avec celle de leurs horloges internes. En cas d'écart, ils corrigent l'heure enregistrée pour les événements d'audit suivants.

En fonction du type de candidat à l'audit, le système utilise l'un des workflows suivants pour enregistrer les événements.

Audit de serveur

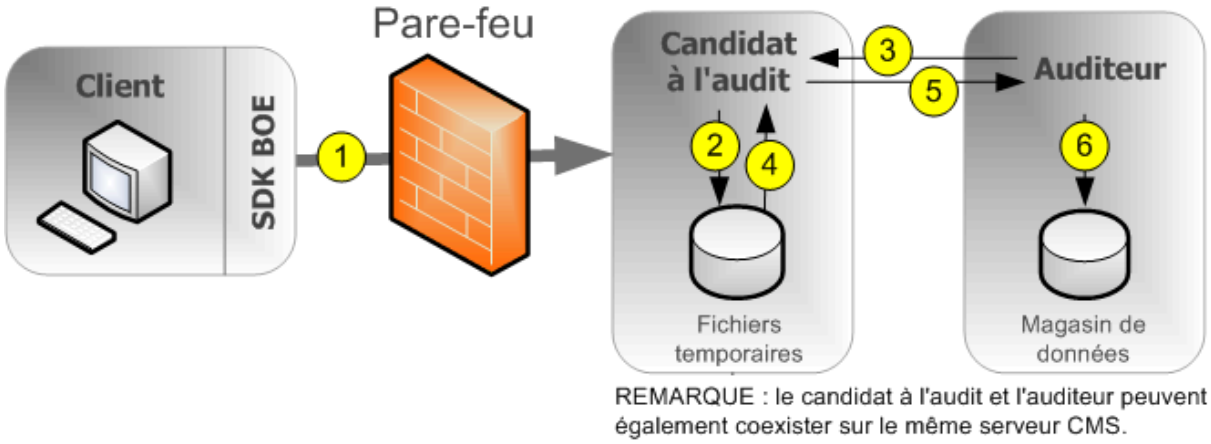
Dans le cas d'événements générés par un serveur, le CMS peut agir à la fois comme candidat à l'audit et auditeur.



1. Un événement auditable est exécuté par le serveur.
2. Le candidat à l'audit écrit les événements dans un fichier temporaire. Les étapes 1 et 2 peuvent être répétées plusieurs fois avant l'étape 3.
3. À intervalles réguliers, l'auditeur interroge le candidat à l'audit et lui demande un lot d'événements d'audit.
4. Le candidat à l'audit extrait les événements des fichiers temporaires.
5. Le candidat à l'audit transmet les événements à l'auditeur.
6. L'auditeur écrit les événements dans le magasin de données d'audit et indique au candidat à l'audit de supprimer les événements des fichiers temporaires.

Audit de connexion client pour les clients connectés via CORBA

Cela inclut des applications telles que SAP BusinessObjects Web Intelligence.



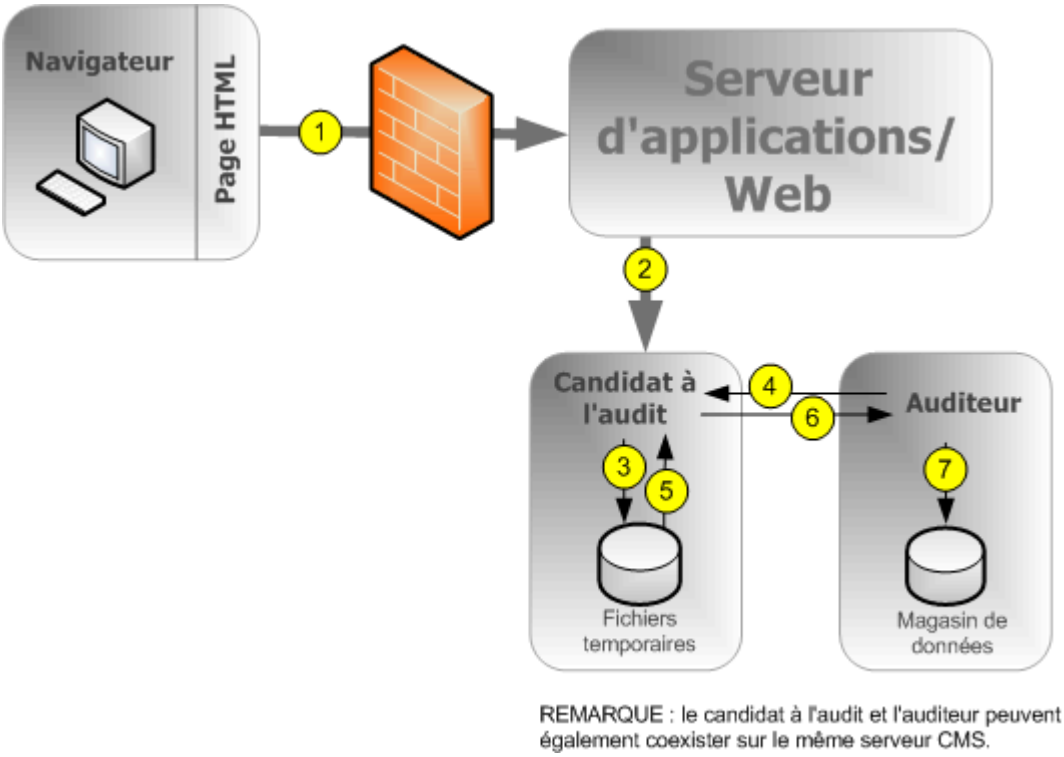
1. Le client se connecte au CMS, qui joue le rôle de candidat à l'audit. Le client fournit son adresse IP et le nom de l'ordinateur afin que le candidat à l'audit les vérifie.

> **Remarque**
>
> Un port doit être ouvert dans le pare-feu entre le CMS et le client. Le chapitre Sécurité du *Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence* contient des informations supplémentaires sur les pare-feu.

2. Le candidat à l'audit écrit les événements dans un fichier temporaire. Les étapes 1 et 2 peuvent être répétées plusieurs fois avant l'étape 3.
3. À intervalles réguliers, l'auditeur interroge le candidat à l'audit et lui demande un lot d'événements d'audit.
4. Le candidat à l'audit extrait les événements des fichiers temporaires.
5. Le candidat à l'audit transmet les événements à l'auditeur.
6. L'auditeur écrit les événements dans le magasin de données d'audit et indique au candidat à l'audit de supprimer les événements des fichiers temporaires.

Audit de connexion client pour les clients connectés via HTTP

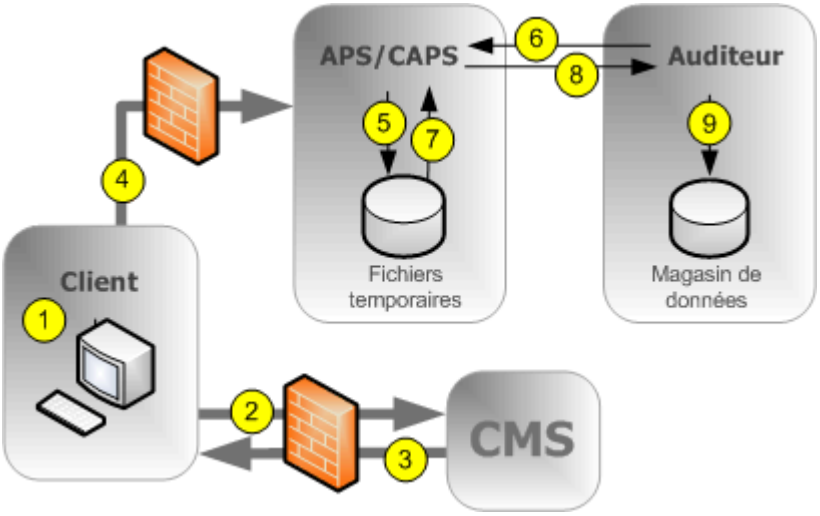
Cela inclut des applications en ligne telles que la zone de lancement BI, la CMC, SAP BusinessObjects Web Intelligence, etc.



1. Le navigateur se connecte au serveur d'applications Web et les données de connexion sont envoyées à ce serveur.
2. Le SDK de la plateforme de BI soumet la requête de connexion au candidat à l'audit (CMS), accompagnée de l'adresse IP et du nom de l'ordinateur sur lequel le navigateur est installé.
3. Le candidat à l'audit écrit les événements dans un fichier temporaire. Les étapes 1 à 3 peuvent être répétées plusieurs fois avant l'étape 4.
4. À intervalles réguliers, l'auditeur interroge le candidat à l'audit et lui demande un lot d'événements d'audit.
5. Le candidat à l'audit extrait les événements des fichiers temporaires.
6. Le candidat à l'audit envoie les événements à l'auditeur.
7. L'auditeur écrit les événements dans le magasin de données d'audit et indique au candidat à l'audit de supprimer les événements des fichiers temporaires.

Audit d'absence de connexion pour les clients connectés via CORBA

Ce workflow s'applique à l'audit d'événements SAP BusinessObjects Web Intelligence en cas de connexion via CORBA.



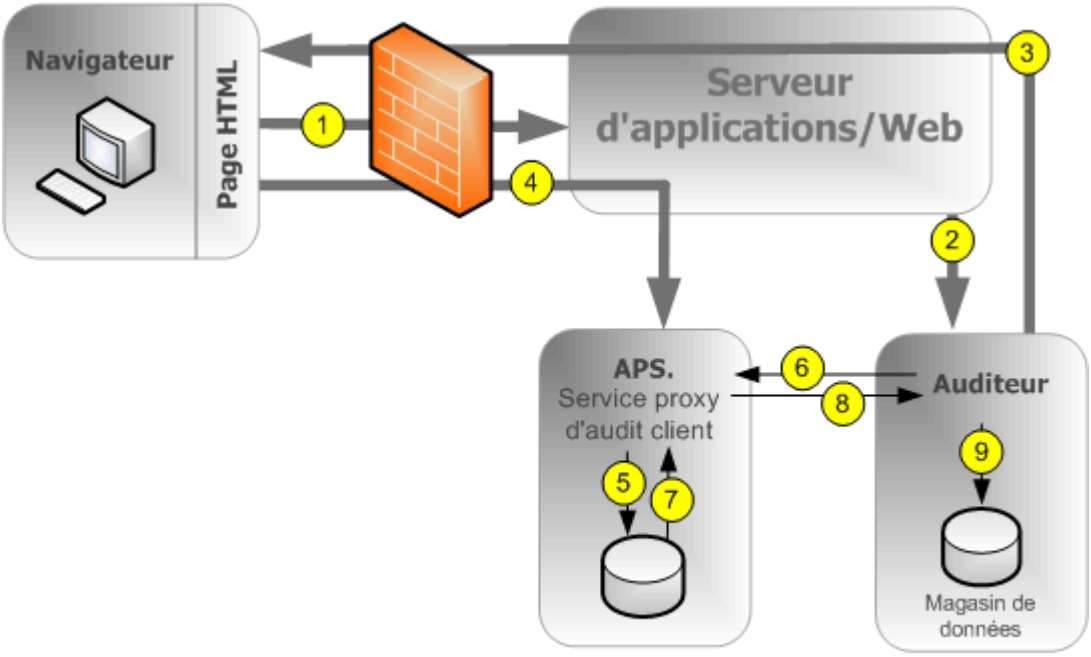
1. L'utilisateur réalise une opération pouvant faire l'objet d'un audit.
2. Le client contacte le CMS pour vérifier si l'opération est configurée pour être auditée.
3. Si l'action est configurée pour être auditée, le CMS communique ces informations au client.
4. Le client envoie les informations d'audit au service du proxy d'audit du client, lequel est hébergé sur un serveur de traitement adaptatif.

   > **Remarque**
   >
   > Un port du pare-feu doit être ouvert entre chaque client et chaque serveur de traitement adaptatif hébergeant un service du proxy d'audit du client, ainsi qu'entre chaque client et le CMS. Le chapitre Sécurité du *Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence* contient des informations supplémentaires sur les pare-feu.

5. Le service du proxy d'audit du client écrit les événements dans un fichier temporaire. Les étapes 1 à 5 peuvent être répétées plusieurs fois avant l'étape 6.
6. À intervalles réguliers, l'auditeur interroge le CAPS et demande un lot d'événements d'audit.
7. Le service du proxy d'audit du client extrait les événements des fichiers temporaires.
8. Le service du proxy d'audit du client envoie les informations sur les événements à l'auditeur.
9. L'auditeur écrit les événements dans le magasin de données d'audit et indique au service du proxy d'audit du client de supprimer les événements des fichiers temporaires.

Audit d'absence de connexion pour les clients connectés via HTTP

Ce workflow s'applique à l'audit d'événements SAP BusinessObjects Web Intelligence (à l'exception des événements de connexion) en cas de connexion via HTTP.



REMARQUE : le candidat à l'audit et l'auditeur peuvent également coexister sur le même serveur CMS.

1. L'utilisateur lance un événement susceptible d'être audité. L'application cliente contacte le serveur d'applications Web.
2. Le serveur d'applications Web vérifie si l'événement est configuré pour être audité.

   > **Remarque**
   >
   > Le schéma montre le CMS auditeur contacté, mais tout CMS du cluster peut être contacté pour ces informations.

3. Le CMS renvoie les informations de configuration d'audit au serveur d'applications Web, qui les retransmet à l'application cliente.
4. Si l'événement est configuré pour être audité, le client envoie les informations sur l'événement au serveur d'applications Web, qui les transmet au service du proxy d'audit du client, lequel est hébergé sur un serveur de traitement adaptatif (APS).
5. Le service du proxy d'audit du client écrit les événements dans un fichier temporaire. Les étapes 1 à 5 peuvent être répétées plusieurs fois avant l'étape 6.
6. À intervalles réguliers, l'auditeur interroge le CAPS et demande un lot d'événements d'audit.
7. Le service du proxy d'audit du client extrait les événements des fichiers temporaires.
8. Le service du proxy d'audit du client envoie les informations sur les événements à l'auditeur.
9. L'auditeur écrit les événements dans le magasin de données d'audit et indique au service du proxy d'audit du client de supprimer les événements des fichiers temporaires.

Clients prenant en charge l'audit

Les applications client suivantes prennent en charge l'audit :

- Édition d'Analysis pour OLAP (AOLAP)
- Zone de lancement BI (BILP)
- Gestionnaire de vues d'entreprise (BVM)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Outil de conception d'information (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Outil de gestion de la traduction (TMT, Translation Management Tool)
- Web Intelligence Rich Client (WIRC)
- Application Lumira Desktop (Discovery)
- Application Lumira Designer

> **Remarque**
>
> Au moins une instance de service du proxy d'audit du client doit être en cours d'exécution pour recueillir les événements d'audit des clients répertoriés ci-dessus.

Les clients non répertoriés ci-dessus ne génèrent pas directement d'événements, mais certaines actions accomplies par les serveurs découlant d'opérations d'applications client peuvent être auditées.

Cohérence de l'audit

Dans la plupart des cas, lorsque la fonction d'audit est correctement installée, configurée et sécurisée et que les versions appropriées de toutes les applications clientes sont utilisées, l'audit consigne tous les événements système indiqués de manière conforme et cohérente. Toutefois, il est important de garder à l'esprit que certaines conditions affectant le système et l'environnement peuvent avoir une incidence négative sur l'audit.

Il existe toujours un décalage entre l'heure à laquelle un événement se produit et l'heure de son transfert final vers le magasin de données d'audit. Des conditions telles que l'indisponibilité du CMS ou de la base de données d'audit ou la perte de la connectivité réseau peuvent augmenter ces délais.

En tant qu'administrateur système, vous devez tout faire pour éviter les conditions suivantes, qui risquent de se solder par des enregistrements d'audit incomplets :

- Un lecteur stockant les données d'audit atteint sa capacité maximale. Vérifiez que l'espace disque est suffisant pour votre base de données d'audit et les fichiers temporaires du candidat à l'audit.
- Un serveur de candidat à l'audit est supprimé à tort du réseau avant d'avoir pu transmettre tous les événements d'audit. Lors de la suppression d'un serveur du réseau, assurez-vous que suffisamment de temps est accordé pour la publication des événements d'audit dans la base de données d'audit.
- La suppression ou la modification des fichiers temporaires du candidat à l'audit.
- Un échec du disque/matériel.
- La destruction physique d'un ordinateur hébergeant l'auditeur ou le candidat à l'audit

Dans certaines conditions, les événements d'audit peuvent être dans l'incapacité d'accéder au CMS auditeur. Citons par exemple :

- Les utilisateurs avec des versions client antérieures.
- Le blocage de la transmission d'informations d'audit par des pare-feu incorrectement configurés.

> **Remarque**
>
> Les événements générés par des applications clientes contenant des informations envoyées côté client, soit en dehors de la zone sécurisée du système. Par conséquent, dans certaines conditions, ces informations peuvent ne pas être aussi fiables que les informations enregistrées par les serveurs du système.

> **Remarque**
>
> Si vous souhaitez supprimer un serveur de votre déploiement, vous devez d'abord désactiver ce serveur tout en le laissant en cours d'exécution et connecté à votre réseau jusqu'à ce que tous les événements des fichiers temporaires aient pu être transmis à la base de données d'audit. La métrique du serveur *Nombre actuel d'événements d'audit en attente* affiche le nombre d'événements d'audit en attente de transfert. Quand cette métrique atteint zéro, vous pouvez arrêter le serveur. L'emplacement des fichiers temporaires est défini par l'espace réservé `%DefaultAuditingDir%` pour ce nœud. Plus en savoir plus sur les espaces réservés, consultez le chapitre Administration du serveur.

> **Remarque**
>
> Si vous envisagez d'utiliser l'audit client, nous vous recommandons de créer un serveur de traitement adaptatif dédié pour le service du proxy de l'audit client. Cela vous garantira une performance système optimale. Afin d'augmenter la tolérance aux pannes de votre système, vous pouvez aussi envisager d'exécuter le service du proxy d'audit du client sur plusieurs APS.

Liens associés

Espaces réservés de nœud et de serveur [page 1230]

24.2 Page Audit de la CMC

La page *Audit* de la CMC se compose des zones suivantes :

- *Résumé des statuts*
- *Définir les événements*
- *Définir les détails des événements*
- *Configuration*

24.2.1 Statut de l'audit

Le *Résumé des statuts* de l'audit présente un ensemble de métriques qui vous aident à optimiser la configuration de votre audit et vous avertissent de tout problème susceptible d'affecter l'intégrité de vos données d'audit. Le résumé du statut s'affiche en haut de la page *Audit* de la Central Management Console.

Le résumé affiche également des avertissements dans les cas suivants :

- La connexion à la base de données du magasin de données d'audit est indisponible.
- Aucun service proxy d'audit client n'étant activé ou en cours d'exécution, les événements client ne peuvent pas être collectés.
- Certains événements d'un candidat à l'audit n'ont pas pu être extraits (le ou les serveurs affectés seront identifiés). Cela indique en général qu'un serveur n'a pas été correctement arrêté ou éteint et que les fichiers temporaires contiennent encore des événements.

> **Remarque**
>
> Les métriques du résumé des statuts sont marquées en vert, en jaune ou en rouge pour indiquer l'état de la fonctionnalité d'audit.

Métriques du statut d'audit

Métrique	Détails
Dernière mise à jour du magasin de données d'audit le	Date et heure auxquelles l'auditeur CMS a terminé sa dernière interrogation des candidats à l'audit pour leurs événements d'audit.
Utilisation du thread d'audit	Pourcentage du cycle d'interrogation correspondant au temps que l'auditeur CMS passe à recueillir les données des candidats à l'audit, le reste du temps correspondant aux pauses entre les interrogations. Si cette valeur atteint 100 %, le chiffre est affiché en jaune, ce qui signifie que l'auditeur continue à collecter des données des candidats à l'audit alors que l'interrogation suivante devrait commencer. Cela peut retarder l'arrivée des événements dans le magasin de données d'audit. Si cela se produit souvent ou de manière persistante, nous vous recommandons soit de mettre à jour le déploiement pour que la base de données du magasin de données d'audit reçoive les données avec un meilleur débit (par exemple, via des connexions réseau plus rapides ou du matériel de bases de données plus puissant), soit de diminuer le nombre d'événements d'audit suivis par le système.

Métrique	Détails
Durée du dernier cycle d'interrogation	Durée du dernier cycle d'interrogation en secondes. Indique le délai maximum nécessaire aux données d'événement pour atteindre le magasin de données d'audit durant le cycle d'interrogation précédent. • Si ce délai est inférieur à 20 minutes (1 200 secondes), le chiffre apparaît sur fond vert. • Si ce délai se situe entre 20 minutes et 2 heures (7 200 secondes), le chiffre apparaît sur fond jaune. • Si ce délai est supérieur à 2 heures, le chiffre apparaît sur fond rouge. Si cet état persiste et que vous jugez le délai trop long, nous vous recommandons soit de mettre à jour le déploiement pour que la base de données du magasin de données d'audit reçoive les données avec un meilleur débit (par exemple, via des connexions réseau plus rapides ou du matériel de bases de données plus puissant), soit de diminuer le nombre d'événements d'audit suivis par votre système.
Auditeur CMS	Nom du CMS agissant actuellement comme auditeur.
Nom de la connexion de la base de données du magasin de données d'audit	Nom de la connexion de base de données en cours d'utilisation par l'auditeur CMS pour se connecter au magasin de données d'audit. Pour les serveurs SQL Anywhere, SQL Server et SAP HANA, il s'agit du nom de la connexion ODBC. Pour les autres types de base de données, il s'agit du nom de la base de données et du port de connexion, suivis par le nom du serveur.
Nom d'utilisateur de la base de données du magasin de données d'audit	Nom d'utilisateur utilisé par l'auditeur CMS pour se connecter à la base de données du magasin de données d'audit.

24.2.2 Configuration des événements d'audit

La page Audit de la CMC permet d'activer un audit et de sélectionner les événements à auditer sur la totalité de votre système.

Si certains événements ou certains détails d'événement ne vous intéressent pas, vous pouvez ne pas les sélectionner afin d'optimiser les performances du système.

> **Remarque**
>
> Les événements d'audit sont transmis dans la base de données d'audit par lot, par opposition à un événement à la fois. La taille du lot est actuellement définie sur 1 000 événements d'audit.

> **Remarque**
>
> Si vous avez choisi de ne pas configurer la connexion du magasin de données d'audit lors de l'installation de la plateforme de BI, vous devez configurer une connexion à la base de données pour pouvoir configurer vos événements d'audit. Sans connexion, les événements seront toujours collectés, mais une fois la connexion établie, ils seront écrits dans le magasin de données d'audit. Pour arrêter l'audit, le niveau doit être défini sur désactivé. Voir *Paramètres de configuration des magasins de données d'audit*.

24.2.2.1 Configuration des événements d'audit

Pour configurer les événements d'audit, procédez comme suit :

1. Dans la Central Management Console, sélectionnez l'onglet *Audit*.
   La page *Audit* apparaît.
2. Définissez le curseur *Définir les événements* sur le niveau d'audit souhaité, où chaque niveau d'audit correspond à une valeur de métrique spécifique.
   - *Désactivé* : 1
   - *Minimal* : 2
   - *Par défaut* : 3
   - *Terminé* : 4
   - *Personnalisé* : 0

   Le tableau suivant présente les paramètres possibles pour le curseur et les événements capturés à chaque niveau.

Niveau d'audit	Evénements capturés
Désactivé	Aucun
Minimal	• Connexion • Déconnexion • Modification des droits • Niveau d'accès personnalisé modifié • Modification de l'audit
Par défaut	Evénements de niveau *Minimal*, plus : • Affichage • Actualisation • Invite • Créer • Supprimer • Modifier • Enregistrer • Recherche • Modifier • Exécuter • Livraison

Niveau d'audit	Evénements capturés
Terminé	Evénements de niveau *Minimal* et *Par défaut* plus : • Déclenchement • Exploration hors du périmètre • Page extraite • Configuration de la gestion des promotions • Reprise • Ajout VMS • Extraction VMS • Vérification VMS • Retrait VMS • Exportation VMS • Verrouillage VMS • Déverrouillage VMS • Suppression de VMS • Connexion au cube • Session MDAS **Remarque** Vous pouvez afficher plus d'événements lorsque les add-ons sont installés.
Personnalisé	Vous sélectionnez un ensemble d'événements personnalisé.

Remarque

Lorsque l'option *Définir les événements* est définie sur *Par défaut*, la valeur du *niveau d'audit* est 3.

Lorsque l'option *Définir les événements* est *désactivée*, la valeur du *niveau d'audit* passe de 3 à 1.

3. Sélectionnez *Personnalisé* et cliquez sur les événements que vous souhaitez capturer dans la liste figurant sous le curseur *Définir les événements*.
4. Cliquez sur les détails facultatifs sous *Définir les détails des événements* que vous souhaitez enregistrer avec les événements. Moins vous enregistrez de détails et plus les performances du système augmente.

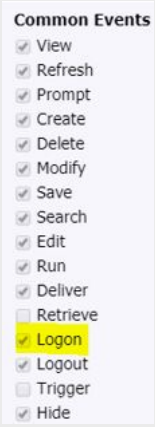
Détail	Description
Requête	Si cette option est activée, les détails concernant les événements relatifs à la *Requête* (ID de détail 25) sont enregistrés pour tout événement envoyant une requête auprès d'une base de données.
Détails du chemin d'accès au dossier	Si cette option est activée, les détails suivants sont capturés : • *Chemin du dossier d'objet (ID de détail 71)* • *Nom du dossier supérieur (ID de détail 72)* • *Chemin du dossier du conteneur (ID de détail 64)*

Détail	Description
Détails des droits	Si cette option est activée, les détails suivants sont capturés : • *Droit ajouté (ID de détail 55)* • *Droit supprimé (ID de détail 56)* • *Droit modifié (ID de détail 57)*
Détails du groupe utilisateur	Si cette option est activée, les détails suivants sont capturés : • *Nom du groupe utilisateur (ID de détail 16)* • *ID du groupe utilisateur (ID de détail 16)*
Détails de la valeur de la propriété	Si cette option est activée, les détails concernant les événements relatifs à la *Valeur de la propriété* (ID de détail 29) sont capturés lors de la mise à jour des propriétés d'un objet. Cette génération ne s'applique qu'aux événements CMC, Zone de lancement BI ou SharePoint.

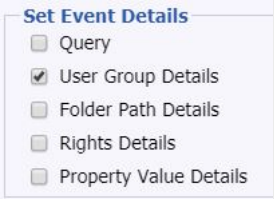
5. Cliquez sur *Enregistrer*.

> **Remarque**
>
> Pour un audit client, un délai de jusqu'à deux minutes est observé après l'application des modifications avant que le système ne commence à enregistrer les données de nouveaux événements. Veillez à tenir compte de ce délai lors de l'implémentation des modifications dans le système.

24.2.2.2 Enregistrement amélioré des détails d'événement dans le tableau des détails d'audit

> **Remarque**
>
> - Vous devez disposer des connaissances nécessaires concernant le Page Audit de la CMC [page 911], en particulier les fonctions *Evénements courants, Définir les détails des événements, Détails du groupe utilisateur* et *Connexion*, pour pouvoir utiliser les informations fournies ci-dessous.
> - *Connexion* : événement qui fournit des informations sur l'utilisateur accédant à l'application.
>
> 
>

- *Détails du groupe utilisateur* fournit des informations sur les groupes d'utilisateurs associés à un utilisateur pour chaque événement.



L'enregistrement des détails d'un groupe d'utilisateurs dans la table AUDIT_EVENT_DETAIL dépend, en partie, des sélections effectuées sous *Evénements courants* et *Définir les détails des événements* dans la page Audit. Prenez l'exemple d'un scénario dans lequel vous avez sélectionné *Connexion*, mais pas *Détails du groupe utilisateur* dans la page *Audit*. Dans ce scénario, les détails du groupe d'utilisateurs restent enregistrés pour l'événement *Connexion* dans la table AUDIT_EVENT_DETAIL. Reportez-vous au tableau ci-dessous pour comprendre le comportement dans BI 4.2 Support Package 5.

Connexion	Détails du groupe utilisateur	Comportement
Sélectionné	Sélectionné	Les détails du groupe utilisateur sont enregistrés pour tous les événements sélectionnés sous Evénements courants.
Sélectionné	Non sélectionné	Les détails du groupe utilisateur sont enregistrés uniquement pour les événements Connexion.
Non sélectionné	Non sélectionné	Les détails du groupe utilisateur ne sont pas enregistrés.
Non sélectionné	Sélectionné	Les détails du groupe utilisateur sont enregistrés pour tous les événements sélectionnés, à l'exception des événements Connexion.

24.2.3 Paramètres de configuration des magasins de données d'audit

Si vous avez choisi de ne pas configurer de base de données d'audit lors de l'installation de la plateforme de BI ou si vous souhaitez modifier l'emplacement ou les paramètres de la base de données, vous pouvez procéder de la façon suivante pour configurer la connexion au magasin de données d'audit.

C'est également là que vous pouvez configurer la durée pendant laquelle les événements d'audit seront conservés dans la base de données.

Si vous avez effectué une mise à niveau à partir d'une version précédente de SAP BusinessObjects Enterprise XI 3.x et que vous avez installé la version 3.x de Business Objects Metadata Manager (BOMM), nous vous recommandons de configurer le magasin de données d'audit de manière à utiliser la même base de données ou le même espace de table que BOMM.

> **Remarque**
>
> Si vous utilisez un Workgroup DB2 9.7 comme base de données d'audit, assurez-vous que le compte de base de données est configuré pour une taille de page supérieure à 8 Ko.

24.2.3.1 Configuration des paramètres de base de données du magasin de données d'audit

1. Dans la Central Management Console, sélectionnez l'onglet *Audit*.
2. Dans la zone *Configuration*, sous l'en-tête *Base de données du magasin de données d'audit*, sélectionnez le type de base de données que vous avez défini pour les données d'audit.
3. Dans le champ *Nom de la connexion*, saisissez le nom de la connexion que vous avez configurée pour la base de données d'audit.

Type de base de données	Nom de la connexion
IBM DB2	Nom du service
Microsoft SQL Server	DSN ODBC
MySQL	`<nomhôteserveur>,<port>,<nombasededonnées>`
Oracle	Nom du service TNS
SAP HANA	ODBC DSN
SAP MaxDB	`<nomhôteserveur>,<port>,<nombasededonnées>`
Sybase Adaptive Server Enterprise	nom du service
Sybase SQL Anywhere	ODBC DSN

   a. Si vous utilisez une base de données Microsoft SQL avec authentification Windows, activez l'option *Authentification Windows*.

4. Dans les champs *Nom d'utilisateur* et *Mot de passe*, saisissez le nom d'utilisateur et le mot de passe que vous souhaitez que l'auditeur CMS utilise pour se connecter à la base de données.
5. Dans le champ *Supprimer les événements datant de plus de (jours)*, saisissez le nombre de jours durant lequel vous souhaitez que les informations soient conservées dans la base de données. (Valeur minimale : 1, valeur maximale : 109 200.)

> **Attention**
>
> Les données dépassant le nombre de jours indiqué ici seront définitivement supprimées du magasin de données d'audit et ne pourront plus être récupérées. Vous pouvez opter pour déplacer régulièrement les enregistrements dans une base de données d'archives si vous souhaitez les conserver à long terme.

6. En cas de perte de la connexion à la base de données, si vous souhaitez reconnecter manuellement l'auditeur CMS à la base de données, désactivez l'option *Reconnexion automatique du magasin de données d'audit*.

> **Remarque**
>
> Si cette option n'est pas cochée, vous devrez rétablir manuellement une connexion au magasin de données d'audit. Pour ce faire, vous pouvez redémarrer le CMS ou activer *Reconnexion automatique du magasin de données d'audit*. Les événements seront enregistrés et resteront stockés dans les fichiers temporaires jusqu'à la reconnexion du magasin de données d'audit.

7. Cliquez sur *Enregistrer*.
8. Redémarrez tous les CMS du cluster.

> **Remarque**
>
> Le *Résumé des statuts* situé en haut de la page affiche les valeurs actuelles du magasin de données d'audit, qui peuvent être différentes de celles de la section *Base de données du magasin de données d'audit* tant que les CMS ne sont pas redémarrés.

24.3 Evénements d'audit

Le tableau suivant affiche tous les événements d'audit du système et donne une brève description de chacun. Une liste des types de service créant l'événement suit.

Événement	
Description de la modification d'audit, serveurs et clients qui génèrent le type d'événement	Les paramètres d'audit du système sont modifiés. • Service de gestion centralisée
Créer	Un nouvel objet est ajouté au système. • Services des commentaires BI • Service de gestion centralisée • Service de modification et de visualisation Crystal Reports • Desktop Intelligence • Service du moteur d'informations • Gestion du cycle de vie • Web Intelligence • Service commun Web Intelligence • Description, serveurs et clients qui génèrent les services principaux Web Intelligence • Service de traitement Web Intelligence
Connexion au cube	Une opération de connexion au cube OLAP est effectuée. • Service MDAS (Multi-Dimensional Analysis Service) • Applications d'analyse

Événement	
Niveau d'accès personnalisé modifié	Les informations concernant les privilèges sont modifiées. • Service de gestion centralisée
Supprimer	Un objet est supprimé du système. • Services des commentaires BI • Service de gestion centralisée • Service de gestion du cycle de vie
Livraison	Un objet est envoyé ou livré à vers une destination. • Service de planification de la mise à jour de l'authentification • Service de gestion centralisée • Service de planification Crystal Reports pour Enterprise • Service de planification Crystal Reports • Desktop Intelligence • Service de planification de livraison vers la destination • Service de planification de recherche de plateformes • Service de planification de la métrique • Service de planification du programme • Service de planification des requêtes de sécurité • Service de planification d'importation d'utilisateurs et de groupes • Service de planification et de publication Web Intelligence
Exploration hors du périmètre	Un utilisateur de document Web Intelligence a réalisé une exploration avant à un niveau de détail à l'extérieur des données préchargées du rapport. • Web Intelligence • Service de traitement Web Intelligence • Services communs Web Intelligence • Services principaux Web Intelligence • Service de moteur d'informations
Modifier	Le contenu d'un objet est modifié. • Application Espaces de travail BI • Desktop Intelligence • Service du moteur d'informations • Web Intelligence • Service commun Web Intelligence • Services principaux Web Intelligence • Service de traitement Web Intelligence
Configuration LCM	Les détails de configuration de la console de gestion du cycle de vie (LCM, Lifecycle Management) sont modifiés. • Gestion du cycle de vie

Événement	
Connexion	Un utilisateur se connecte au système. • Service de gestion centralisée
Déconnexion	Un utilisateur se déconnecte du système. • Service de gestion centralisée
Modifier	Les propriétés de fichier d'un objet sont modifiées. • Web Intelligence • Gestion du cycle de vie • Service de gestion centralisée • Services des commentaires BI
Session MDAS	Une opération de services d'analyse multidimensionnelle est effectuée. • Service MDAS (Multi-Dimensional Analysis Service)
Page extraite	Un client SAP BusinessObjects Web Intelligence extrait des informations supplémentaires du référentiel. • Service de traitement Web Intelligence • Services communs Web Intelligence • Services principaux Web Intelligence • Service de moteur d'informations
Invite	Les informations d'une invite d'objet sont saisies. • Service de mise en cache Crystal Reports • Service de planification Crystal Reports pour Enterprise • Service de planification Crystal Reports • Desktop Intelligence • Service du moteur d'informations • Live Office • Web Intelligence • Service commun Web Intelligence • Services principaux Web Intelligence • Service de traitement Web Intelligence
Actualisation	Les données d'un objet sont mises à jour à partir de la base de données à la demande de l'utilisateur. • Service de mise en cache Crystal Reports • Service de planification Crystal Reports pour Enterprise • Service de planification Crystal Reports • Desktop Intelligence • Service du moteur d'informations • Live Office • Web Intelligence

Événement	
	• Service commun Web Intelligence • Services principaux Web Intelligence • Service de traitement Web Intelligence
Extraction	Un objet est extrait du référentiel. • Service de gestion centralisée • Desktop Intelligence
Modification des droits	Les informations de sécurité d'un utilisateur, d'un groupe ou d'un objet sont modifiées. • Service de gestion centralisée
Reprise	LifeCycle Manager est utilisé pour rétablir un objet à sa version précédente. • Gestion du cycle de vie
Exécuter	Un travail est exécuté. • Service de planification de mise à jour de l'authentification • Service de planification Crystal Reports pour Enterprise • Service de planification Crystal Reports • Desktop Intelligence • Service de planification de livraison vers la destination • Service de planification de LCM • Gestion du cycle de vie • Service de planification de recherche de plateformes • Service de planification de la métrique • Service de planification du programme • Service de planification de la publication • Service de réplication • Service de planification des requêtes de sécurité • Service de planification d'importation d'utilisateurs et de groupes • Service de planification de la différence visuelle • Service de planification et de publication Web Intelligence
Enregistrer	Un objet est enregistré après avoir été mis à jour ou modifié. • Analysis, édition pour OLAP • Service de mise en cache Crystal Reports • Service de planification Crystal Reports pour Enterprise • Service de planification Crystal Reports • Service de modification et de visualisation Crystal Reports • Desktop Intelligence

Événement	
	• Service du moteur d'informations • Gestion du cycle de vie • Service MDAS (Multi-Dimensional Analysis Service) • SAP BusinessObjects Mobile • Web Intelligence • Service commun Web Intelligence • Services principaux Web Intelligence • Service de traitement Web Intelligence
Recherche	Une recherche est effectuée. • Service de recherche • Explorer • Gestion du cycle de vie
Déclenchement	Un événement de fichier est déclenché. • Service d'événement • Service de gestion centralisée
Affichage	Un objet est visualisé. • Applications d'analyse • Analysis, édition pour OLAP • Zone de lancement BI • Application Espaces de travail BI • Services des commentaires BI • CMC • Service de mise en cache Crystal Reports • Service de modification et de visualisation Crystal Reports • Desktop Intelligence • Service du moteur d'informations • Open Document • SAP BusinessObjects Mobile • Web Intelligence • Service commun Web Intelligence • Services principaux Web Intelligence • Service de traitement Web Intelligence
Ajout VMS	Un objet est ajouté au système de gestion des versions de LCM. • Gestion du cycle de vie
Vérification VMS	Un objet est vérifié dans le système de gestion des versions de LCM. • Gestion du cycle de vie
Extraction VMS	Un objet est extrait du système de gestion des versions de LCM.

Événement	
	• Gestion du cycle de vie
Exportation VMS	Une ressource est exportée du VMS. • Gestion du cycle de vie
Verrouillage VMS	Une ressource du VMS est verrouillée. • Gestion du cycle de vie
Déverrouillage VMS	Une ressource du VMS est déverrouillée. • Gestion du cycle de vie
Extraction VMS	Un objet est extrait du système de gestion des versions de LCM. • Gestion du cycle de vie
Suppression de VMS	Un objet est supprimé du système de gestion des versions de LCM. • Gestion du cycle de vie

Événements par type de service

Type de service	Types d'événement générés
Applications d'analyse	• Afficher • Connexion au cube
Service de planification de mise à jour de l'authentification	• Livraison • Exécution
Zone de lancement BI façon Fiori	Afficher
Services des commentaires BI	• Création • Suppression • Affichage • Modification • Masquer
Service de gestion centralisée	• Modification de l'audit • Création • Niveau d'accès personnalisé modifié • Supprimer • Livraison • Connexion • Déconnexion • Modification

Type de service	Types d'événement générés
	• Extraction • Modification des droits • Déclenchement
Central Management Console	Affichage
Service de planification Crystal Reports	• Livraison • Invite • Actualisation • Exécuter • Enregistrer
Service de mise en cache Crystal Reports	• Invite • Actualiser • Enregistrer • Afficher
Service de planification Crystal Reports pour Enterprise	• Livraison • Invite • Actualiser • Exécuter • Enregistrer
Service de planification Crystal Reports	• Livraison • Invite • Actualiser • Exécuter • Enregistrer
Service de modification et de visualisation Crystal Reports	• Créer • Enregistrer • Afficher
Desktop Intelligence (client)	• Livraison • Invite • Extraire • Exécuter
Processus du planificateur Desktop Intelligence	• Livraison • Exécution
Service de planification de livraison vers la destination	• Livraison • Exécution
Service d'événement	Déclencher
Service du moteur d'informations	• Créer • Exploration hors du périmètre

Type de service	Types d'événement générés
	• Modification • Page extraite • Invite • Actualiser • Enregistrer • Afficher
Service de planification de LCM	Exécuter
service LCM	• Créer • Supprimer • Configuration LCM • Modifier • Reprise • Exécuter • Enregistrer • Ajout VMS • Vérification VMS • Retrait VMS • Suppression de VMS • Exportation VMS • Verrouillage VMS • Extraction VMS • Déverrouillage VMS • Recherche
Live Office	• Invite • Actualiser
Service MDAS (Multi-Dimensional Analysis Service)	• Connexion au cube • Session MDAS • Enregistrer
OpenDocument	Afficher
Service de planification de recherche de plateformes	• Livraison • Exécution
Service de recherche de plateformes	Recherche
Service de planification de la métrique	• Livraison • Exécution
Service de planification du programme	• Livraison • Exécution
Service de planification de la publication	Exécuter
Service de réplication	Exécuter

Type de service	Types d'événement générés
SAP BusinessObjects Design Studio, version 1.3 et versions supérieures	• Connexion • Déconnexion
Service de planification des requêtes de sécurité	• Exécuter • Livraison
Service de planification d'importation d'utilisateurs et de groupes	• Exécuter • Livraison
Service de planification de la différence visuelle	Exécuter
Application Web Intelligence	• Créer • Exploration hors du périmètre • Modification • Modifier • Invite • Actualiser • Enregistrer • Afficher
Service commun Web Intelligence	• Créer • Exploration hors du périmètre • Modification • Page extraite • Invite • Actualiser • Enregistrer • Afficher
Service principal Web Intelligence	• Créer • Exploration hors du périmètre • Modification • Page extraite • Invite • Actualiser • Enregistrer • Afficher
Service de traitement Web Intelligence	• Créer • Exploration hors du périmètre • Modification • Page extraite • Invite • Actualiser • Enregistrer • Afficher

Type de service	Types d'événement générés
Service de planification et de publication Web Intelligence	• Livraison • Exécution

Propriétés et détails d'événement

Chaque événement enregistré par la plateforme de BI contient un ensemble de propriétés et de détails d'événement.

Les propriétés d'événement sont toujours générées avec un événement, bien que certaines puissent ne pas avoir de valeur si les informations ne sont pas applicables à un événement donné. Dans le magasin de données d'audit, les propriétés d'événement sont incluses dans la table qui stocke l'événement, de sorte qu'elles puissent être utilisées pour trier ou regrouper des événements lorsque vous créez des rapports.

Les détails d'événement enregistrent des informations supplémentaires concernant l'événement, qui ne sont pas incluses dans les propriétés de l'événement. Si un détail d'événement n'est pas pertinent pour un événement donné, ce détail d'événement ne sera pas généré. Il existe un ensemble d'événements courants qui peuvent être générés pour tous les types d'événement lorsqu'ils sont pertinents. Il existe également des ensembles de détails d'événement supplémentaires qui sont générés pour des types d'événement précis. Par exemple, les événements Invite enregistrent les valeurs saisies pour l'invite dans un détail d'événement, mais aucun autre type d'événement ne génère un détail d'événement de valeur d'invite. Dans le magasin de données d'audit, les détails sont stockés dans une table séparée qui est liée à l'événement parent.

Dans certains cas, les détails d'événement peuvent contenir plusieurs valeurs. Ces détails peuvent être regroupés à l'aide de l'ID de tas. Pour en savoir plus sur les ID de tas, voir la rubrique associée.

Toutes les données multilingues (telles que les noms d'objet ou de dossier) des paramètres régionaux du CMS de l'auditeur sont enregistrées dans la langue par défaut.

Informations associées

Auditing Data Store Tables [page 1240]

24.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Remarque**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Remarque**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **Remarque** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`

Event Property	Description
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

> **Remarque**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An

Event Detail	ID	Description
		event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **Remarque**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **Remarque** For View on Demand Crystal Reports this will be set to 0.

Event Detail	ID	Description
Number of Rows	63	The number of records the database server returned. **Remarque** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

Prompt

A value was entered for a prompt.

- Event Type ID: 1004

Event Detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Event Detail	ID	Description
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

Delete

User deleted an object.

- Event Type ID: 1006

Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event Detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.

Event Detail	ID	Description
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.
Old Property Value	120	A user's old email address.
New Property Value	121	The same user's new email address.

Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable.

Search

A search was conducted.

- Event Type ID: 1009

Event Detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

Edit

User edited the content of an object.

- Event Type ID: 1010

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.

Event Detail	ID	Description
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment.
Account Name	45	This records one of the following:

Event Detail	ID	Description
		• For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful

- Event Type ID: 123
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "2" indicates a named-user license logon was successful

Event Detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded.
Authentication Type	122	Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3
User Type	123	Type of the user.
Session Count	125	Count of the session is recorded.
Tenant ID	126	The ID of the tenant is recorded.
Concurrent Tenant Session	127	The count of the concurrent session of the tenant is recorded.

Logout

A user logs off.

- Event Type ID: 1015

Event Detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

Trigger

A file event is triggered.

- Event Type ID: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

24.3.1.1 Evénements de plateforme

Les événements suivants sont spécifiques à la plateforme de BI.

Modification des droits

Les droits d'un objet ont été modifiés

- ID de type d'événement : 10003

Détail d'événement	ID	Description
Droits ajoutés	55	Type de droit ajouté, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`.
Droits supprimés	56	Type de droit supprimé, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Droits modifiés	57	Type de droit modifié, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Utilisateur ou groupe principal	118	ID d'un utilisateur ou d'un groupe d'utilisateurs (principal) pour lequel les droits de sécurité ont été modifiés.
Nom d'utilisateur ou groupe principal	119	Nom d'un utilisateur ou d'un groupe d'utilisateurs (principal) pour lequel les droits de sécurité ont été modifiés.

Niveau d'accès personnalisé modifié

Un niveau d'accès personnalisé a été modifié.

- ID de type d'événement : 10004

Détail d'événement	ID	Description
Droits ajoutés	55	Type de droit ajouté, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
Droits supprimés	56	Type de droit supprimé, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Droits modifiés	57	Type de droit modifié, périmètre du nouveau droit (sur quels objets) et type d'objet auquel il a été appliqué. Les informations sont structurées selon l'exemple suivant : `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Utilisateur ou groupe principal	118	ID d'un utilisateur ou d'un groupe d'utilisateurs (principal) pour lequel les droits de sécurité ont été modifiés.

Modification de l'audit

Une modification a été effectuée sur les paramètres d'audit du système.

- ID de type d'événement : 10006

Détail d'événement	ID	Description
ID de type d'événement :	58	Enregistre l'ID du type d'événement d'audit qui a été activé ou désactivé. Si plusieurs types d'événement sont activés ou désactivés en une seule action, un détail d'événement sera généré pour chaque type d'événement.

Détail d'événement	ID	Description
Action	59	Enregistre quels événements d'audit ont été activés ou désactivés.
Nouveau niveau d'audit	60	Si le niveau d'audit du détail est modifié, enregistre le nouveau paramètre de niveau (par exemple :désactivé, minimal ou par défaut).
Ancien niveau d'audit	61	Si le niveau d'audit du détail est modifié, enregistre le précédent paramètre de niveau (par exemple :désactivé, minimal ou par défaut).
Option d'audit	62	Si un détail facultatif est activé ou désactivé, le détail modifié est enregistré, ainsi que l'action effectuée (activé ou désactivé). Si plusieurs détails sont activés ou désactivés par une seule action, un enregistrement détaillé sera généré pour chaque détail modifié.
Connexion du magasin de données d'audit (ADS)	78	Si la connexion du magasin de données d'audit est modifiée, enregistre les paramètres de la nouvelle connexion selon le format suivant : `TypeBDD=Oracle,NomBDD=MonADS,NomUtilisateur=USR1,MotDePasse="*****",ConnexionUnique=désactivée,ReconnexionBDD=activée`. Seuls les détails modifiés sont enregistrés. Par exemple, si seul le nom d'utilisateur a été modifié, seul `NomUtilisateur="nouveau"` sera enregistré. **Remarque** Les informations de mot de passe sont toujours masquées par `*` dans la base de données.
Intervalle de suppression automatique	105	Ce détail enregistre toute modification du champ *Supprimer les événements datant de plus de* dans la page Audit de la CMC. Cela définit le nombre de jours pendant lesquels les informations d'audit seront gérées dans l'ADS.

24.3.1.2 Événements de commentaire

Les droits suivants sont spécifiques à **Commentaires BI** dans la plateforme de Business Intelligence.

Ajouter un commentaire

Cet événement est généré lorsque vous ajoutez un nouveau commentaire, lorsque vous dupliquez un commentaire et lorsque vous ajoutez des commentaires en bloc. Lorsque vous ajoutez un commentaire, seuls les ID de document parent sont enregistrés. En cas de doublon ou d'ajout de commentaires en bloc, tous les détails des événements mentionnés dans le tableau ci-dessous sont enregistrés.

ID de type d'événement : 11001

Détail d'événement	ID	Description
ID de document parent	12	Enregistre l'ID de l'objet.
Description	24	Enregistre toutes les informations supplémentaires dans l'événement.
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement.
Nom du fichier	18	Enregistre le nom de fichier de l'objet.

Recevoir un commentaire

L'événement est généré lorsque vous affichez un commentaire.

ID de type d'événement : 11002

Détail d'événement	ID	Description
ID de document parent	12	Enregistre l'ID de l'objet.
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement.

Modifier un commentaire

L'événement est généré lorsque vous modifiez un commentaire existant.

ID de type d'événement : 11003

Détail d'événement	ID	Description
ID de document parent	12	Enregistre l'ID de l'objet.

Supprimer un commentaire

L'événement est généré lorsque vous supprimez un commentaire existant.

ID de type d'événement : 11004

Détail d'événement	ID	Description
ID de document parent	12	Enregistre l'ID de l'objet.

Masquer un commentaire

L'événement est généré lorsque vous masquez un commentaire.

ID de type d'événement : 11005

Détail d'événement	ID	Description
ID de document parent	12	Enregistre l'ID de l'objet.

24.3.1.3 Evénements de SAP BusinessObjects Web Intelligence

Les événements suivants sont spécifiques au composant SAP BusinessObjects Web Intelligence.

Exploration hors du périmètre

Un utilisateur a exploré hors du périmètre du rapport.

- ID de type d'événement : 10201

Détail d'événement	ID	Description
Instance d'objet	11	Enregistre si l'événement est le résultat d'une mise à jour planifiée ou d'un

Détail d'événement	ID	Description
		utilisateur visualisant l'objet ("0" = résulte d'un utilisateur visualisant l'objet, "1" = résulte d'une actualisation planifiée de l'objet).
Nombre de lignes	63	Nombre de lignes retournées par le serveur de base de données.
Requête	25	Enregistre la requête utilisée pour actualiser les données (facultatif, défini dans la CMC).
Nom de l'objet d'univers	31	Nom de l'univers utilisé par le document. Une instance est enregistrée pour chaque univers auquel a accédé le document.
ID de l'univers	32	CUID de l'univers utilisé par le document. Une instance est enregistrée pour chaque univers auquel a accédé le document.

Page extraite

La page de document Web Intelligence a été extraite.

- ID de type d'événement : 10202

Détail d'événement	ID	Description
Nom du rapport Web Intelligence	10220	Enregistre le nom du rapport du document Web Intelligence visualisé.
Type de sortie	10221	Format de sortie du document visualisé (par exemple : • `xml.ro` pour WebIntelligence • `pdf` pour Adobe Acrobat • `xls` pour Microsoft Excel • `text/xml` si inconnu
Numéro de page	10222	Enregistre le numéro de la page du rapport du document Web Intelligence visualisée. NB : • « 0 » lorsque cette donnée ne peut pas être extraite (par exemple PDF) • « -1 » en cas d'erreur

Statistiques BW

> **Remarque**
>
> Ces événements d'audit sont directement envoyés à SAP BW. Ils sont répertoriés ci-dessous pour référence en tant qu'événements de Web Intelligence, mais ils ne sont pas stockés dans le magasin de données d'audit de la plateforme de de BI. Ils sont disponibles à compter de la version 4.2 SP03.

Option	Valeurs possibles	Description

Nom long
`sap.sal.bics.postBWstatistics`
Nom court
`postBWstatistics`
Valeur par défaut : `false`
	`true`
	`false`
		Active les événements de statistiques BW suivants :
		• 20100 : extrait les membres de la caractéristique BEx
		• 20101 : extrait les résultats de la requête BEx
		• 20102 : soumet les variables BEx
		• 20103 : ouvre une requête BEx à l'aide de l'API BICS.
		• 20104 : lance la synchronisation avec BW
		• 20105 : définit la chaîne d'entrée de la variable

24.3.1.4 Evénements de SAP BusinessObjects Analysis, édition pour OLAP

Session MDAS

Une opération de session MDAS est effectuée

- ID de type d'événement : 10300
- Statuts :
  - "0" = ouverture réussie d'une nouvelle session.
  - "1" = échec d'une nouvelle session.
  - "2" = la session existante est fermée.

Connexion au cube MDAS

Une opération de connexion au cube est effectuée.

- ID de type d'événement : 10301
- Statuts :

- "0" = ouverture réussie d'une nouvelle connexion.
- "1" = échec d'une nouvelle connexion.
- "2" = une connexion existante est fermée.

Détail d'événement	ID	Description
ID de connexion	94	Identifiant unique de la connexion.
Connection Name (Nom de la connexion)	95	Nom de la connexion.
Type de fournisseur	96	Type de fournisseur pour le cube
Nom du cube	97	Nom complet du cube utilisé.

24.3.1.5 Evénements de la console de gestion des promotions SAP BusinessObjects

Les événements suivants sont propres au composant Gestion des promotions pour SAP BusinessObjects.

Détails communs de l'outil de gestion des promotions SAP BusinessObjects

Tous les événements de gestion des promotions possèdent les détails supplémentaires suivants.

Détail d'événement	ID	Description
Cluster d'éléments	6	CUID des clusters affectés lorsque l'outil de gestion des promotions effectue une opération sur des objets se trouvant dans des clusters différents. Un détail d'événement sera généré pour chaque cluster affecté.
Commentaire d'élément	7	Informations supplémentaires sur l'objet.
Elément principal	8	Si l'élément est un élément principal, ce détail sera défini sur "1" ; si c'est un élément dépendant, il sera défini sur "0".
Statut d'élément	9	Si l'élément d'opération échoue, ce détail sera défini sur "1" ; sinon, il sera défini sur "0".
Opération	10	Décrit le type d'opération effectuée (par exemple Ajouter, Supprimer ou Modifier).

Configuration de l'outil de gestion des promotions SAP BusinessObjects

La configuration de la gestion des promotions est modifiée.

- ID de type d'événement : 10900

Détail d'événement	ID	Description
Configuration	100	Un utilisateur affiche la configuration de l'outil de gestion des promotions. La configuration s'affiche sous forme de paires de valeurs séparées par des virgules, par exemple : paramètres de reprise=activés, port=900.
Configuration avant	101	Si les paramètres de l'outil de gestion des promotions sont modifiés pour un objet, enregistre les paramètres de la configuration précédente. Utilise le même format que Configuration.
Configuration après	102	Si les paramètres de l'outil de gestion des promotions sont modifiés pour un objet, enregistre les paramètres de la nouvelle configuration. Utilise le même format que Configuration.
Type VMS	10900	Type du système de gestion des versions.

Reprise

Un objet a été repris dans une version précédente du VMS (système de gestion des versions).

- ID de type d'événement : 10901

Ajout VMS

Une ressource est ajoutée au VMS.

- ID de type d'événement : 10902

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le système de gestion des versions.

Extraction VMS

Une ressource est extraite du VMS.

- ID de type d'événement : 10903

Détail d'événement	ID	Description
Restaure l'objet supprimé	103	Indique si un objet extrait a été supprimé du système. "0" indique que l'objet n'a pas été supprimé ; "1" indique que l'objet a été supprimé.
Version	104	Enregistre le numéro de version du document dans le VMS.

Vérification VMS

Une ressource est vérifiée dans le VMS.

- ID de type d'événement : 10904

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le VMS.

Retrait VMS

Une ressource est validée à partir du VMS.

- ID de type d'événement : 10905

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le VMS.

Exportation VMS

Une ressource est exportée du VMS.

- ID de type d'événement : 10906

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le VMS.

Verrouillage VMS

Une ressource du VMS est verrouillée pour empêcher les utilisateurs de la modifier.

- ID de type d'événement : 10907

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le VMS.
Verrouillé par	10901	Nom d'utilisateur de la personne qui a effectué l'action.

Déverrouillage VMS

Une ressource du VMS est déverrouillée pour permettre aux utilisateurs de la modifier.

- ID de type d'événement : 10908

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le VMS.
Déverrouillé par	10902	Nom d'utilisateur de la personne qui a effectué l'action.

Suppression de VMS

Une ressource est supprimée du VMS.

- ID de type d'événement : 10909

Détail d'événement	ID	Description
Version	104	Enregistre le numéro de version du document dans le système de gestion des versions.

25 Événements

25.1 À propos des événements

Les événements sont similaires aux indicateurs et aux points de contrôles qui fournissent des informations sur les événements ou les actions qui se produisent sur le serveur. La planification basée sur des événements vous fournit un contrôle supplémentaire sur la planification des objets : vous pouvez configurer des événements afin que les objets soient traités uniquement après l'exécution d'un événement spécifié.

Voici une liste des événements disponibles sur la CMC :

Événements de Crystal Reports

Les événements de Crystal Reports déclenchent une exécution de rapport uniquement si le rapport en attente de l'événement est déjà planifié et prêt à être exécuté. Les événements de Crystal Reports peuvent être basés sur un nouveau fichier et les rapports peuvent être planifiés pour attendre le déclenchement de l'événement.

Événements personnalisés

Les événements personnalisés sont également appelés "événements manuels". Chaque événement personnalisé a deux propriétés : le nom de l'événement et la description correspondante. Les événements personnalisés sont utilisés pour déclencher des alertes vers une boîte de réception BI d'un utilisateur et l'ID de l'adresse électronique de l'utilisateur. Les événements personnalisés vous offrent également l'option de planifier des objets basés sur le déclenchement d'événement si vous paramétrez les conditions requises.

Événements de surveillance

Les événements de surveillance sont des événements gérés par le système associés à l'état de santé du service. La surveillance est une application intégrée dans la CMC qui permet aux administrateurs de surveiller la santé du système. Les aspects les plus importants de la surveillance sont les veilles et les tests.

Les veilles permettent de définir les seuils pour plus de 250 métriques au sein du système. Vous êtes informé lorsque les seuils définis sont franchis.

> Exemple
>
> Si vous avez une veille qui surveille l'espace du disque consommé par l'Output FRS, vous êtes informé lorsque cette consommation dépasse le volume spécifié pour l'espace de disque.

Événements du système

Il existe deux types d'événements de système :

- **Événements basés sur un fichier**
  Les événements basés sur un fichier se basent sur n'importe quel fichier situé sous un chemin. Par exemple, si un fichier est situé sous l'un des chemins du serveur, vous pouvez exécuter des rapports en effectuant une planification basée sur le chemin d'un fichier. Du point de vue de gestion, si vous considérez que les tables requises pour le reporting doivent être chargées de façon mensuelle/hebdomadaire/quotidienne, placer un fichier texte sous le chemin après le chargement des rapports permettra le déclenchement d'un événement de système basé sur un fichier.
- **Événements basés sur la planification**
  Les événements basés sur la planification sont utilisés pour exécuter des rapports ou des objets BI de façon séquentielle. Cette définition d'événement comprend trois actions : réussite, échec et réussite ou échec. Cela est dû au fait que le statut d'un objet en exécution, à un moment donné, peut soit être une réussite soit un échec.

Notifications d'utilisateur

Les événements de notification d'utilisateur sont utilisés par les administrateurs pour informer d'événements importants les utilisateurs finaux BI qui utilisent la zone de lancement BI. Les administrateurs peuvent informer une sélection d'utilisateurs de messages importants et leur fournir les informations correspondantes à l'heure planifiée (par exemple dans le cas d'un arrêt du système). Le message d'alerte apparaît dans une fenêtre contextuelle de notification dans l'écran de la zone de lancement BI lorsque l'utilisateur se connecte.

Événements BW

Dans le système BW, l'*Déclencher un événement BOE* (un type de processus dans une chaîne de processus BW) déclenche des événements BW pour la plateforme BI. Chaque événement BW possède un nom et une description. Les événements BW permettent de configurer une planification des rapports (basés sur une source de données BW) basée sur les événements,. Un système BW déclenche un événement BW lorsque des données sont modifiées sur le système. Les événements BW sont également utilisés pour déclencher des alertes vers la boîte de réception BI et l'ID de courrier électronique d'un utilisateur.

25.1.1 Notifications d'utilisateur

La fonctionnalité de notification permet à l'administrateur d'envoyer des messages d'alerte de la CMC à l'utilisateur. À l'aide de cette fonctionnalité, les administrateurs peuvent informer les utilisateurs de messages importants et autres informations liées (un arrêt du système par exemple). Le message d'alerte apparaît dans une fenêtre contextuelle de notification dans le coin supérieur droit de l'écran de la zone de lancement BI lorsque l'utilisateur se connecte.

25.1.1.1 Création d'un événement de notification

L'événement de notification est un plug-in planifiable. Lors de la création d'un événement de notification, l'administrateur doit spécifier la date et l'heure de "début" et de "fin". L'Adaptive Job Server responsable de la planification crée une instance de planification à l'heure de "début" spécifiée de la notification. L'AJS envoie alors l'alerte à la boîte de réception des alertes dans la zone de lancement. Ces notifications apparaissent dans le coin supérieur droit de l'écran de la zone de lancement BI.

Pour créer un événement de notification, procédez comme suit :

1. Connectez-vous à la CMC.
2. Sur la page d'accueil de la CMC, sélectionnez *Événements* dans le menu déroulant.
3. Dans le volet *Événements* à gauche, cliquez avec le bouton droit sur *Notifications d'utilisateur* et accédez à *Nouveau* > *Nouvelle notification*.

   La fenêtre contextuelle *Nouvelle notification* apparaît.
4. Pour planifier un message de notification, procédez comme suit :
   a. Sélectionnez le fuseau horaire requis depuis le menu déroulant *Fuseau horaire*.
   b. Définissez la *Date/Heure de début* requise.
   c. Définissez la *Date/Heure de fin* requise.

   > **Remarque**
   >
   > - L'heure de *fin* ne peut pas être antérieure à l'heure de *début*.
   > - La différence entre l'heure de *début* et l'heure de *fin* ne peut pas être supérieure à 14 jours.
   > - Indépendamment du fuseau horaire sélectionné, l'heure de *début* ne peut pas être antérieure à l'heure du serveur CMS. Si l'heure de *début* est antérieure à celle du serveur CMS, la notification ne sera pas déclenchée.

   d. Dans la zone *Titre de la notification*, saisissez le titre de la notification.

   > **Remarque**
   >
   > Le *Titre de la notification* ne peut pas dépasser 256 caractères.

   e. Dans la zone *Description*, saisissez une description appropriée de la notification.

   > **Remarque**
   >
   > La *Description* ne peut pas dépasser 1024 caractères.

   > **Remarque**
   >
   > Vous pouvez choisir d'envoyer une notification à l'adresse électronique de l'utilisateur en cochant la case *Envoyer ce message comme notification à un ID d'adresse électronique d'utilisateur*.
5. Cliquez sur *OK*.

Vous avez correctement créé un événement de notification.

> **Remarque**
>
> Dans la page Propriétés de notification, l'heure de création et de modification correspond à l'heure du serveur CMS.
>
> L'administrateur peut désactiver la fenêtre contextuelle automatique de la bannière de notifications dans la zone de lancement BI en modifiant le fichier `BIlaunchpad.properties` et en désactivant l'interrogation en définissant le champ `Notification.enabled` sur `false`. Pour que l'interrogation de notification fonctionne par défaut, la propriété `pinger.enabled` doit être activée dans le fichier `global.properties`. Si l'interrogation et le ping ne sont pas activés, la fenêtre contextuelle de notification apparaît uniquement lorsque l'utilisateur actualise la page, se connecte pour la première fois ou se reconnecte une fois que la notification est active.
>
> L'interrogation se produit toutes les trois minutes dans la zone de lancement.

25.1.1.2 Sélection d'un public pour une notification

La fonctionnalité de notification vous permet de sélectionner le public requis pour chaque notification créée.

Procédez comme suit pour sélectionner le public d'une notification :

1. Faites un clic droit sur la notification créée puis sélectionnez *Gérer les abonnés* dans le menu contextuel.

   La fenêtre contextuelle *Gérer les abonnés* apparaît.
2. Dans le volet *Liste d'abonnés*, sélectionnez *Ajouter*.

   La fenêtre contextuelle *Ajouter des abonnés* apparaît.
3. Sélectionnez les utilisateurs ou groupes d'utilisateurs que vous souhaitez notifier.
4. Cliquez sur *Ajouter des inscriptions par défaut*.

   La fenêtre contextuelle *Ajouter des abonnés* disparaît.
5. Dans la fenêtre contextuelle *Gérer les abonnés*, sélectionnez *Enregistrer et fermer*.

Vous avez correctement sélectionné le public d'une notification.

> **Remarque**
>
> - Vous ne pouvez pas modifier la liste d'abonnement après le déclenchement de la notification.
> - Vous pouvez désormais envoyer des notifications aux utilisateurs OpenDocument.

25.1.1.3 Modification d'un événement de notification

Pour modifier un événement de notification, procédez comme suit :

1. Connectez-vous à la CMC.
2. Sur la page d'accueil de la CMC, sélectionnez *Événements* dans le menu déroulant.
3. Dans le volet *Événements* à gauche, sélectionnez *Notifications d'utilisateur*.

4. Faites un clic droit sur la notification à modifier puis sélectionnez *Modifier l'événement* dans le menu contextuel.

   La boîte de dialogue *Modifier l'événement* s'affiche.
5. Modifiez les paramètres requis de l'événement de modification.

   > **Remarque**
   >
   > Il est possible de modifier les paramètres suivants d'un événement de notification :
   > - Fuseau horaire
   > - Date/heure de début
   > - Date/heure de fin
   > - Titre de la notification
   > - Description
   > - Gérer les abonnés
6. Cliquez sur *OK*.

Vous avez correctement modifié un événement de notification.

> **Remarque**
>
> Vous pouvez modifier un événement de notification en accédant à *Événements* > *Notifications d'utilisateur* > *Propriétés* >, la notification sera déclenchée uniquement si vous sélectionnez *OK* dans la page *Modifier l'événement*.

26 Recherche de plateformes

26.1 Description de la recherche de plateformes

La recherche de plateformes permet de rechercher un contenu au sein du référentiel de la plateforme de BI. Elle permet d'affiner les résultats de la recherche en les regroupant par catégories et en les classant par niveau de pertinence.

Dans cette version de la plateforme de BI, la recherche de plateformes contient les fonctionnalités suivantes :

- Effectuer une recherche sur le contenu de la plateforme de BI.
- Suggérer une requête pour créer un document si un document existant ne peut être trouvé.
- Prendre en charge à la fois l'indexation continue et planifiée.
- Prendre en charge l'indexation dans un environnement en cluster.
- Définir et modifier le niveau d'indexation.
- Fournir des options de configuration de recherche avancée.
- Prendre en charge la recherche et l'indexation multilingues.
- Fournir une syntaxe de recherche avancée.
- Prendre en charge les métadonnées, le contenu et les facettes dynamiques.
- Prendre en charge l'auto-guérison sur la base de la charge système.

> **Remarque**
>
> Si vous effectuez une migration de la version précédente vers la nouvelle version, l'index n'est pas inclus dans la migration.

26.1.1 SDK de recherche de plateformes

La recherche de plateformes prend également en charge un SDK public qui sert d'interface entre l'application client et l'application de recherche de plateformes. Il est fourni pour vous aider à personnaliser le service de recherche et à l'intégrer à votre application.

Lorsqu'un paramètre de requête de recherche est envoyé via l'application client à la couche du SDK, cette dernière convertit le paramètre de requête au format codé XML et le transmet au service de recherche de plateformes.

Pour en savoir plus sur l'API de recherche de plateformes, voir le guide *Business Intelligence platform Java API Reference*.

26.1.2 Environnement en cluster

La recherche de plateformes peut partager la charge à travers plusieurs nœuds dans un environnement en cluster. Le déploiement dans un environnement en cluster optimise les ressources système et améliore les performances des serveurs.

La recherche de plateforme prend en charge aussi bien la mise en cluster horizontale que verticale pour les fonctions de recherche et d'indexation. Avec les environnements en cluster, elle optimise les performances des processus de recherche et d'indexation.

Pour plus d'informations sur la configuration de l'emplacement de l'index de recherche de plateformes dans un environnement en cluster, consultez cette note SAP.

Equilibrage de charge

La recherche de plateformes prend en charge l'équilibrage de charge pour l'indexation et la recherche. Dans un environnement en cluster, les requêtes d'indexation et de recherche peuvent être exécutées sur plusieurs nœuds pour partager la charge. Chaque nœud fonctionne indépendamment pour indexer le contexte et créer des index delta. Toutefois, seul un nœud du cluster agit en tant qu'index maître et fusionne les index delta dans l'index maître. Tous les nœuds peuvent accéder à l'index maître. Les requêtes de recherche simultanées sont possibles.

Basculement

Le mécanisme de basculement garantit à l'utilisateur la possibilité de poursuivre la recherche et l'indexation sans interruption. Lorsqu'un nœud du cluster devient indisponible en raison d'une panne technique ou d'activités liées à la maintenance, un autre nœud reprend automatiquement le processus des requêtes d'indexation et de recherche.

26.2 Installation de la recherche de plateformes

26.2.1 Déploiement d'OpenSearch

La recherche de plateformes prend en charge le standard OpenSearch, permettant les applications client d'utiliser le standard ou format OpenSearch pour communiquer avec la recherche de plateformes. OpenSearch n'est pas installé par défaut avec la suite SAP BusinessObjects Business Intelligence, l'utilisateur doit donc le déployer manuellement sous forme de fichier WAR (`opensearch.war`) séparé sur un serveur d'applications tel que Tomcat, ou en utilisant l'outil WDeploy. Le fichier est copié dans le répertoire `<REPINSTALL>\warfiles\OpenSearch` par le programme d'installation.

> **Remarque**
>
> Les programmes client doivent respecter les normes OpenSearch pour communiquer avec la recherche de plateformes.

> **Remarque**
>
> Lorsque vous installez la plateforme de BI, le serveur d'applications Tomcat est installé par défaut.

26.2.1.1 Déploiement manuel

Pour déployer OpenSearch dans un environnement de plateforme de BI, procédez comme suit :

1. Accédez à l'emplacement suivant : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Copiez le dossier OpenSearch dans `<REPINSTALL>\tomcat\webapps\`.
3. Modifiez les paramètres de configuration dans le fichier `\OpenSearch\WEB-INF\config.properties` :
   - CMS : le nom du CMS avec numéro de port : `<Nom du CMS>:<Numéro de port>`.
   - OpenDocURL : l'URL de l'application OpenDocument : `http://<hôtetomcat>:<port du connecteur>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   - Proxy.rpurl : le nom du serveur proxy inverse est requis si vous souhaitez en utiliser un.
   - Proxy.opendoc.rpurl : le nom du serveur proxy inverse opendoc est requis si vous souhaitez utiliser le proxy inverse.
4. Redémarrez le serveur d'applications Tomcat pour déployer OpenSearch.

26.2.1.2 Déploiement à l'aide de WDeploy

Pour Windows, les commandes sont décrites comme `wdeploy.bat <paramètres>`. Pour UNIX, les commandes sont décrites comme `wdeploy.sh <paramètres>`.

1. Mettez à jour le fichier `config.<ServeurApplications>` qui se trouve à l'emplacement `<RepInstall>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` avec les paramètres du serveur d'applications Web requis (par exemple, répertoire d'installation, nom de l'instance, port, nom d'utilisateur et mot de passe de l'administrateur).
2. Modifiez les paramètres suivants dans le fichier `<RepInstall>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties` :
   a. Pour le paramètre `CMS`, saisissez `<NomCMS>:<Port>`.
   b. Pour le paramètre `OpenDocURL`, saisissez l'URL de l'application OpenDocument.

      L'URL doit être `http://<HôteServeurApplicationsWeb>:<PortConnecteur>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   c. (Requis pour un proxy inverse) Pour le paramètre `Proxy.rpurl`, saisissez le nom du serveur proxy inverse.

d. (Requis pour un proxy inverse) Pour le paramètre `Proxy.opendoc.rpurl`, saisissez le nom du serveur proxy inverse de l'application OpenDocument.

3. Exécutez la commande `wdeploy.bat <ServeurApplicationsWeb> -Dapp_source_tree=<ApplicationWebOpenSearchDossierParent> -DAPP=OpenSearch deploy` de `<RepInstall>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   La commande suivante, par exemple, permet de déployer OpenSearch sur un serveur d'applications Web WebSphere 7 :

```
wdeploy.bat websphere7 -Dapp_source_tree="<RepInstall>\SAP BusinessObjects
Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

4. Redémarrez le serveur d'applications Web.

26.2.2 Configuration du proxy inverse

Pour déployer des applications Web sur un serveur d'applications Web situé derrière le serveur proxy inverse, configurez ce dernier de sorte à mapper les requêtes d'URL entrantes au fichier WAR correspondant.

Pour illustrer les étapes de configuration, le serveur proxy inverse Apache 2.2 est utilisé comme exemple. Pour configurer le serveur proxy inverse Apache 2.2 pour OpenSearch :

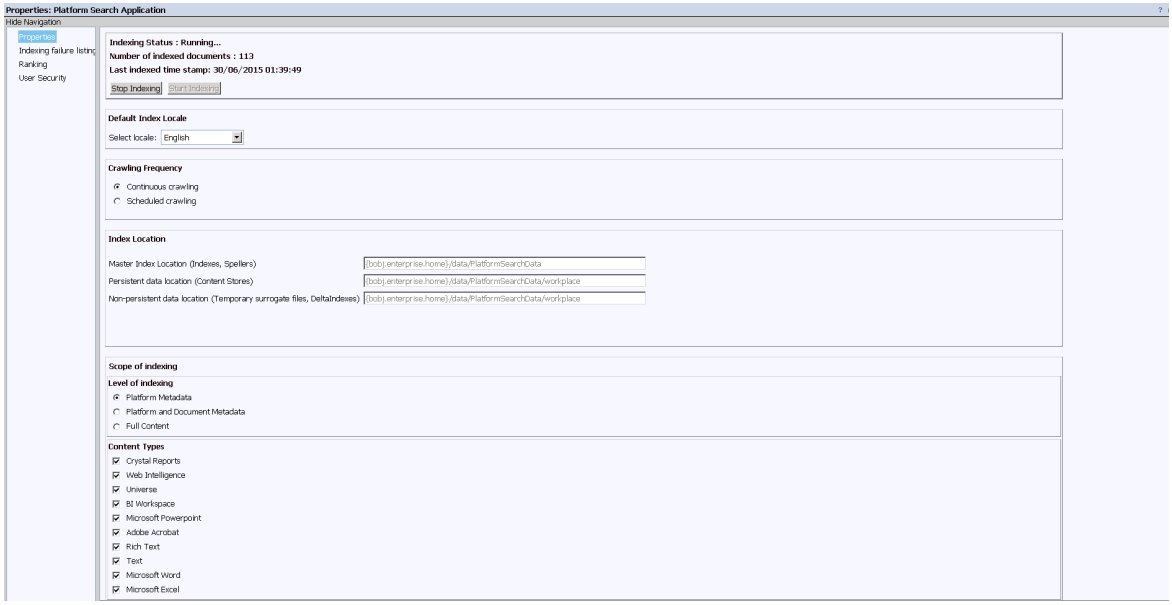
1. Configurez le proxy inverse et effectuez les modifications dans le fichier `WEB-INF\config.properties` de OpenSearch.
2. Activez les paramètres de contexte suivants et modifiez les valeurs en conséquence.
   - `proxy.rpurl` : URL du proxy inverse pour OpenSearch (par exemple, `http://AdresseIPordinateur/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: URL du proxy inverse pour OpenDocument (par exemple, `http://AdresseIPordinateur/RP/BOE/`).
3. Mettez à jour le fichier `httpd.conf` situé sous le dossier d'installation du proxy inverse Apache avec les paramètres suivants :
   - `ProxyPass /RP/BOE/OpenDocument/ http://<hôte Tomcat>:<Port connecteur>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<hôte Tomcat>:<Port connecteur>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Redémarrez le serveur proxy inverse Apache 2.2.

26.2.3 Configuration des propriétés de l'application dans la CMC

Pour configurer les propriétés de l'application de recherche de plateformes, procédez comme suit :

1. Accédez à la zone *Applications* de la CMC.

2. Sélectionnez *Application de recherche de plateformes*.
3. Cliquez sur *Gérer* > *Propriétés*. La boîte de dialogue *Propriétés* s'affiche.



4. Configurez les paramètres de la recherche de plateformes :

Option	Description
Statistiques de recherche	La recherche de plateformes fournit les statistiques de recherche suivantes : • Statut de l'indexation : affiche le statut du processus d'indexation. • Nombre de documents indexés : affiche le nombre de documents indexés. • Dernier horodatage indexé : affiche l'horodatage de la dernière indexation du document.
Arrêter/Démarrer l'indexation	Les options de démarrage ou d'arrêt d'indexation permettent de démarrer ou d'arrêter le processus d'indexation pour basculer de l'analyse continue à l'analyse planifiée ou à des fins de maintenance. Pour arrêter l'indexation, cliquez sur *Arrêter l'indexation*.
Paramètres régionaux de l'index par défaut	La recherche de plateformes utilise les paramètres régionaux spécifiés dans la CMC pour l'indexation de tous les documents BI non localisés. Une fois le document localisé, l'analyseur de langage correspondant procède à l'indexation. La recherche est basée sur les paramètres régionaux du produit du client et la pondération est accordée aux paramètres régionaux du produit du client. Vous pouvez configurer la pondération dans les propriétés de configuration de la CMC.

Option	Description
Fréquence de l'analyse	Vous pouvez indexer l'ensemble du référentiel de la plateforme de BI à l'aide des options suivantes : • Analyse continue : avec cette option, l'indexation est continue. Le référentiel est indexé à chaque fois qu'un objet est ajouté, modifié ou supprimé. Cela permet de visualiser ou d'utiliser le plus récent contenu de la plateforme de BI. Définie par défaut, l'analyse continue met à jour de façon continue le référentiel en fonction des actions que vous réalisez. L'analyse continue fonctionne sans intervention de l'utilisateur et réduit le temps nécessaire à l'indexation d'un document. • Analyse planifiée : avec cette option, l'indexation est basée sur la planification définie par les options de planification. Pour en savoir plus sur la planification d'un objet, consultez la section *Planification d'un objet* de l'application de recherche de plateformes dans l'*Aide en ligne de la CMC de la plateforme SAP BusinessObjects Business Intelligence*. **Remarque** • Si vous sélectionnez *Analyse planifiée* et définissez la *Périodicité* sur une option autre que *Maintenant*, l'application de recherche de plateformes affiche la date et l'horodatage de la prochaine indexation planifiée du document. • Si vous sélectionnez *Analyse planifiée*, le bouton *Démarrer l'indexation* est activé et le bouton *Arrêter l'indexation* est désactivé. • Une fois la planification terminée, le bouton *Arrêter l'indexation* est désactivé.

Option	Description
Emplacement de l'index	Les index sont stockés dans des dossiers partagés aux emplacements suivants : • Emplacement de l'index maître (index, vérificateur d'orthographe) : les index maître et de vérificateur d'orthographe sont stockés à cet emplacement. Au cours d'une recherche, les résultats initiaux sont extraits à l'aide de l'index maître tandis que les index de vérificateur d'orthographe sont utilisés pour extraire des suggestions. Dans un déploiement de la plateforme de BI en cluster, cet emplacement doit être situé sur un système de fichiers partagé accessible depuis tous les nœuds du cluster. • Emplacement des données persistantes (stockages de contenu) : le stockage de contenu est situé à cet emplacement. Il est créé depuis l'emplacement de l'index maître et reste synchronisé avec lui. Le stockage de contenu sert à générer des facettes à traiter les accès initiaux générés depuis l'emplacement de l'index maître. Dans un déploiement en cluster de la plateforme de BI, les stockages de contenu sont générés à tous les nœuds. L'emplacement des données persistantes est le seul emplacement d'index affecté par l'environnement en cluster, étant donné qu'il contient les dossiers de stockage du contenu. Si un ordinateur ne dispose que d'un seul service de recherche, il n'existe qu'un seul emplacement de stockage de contenu. Par exemple, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur>\ContentStores. Toutefois, dans un environnement en cluster, s'il existe plusieurs services de recherche, chacun possède un emplacement de stockage de contenu. Par exemple, si deux instances d'un même serveur sont en cours d'exécution, les emplacements de stockage de contenu sont les suivants : 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nom du serveur 1>\ContentStores. • Emplacement des données non persistantes (fichiers temporaires, index Delta) : les index delta sont créés et stockés temporairement à cet emplacement avant d'être fusionnés avec l'index maître. Les index de cet emplacement sont supprimés après avoir été fusionnés avec l'index maître. En outre, les fichiers de substitution (résultat des extracteurs) sont créés à cet emplacement et stockés temporairement jusqu'à ce qu'ils soient convertis en index delta. **Remarque** • L'emplacement de l'index maître doit être un emplacement partagé. • Vous devez cliquer sur *Arrêter l'indexation* pour modifier l'emplacement de l'index. • Si vous modifiez l'emplacement d'un index, vous devez copier le contenu sur un nouvel emplacement, sinon les informations d'index existantes seront perdues. • Les fichiers d'index peuvent contenir des informations personnelles et confidentielles, en particulier si vous choisissez d'indexer le contenu du document.

Option	Description
	Vous devez autoriser un seul utilisateur système à accéder au dossier partagé et vous devez stocker les dossiers partagés dans un environnement chiffré afin d'éviter tout vol de données.

Niveau d'indexation	Vous pouvez ajuster le contenu de la recherche en définissant le niveau d'indexation de l'une des façons suivantes :
	• Métadonnées de plateformes : un index est créé uniquement pour les informations de métadonnées de plateforme telles que titres, mots clés et descriptions des documents. Par défaut, cette option est sélectionnée.
	• Métadonnées de plates-formes et de documents : cet index comprend les métadonnées de plates-formes ainsi que les métadonnées de documents. Les métadonnées du document comprennent la date de création, la date de modification et le nom de l'auteur.
	• Contenu complet : cet index comprend les métadonnées de plateformes, les métadonnées de documents et les autres contenus tels que :
	  • Le contenu réel du document
	  • Le contenu des invites et listes de valeurs
	  • Diagrammes, graphiques et étiquettes
	Remarque
	L'indexation de l'ensemble du contenu n'est pas prise en charge pour les documents Analysis Office et Lumira. Seule l'indexation des métadonnées est prise en charge pour les documents Analysis Office et Lumira.
	Remarque
	Lorsque vous modifiez le niveau d'indexation, l'indexation est initialisée pour l'actualisation de l'ensemble du référentiel de la plateforme de BI.

Option	Description
Types de contenus	Vous pouvez sélectionner les types de contenu suivants pour l'indexation : • Crystal Reports • Web Intelligence • Univers • Espace de travail BI • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • Texte enrichi • Texte • Microsoft Word • Microsoft Excel Le filtre de type de contenu n'est pas applicable à l'indexation des métadonnées de plateformes. Quels que soient les types de contenu sélectionnés, l'indexation des métadonnées de plateformes s'effectue pour tous les types d'objet pris en charge et la recherche entraîne le renvoi par la zone de lancement BI de tous les objets pour le mot clé associé aux métadonnées de plateformes. Le filtre de type de contenu concerne l'indexation des métadonnées de documents (auteur du document, en-tête du document, pied de page du document, etc.) et l'indexation de contenu (diagrammes, graphiques, tableau avec un rapport). En fonction du niveau d'indexation et des types de contenu sélectionnés, la recherche de plateformes indexe les métadonnées et le contenu des documents pour les types d'objet sélectionnés dans le référentiel et seuls ces objets s'affichent dans les résultats de la recherche de la zone de lancement BI lors de la recherche d'un mot clé associé aux métadonnées et au contenu de documents.
Régénérer l'index	Cette option supprime les index existants et réindexe l'ensemble du référentiel. Vous pouvez sélectionner l'option *Régénérer l'index*, que l'indexation soit en cours ou arrêtée. L'index existant est supprimé lorsque vous enregistrez vos modifications dans la page Propriétés. Cependant, si l'indexation est arrêtée, l'index ne commence pas à se régénérer tant que l'indexation n'est pas redémarrée. Si vous ne souhaitez pas que l'application de recherche de plateformes réindexe les documents, désélectionner l'option *Régénérer l'index* avant de cliquer sur *Démarrer l'indexation*.

Option	Description
Documents exclus de l'indexation	L'option *Documents exclus de l'indexation* exclut des documents de l'indexation. Par exemple, vous pouvez décider que les rapports Crystal extrêmement volumineux ne puissent pas être recherchés afin d'éviter de surcharger les ressources des serveurs d'applications de rapports. De même, vous pouvez décider que les publications incluant des centaines de rapports personnalisés ne soient pas indexées. En excluant des documents particuliers, vous pouvez empêcher que les utilisateurs y accèdent à partir de la recherche de plateformes. Il est important de noter que lorsqu'un document est déjà indexé avant d'être ajouté à ce groupe, il peut toujours faire l'objet d'une recherche. Pour que les documents du groupe *Documents exclus de l'indexation* ne puissent pas être recherchés, vous devez régénérer l'index. Par défaut, seul le compte Administrateur dispose du contrôle complet de l'option *Documents exclus de l'indexation*. Les autres utilisateurs disposant des droits suivants peuvent seulement ajouter des documents aux *Documents exclus de l'indexation*. • Droits de visualisation et de modification sur la catégorie • Modifier le document directement
Autre configuration - Ignorer l'instance	Par défaut, les instances de documents sont sélectionnées pour être indexées. De ce fait, la taille de l'index augmente, ce qui entraîne une consommation d'autant plus importante de l'espace disque. La taille du dossier "Lucene Index Engine" dans le dossier PlatformSearchData augmente de façon démesurée en raison de l'indexation d'un très grand nombre d'instances dans le référentiel. S'il y a des millions de documents (ou plus) et que la plupart de ces documents ont également un grand nombre d'instances existantes (ainsi que des instances planifiées générées à intervalles réguliers) dans le système, alors la taille du dossier "Lucene Index Engine" augmente de façon excessive même si le niveau d'indexation est défini sur "Métadonnées de plateformes". La fonctionnalité Ignorer l'instance lors de la recherche de plateformes vous permet de contrôler l'indexation d'instances en l'activant ou la désactivant, via une case à cocher disponible sous "Autre configuration - Ignorer l'instance" dans la page des propriétés de l'application de recherche de plateformes dans la CMC. **Remarque** • Si vous Activez/Désactivez Ignorer l'instance, vous devez redémarrer le serveur de traitement adaptatif de la recherche de plateformes. Cette modification affecte tous les niveaux de l'indexation. • Si vous modifiez Ignorer l'instance et que vous voulez que ces modifications soient appliquées à toutes les instances existantes (c'est à dire toutes les instances devant être sélectionnées pour être indexées), alors vous devez régénérer l'index.

Option	Description
Objets exclus de l'indexation	L'option *Objets exclus de l'indexation* exclut des objets de l'indexation. Par exemple, vous pouvez décider que certains objets ne puissent pas être recherchés afin d'éviter de surcharger les ressources des serveurs d'applications de rapports. En excluant des objets particuliers, vous pouvez empêcher que les utilisateurs y accèdent à partir de la recherche de plateformes. Il est important de noter que lorsqu'un objet est déjà indexé avant d'être ajouté à ce groupe, il peut toujours faire l'objet d'une recherche. Pour que les documents du groupe *Objets exclus de l'indexation* ne puissent pas être recherchés, vous devez régénérer l'index. Liste des objets pouvant être exclus de l'indexation : • Rapport Crystal • Webi • LCMJob • Univers • Excel • PDF • PowerPoint • Rtf • Txt • Word • Page de tableau de bord AF • Lot d'objets • QaaWS • Profil • Événement • Discussions • InformationDesigner • Analyse MD • Publication • Agnostique • Analyses • Lien hypertexte • Programme • pQuery • Fichier de métadonnées DSL • Raccourci • Album DataDiscovery • Classeur AO • Récit VISI • Jeu de données VISI

Option	Description
	• VISI.Lums • VISILums • Utilisateur • Groupe d'utilisateurs

5. Cliquez sur *Enregistrer et fermer*.

> **Remarque**
>
> Si l'utilisateur ne sélectionne pas l'option *Régénérer l'index* et modifie le niveau d'indexation ou sélectionne/désélectionne des extracteurs, l'index est progressivement mis à jour sans supprimer l'index existant.

26.3 Utilisation de la recherche de plateformes

26.3.1 Indexation de contenu dans le référentiel CMS

L'indexation est un processus continu impliquant les tâches séquentielles suivantes :

1. Analyse : l'analyse est un mécanisme d'interrogation du référentiel CMS et d'identification des objets publiés, modifiés ou supprimés. Elle peut s'effectuer de deux manières : analyse continue et analyse planifiée.
   Pour en savoir plus sur l'analyse continue et planifiée, reportez-vous à la rubrique *Configuration des propriétés de l'application* dans les rubriques associées.
2. Extraction : l'extraction est un mécanisme d'appel des extracteurs sur base du type de document. Il existe un extracteur dédié pour chaque type de document disponible dans le référentiel. Les nouveaux types de documents peuvent être recherchés en définissant de nouveaux plug-ins d'extracteur. Chacun de ces extracteurs est suffisamment extensible pour extraire le contenu de documents volumineux contenant de nombreux enregistrements.
   Les extracteurs suivants sont pris en charge :
   - Extracteur de métadonnées
   - Extracteur de rapports Crystal
   - Extracteur Web Intelligence
   - Extracteur d'univers
   - Extracteurs agnostiques (MS Office 2003 et 2007 et documents PDF)

   Pour en savoir plus sur les types de documents pouvant être recherchés, reportez-vous à la rubrique *Types de contenu pouvant être recherchés* dans les rubriques associées.
3. Indexation : l'indexation est un mécanisme permettant d'indexer tout le contenu extrait via une bibliothèque tierce nommée Apache Lucene Engine. Le temps nécessaire à l'indexation varie en fonction du nombre d'objets du système, de la taille et du type des documents.
   Pour que l'indexation se déroule correctement, les serveurs suivants doivent être exécutés et activés :
   - Input File Repository Server (IFRS)
   - Output File Repository Server (OFRS)

- Central Management Server (CMS)
- Le serveur de traitement adaptatif (APS) qui héberge le service de recherche de plateformes

Si le type d'objet est sélectionné en tant que rapport Web Intelligence ou Crystal, le serveur de traitement Web Intelligence et le serveur d'applications Crystal Reports correspondants doivent être en cours d'exécution et activés pour les types d'objets respectifs sélectionnés.

4. Stockage de contenus : le stockage de contenus contient des informations telles que l'ID, le CUID, le nom, le genre et l'instance, extraites de l'index maître dans un format aisément lisible. Cela optimise la durée du processus de recherche.

Informations associées

Configuration des propriétés de l'application dans la CMC [page 958]
Types de contenus pouvant être recherchés [page 969]

26.3.2 Liste d'échecs d'indexation

La liste d'échecs d'indexation fournit une liste de documents qui n'ont pas pu être indexés. La recherche de plateformes offre trois tentatives d'indexation pour un document. Si un document ne peut pas être indexé, il figure dans la liste d'échecs d'indexation.

Pour afficher la liste d'échecs d'indexation, procédez comme suit :

1. Accédez à la zone Applications de la CMC.
2. Sélectionnez *Application de recherche de plateformes*.
3. Choisissez *Actions > Liste d'échecs d'indexation*.

   La boîte de dialogue Application de recherche de plateformes qui s'ouvre affiche une liste de documents accompagnée des détails suivants :
   - Titre : Affiche le titre du document qui n'a pas pu être indexé.
   - Type : Affiche le nom du type de document, comme Crystal Reports et Web Intelligence, ainsi que l'emplacement du document.
   - Type d'échec : Affiche le code d'erreur et le motif d'échec d'indexation du document. Cliquez sur le lien hypertexte En savoir plus pour consulter la trace de la pile et en savoir plus sur la cause de l'erreur.
   - Heure de la dernière tentative : Affiche l'horodatage de la dernière tentative d'indexation d'un document.

26.3.3 Recherche des résultats

26.3.3.1 Avant la recherche

26.3.3.1.1 Requêtes suggérées

Lorsqu'il utilise la recherche de plateformes, l'utilisateur recherche parfois des réponses à une question spécifique, plutôt qu'un objet spécifique. Ces questions peuvent ou non trouver leur réponse dans des rapports disponibles dans le référentiel de la plateforme de BI.

La recherche de plateformes analyse la structure des univers et des rapports existants dans votre référentiel et compare ces informations à la requête de recherche fournie par l'utilisateur pour suggérer de nouvelles requêtes SAP BusinessObjects Web Intelligence susceptibles d'aider les utilisateurs à trouver des réponses à leurs questions.

Pour créer des rapports potentiels, la recherche de plateformes met en correspondance les mots contenus dans tous les univers en termes de dimension, d'indicateur, de condition et de valeur de filtre.

La recherche de plateformes recherche des correspondances dans les informations suivantes sur les univers ou les documents Web Intelligence existants :

- Indicateurs des univers correspondant aux termes recherchés.
  Lorsqu'un indicateur correspond à un des termes recherchés, cet indicateur est utilisé dans le document Web intelligence obtenu.
- Noms de dimensions des univers correspondant aux termes recherchés.
  Lorsqu'un nom de dimension correspond à un des termes recherchés, le document Web Intelligence obtenu décompose les informations en fonction de cette dimension.
- Il est possible d'utiliser des filtres de requête pour cibler les données affichées dans le document. Ces filtres de requête sont générés en analysant les termes recherchés.
  - Si le nom d'une condition d'univers correspond à un des termes recherchés, cette condition est utilisée comme filtre.
  - Si des valeurs de champ figurent dans des documents Web Intelligence existants dont les noms correspondent aux termes recherchés, un filtre est créé à partir de la dimension du rapport historique contenant la valeur correspondante, en utilisant "égal à" comme opérateur de condition.

Si la recherche de plateformes a établi suffisamment de correspondances pour que le document obtenu contienne deux champs de résultat et un filtre, la requête est considérée comme étant prête à exécuter. Dans ce cas, l'utilisateur peut cliquer pour afficher le rapport terminé.

Si les correspondances entre les univers et le document sont insuffisantes, vous pouvez modifier la requête avant de l'exécuter.

La recherche de plateformes suggère plusieurs requêtes si plusieurs univers correspondent aux termes recherchés ou si le même mot apparaît dans deux correspondances différentes, par exemple dans le nom d'une dimension et en tant que valeur de filtre.

26.3.3.1.2 Types de contenus pouvant être recherchés

Le contenu publié sur la plateforme de BI peut être recherché par le biais de la fonctionnalité de recherche de plateformes. Les types d'objets sont répertoriés ci-dessous avec leur contenu indexé correspondant :

Type d'objet	Contenu indexé
Crystal Reports 2020	Titre, description, formules de sélection, données enregistrées, champs de texte des sections, valeurs de paramètres et sous-rapports.
Documents Web Intelligence	Titre, description, nom des filtres d'univers utilisés dans le rapport, données enregistrées, constantes de condition de filtrage définies localement dans le rapport, nom des indicateurs d'univers utilisées dans le rapport, noms des objets d'univers utilisés dans le rapport, données de l'ensemble des enregistrements et texte statique des cellules.
Documents Microsoft Excel (2003 et 2007)	Données de toutes les cellules non vides, champs de la page Résumé des propriétés du document (titre, sujet, auteur, société, catégorie, mots clés et commentaires) et texte des en-têtes et pieds de page des documents. Pour les cellules utilisant des calculs ou des formules, la valeur qui suit l'évaluation peut faire l'objet d'une recherche. Pour les valeurs numériques ou de date et heure, les données brutes peuvent faire l'objet d'une recherche.
Documents Microsoft Word (2003 et 2007)	Texte de tous les paragraphes et tableaux, champs de la page Résumé des propriétés du document (titre, sujet, auteur, société, catégorie, mots clés et commentaires), texte des en-têtes et pieds de page des documents et texte numérique.
Fichiers RTF, PDF, PPT et TXT	L'intégralité du texte de ces documents peut faire l'objet d'une recherche.
LCMJob, ObjectPackage, requête de service Web (QaaWS), Profil, Discussions, InformationDesigner, indicateurs pour la plateforme SAP BusinessObjects BI, MDAnalysis, Publications, Analyses et Hyperlien	Le contenu des métadonnées peut être recherché.
Evénements	Tous les événements (personnalisés, système, Crystal Reports et de surveillance) peuvent être recherchés. Si un événement est associé à une source, la recherche de plateformes fait apparaître la source à côté de l'événement. **Remarque** La recherche de plateformes prend en charge les événements Crystal Reports pour Entreprise.

Type d'objet	Contenu indexé

Espace de travail BI	• Le titre, la description et le contenu des modules BIW suivants sont indexés :
	  • Module texte
	  • Module de type Page Web
	  • Module de liste de navigation
	  • Module de visualiseur
	• Le titre et la description d'un module composé sont indexés.
	• Seul le titre d'un module de modèle d'espace de travail est indexé.
	• Dans le cas d'un module de groupe, le titre et les métadonnées des modules en son sein sont indexés.
	• Le titre, la description et le CUID des modules d'InfoObject sont indexés dans les espaces de travail BI.
	  Remarque
	  Étant donné que seuls le titre et la description d'un module d'InfoObject incorporé sont indexés, la recherche de contenu de l'InfoObject ne renverra aucune référence au module incorporé. Par exemple, si un CR est inséré dans l'espace de travail BI, son titre et sa description sont indexés. Aucune recherche effectuée dans le contenu du CR ne renverra de référence au module incorporé.
	• Si un espace de travail BI contient plusieurs onglets et sous-onglets, le titre et le contenu de chaque onglet et de chaque sous-onglet sont également indexés.

CR Next Gen	Titre, description, formules de sélection, données enregistrées, champs de texte des sections, valeurs de paramètres et sous-rapports. Les objets suivants d'un rapport CR Next Gen ne sont pas pris en charge : • Rapport de tableau croisé • Extraction de données de diagramme • Extraction d'images et de métadonnées associées • OLE incorporé (par exemple, un document Word incorporé dans CR) En outre, il n'est pas possible de lire les données page par page à partir d'un rapport CR Next Gen.

Type d'objet	Contenu indexé
Univers	Le contenu des données peut être recherché. **Remarque** L'option d'indexation d'univers est activée par défaut. Si vous remarquez que l'exécution des requêtes utilisées par la recherche de plateformes pour indexer le contenu d'univers est longue et influe sur les performances du serveur de base de données, il est conseillé de désactiver l'option d'indexation d'univers dans la CMC (Central Management Console). Exemple de requête utilisée par la recherche de plateformes pendant l'indexation du contenu d'univers : `Select distinct SampleColumnName from SampleTableName LIMIT 1000`. Suivez cette procédure pour désactiver l'indexation d'univers : 1. Connectez-vous à la CMC (Central Management Console). 2. Choisissez *Applications*. 3. Accédez aux applications de recherche de plateformes et choisissez *Propriétés*. 4. Accédez aux types de contenu et décochez *Univers*. 5. Cliquez sur *Enregistrer et fermer*.
Document Lumira	Seul le contenu des métadonnées peut être recherché.
Document Analysis Office	Seul le contenu des métadonnées peut être recherché.

Remarque

La taille maximale prise en charge pour les documents agnostiques (MS Office 2003 et 2007 et documents PDF) est de 15 Mo.

26.3.3.2 Recherche

Lorsqu'un utilisateur recherche un mot clé à partir de la zone de lancement BI ou toute autre application utilisant le SDK de recherche de plateformes, c'est dans l'index maître que sont recherchés les termes. En fonction des droits d'affichage de l'utilisateur, le moteur de recherche affiche uniquement les documents pour lesquels l'utilisateur dispose d'un droit d'accès.

Remarque

Lorsque la recherche est effectuée dans la CMC dans un environnement avec une grande base de données CMS, la recherche peut échouer. Pour plus d'informations, consultez laNote SAP 2156647 La recherche dans la CMC est lente ou ne renvoie pas de résultats.

26.3.3.3 Après la recherche

26.3.3.3.1 Facettes

La recherche de plateformes affine les résultats de la recherche en les regroupant par catégories ou facettes de types d'objets similaires et en les classant selon le nombre d'occurrences de la catégorie parmi les résultats renvoyés pour le terme de la recherche. Les facettes permettent d'accéder au résultat précis.

La recherche de plateformes génère des facettes à partir des métadonnées d'InfoObject, des métadonnées de document et du contenu du document. Elle n'affiche que les facettes disposant de plus de deux documents qui correspondent à une requête précise. Les facettes sont rendues de manière dynamique sur la base des documents qui correspondent à la requête de recherche et sont triées par comptage de documents.

Les documents sont groupés dans les facettes ou catégories génériques suivantes :

- Personnel ou public (comme RH, Entreprise et Finance) : valeur basée sur les catégories de documents de la plateforme de BI.
- Type de document : valeur basée sur le type de document, par exemple Web Intelligence, Crystal Reports, Microsoft Word (2003 et 2007) et Microsoft Excel (2003 et 2007).
- Univers et connexions : valeur basée sur la source du contenu.
- Date : il s'agit de la date de la dernière actualisation : (année, trimestre et mois).
- Heure : il s'agit de l'heure de la dernière actualisation (les dernières 24 heures et la semaine dernière, par ex.).
- Auteur : nom de l'utilisateur qui a créé le document.

> **Remarque**
>
> Lors de l'utilisation des paramètres régionaux Hébreux ou Arabe, si vous recherchez des objets contenus dans la zone de lancement BI, le résultat de la recherche n'affiche pas de facettes.

26.3.3.3.2 Normalisation du classement des résultats de la recherche

La recherche de plateformes prend en compte l'emplacement de l'occurrence du terme recherché pour le classement d'un document. Elle regroupe le contenu dans les catégories suivantes d'après l'occurrence du contenu dans le document :

1. Métadonnées de plateformes
2. Métadonnées de documents
3. Métadonnées de contenu
4. Contenu

Vous pouvez configurer la pondération de ces catégories dans la CMC.

26.3.3.3.2.1 Personnalisation de la pondération pour le classement des résultats de la recherche

La recherche de plateformes permet de définir des pondérations pour le contenu groupé dans les catégories sur base de l'occurrence du contenu du document, de sorte que vous puissiez définir une valeur supérieure pour la catégorie souhaitée afin d'extraire plus rapidement les résultats de la recherche correspondants.

Pour définir la pondération, procédez comme suit :

1. Dans la zone *Gérer* de la CMC, cliquez sur *Applications*.
2. Ouvrer l'*application de recherche de plateformes*.
3. Sélectionnez *Classement*.

   Les poids des différentes catégories de contenu telles que Métadonnées de plateformes, Métadonnées de documents, Métadonnées de contenu et Contenu sont affichés. Les *paramètres régionaux de l'utilisateur* sont ceux définis dans les préférences de la zone de lancement BI.
4. Définissez les poids selon vos besoins.
5. Sélectionnez *Enregistrer*.

Dans un scénario de mise à niveau, si un classement doit être appliqué aux documents déjà indexés, vous devez recréer l'index. Pour en savoir plus, voir les informations sur la régénération de l'index dans la section Configuration des propriétés de l'application dans la CMC [page 958].

26.3.3.3.3 Prise en charge multilingue

La recherche de plateformes propose une prise en charge multilingue pour indexer le contenu, récupérer les résultats de la recherche et obtenir des suggestions dans la langue de votre choix. Pour indexer tous les documents non localisés de la plateforme de BI, elle utilise les paramètres régionaux définis dans la CMC sous *Paramètres régionaux de l'index par défaut*.

Une fois l'InfoObject localisé, la recherche de plateformes utilise l'analyseur de langue pour indexer le document.

La recherche se base sur les paramètres régionaux définis comme paramètres régionaux du produit du client. La recherche de plateformes accorde une pondération supérieure aux paramètres régionaux du produit du client durant l'extraction des résultats de la recherche. Vous pouvez configurer les poids dans la CMC.

26.3.3.3.4 Suggestions

La recherche de plateformes propose des suggestions pour les requêtes de recherche mal orthographiées. Si la requête de recherche initiale ne fournit aucun résultat, la recherche de plateformes suggère les termes les plus plausibles sur base du contenu indexé.

Les suggestions apparaissent comme des mots clés avec un lien hypertexte. Cliquez sur un lien hypertexte pour afficher une liste de documents contenant le mot clé susceptible de correspondre à la requête initiale. Ces suggestions sont déterminées de manière algorithmique sur la base de divers facteurs objectifs.

Si plusieurs termes peuvent correspondre à la requête initiale, la recherche de plateformes suggère les trois premières propositions dans la langue définie en tant que *Paramètres régionaux de l'index* dans la CMC.

> **Remarque**
>
> La recherche de plateformes ne génère pas de suggestions dans ces cas :
>
> - Si les requêtes de recherche contiennent moins de trois lettres
> - Pour les recherches attribuées, comme le Type : rapport Crystal
> - Pour le contenu et les métadonnées d'univers
> - Pour les langues multioctets, telles que le chinois, le japonais et le coréen

26.4 Intégration de la recherche de plateformes à SAP NetWeaver Enterprise Search

SAP NetWeaver Enterprise Search 7.20 et versions ultérieures peuvent utiliser un service de recherche sur la base d'OpenSearch (RSS et ATOM). Il peut déléguer des requêtes de recherche à des systèmes fournisseurs de service de recherche. Dans ce cas, OpenSearch est le fournisseur de service, SAP NetWeaver Enterprise Search est le consommateur des résultats de la recherche et la recherche de plateformes SAP BusinessObjects est le fournisseur de service de recherche.

Si un utilisateur soumet une requête de recherche, SAP NetWeaver Enterprise Search transfère la requête de recherche directement au fournisseur OpenSearch. Le fournisseur répond à la requête de recherche et envoie la réponse à SAP NetWeaver Enterprise Search. Elle est ensuite fusionnée avec les résultats reçus de la part d'autres connecteurs d'objets de recherche à un résultat de recherche et affichée sur l'interface utilisateur.

Pour intégrer SAP NetWeaver Enterprise Search et la recherche de plateformes, vous devez procéder comme suit :

1. Créez un connecteur dans SAP NetWeaver Enterprise Search.
2. Importez le rôle d'un utilisateur sur la plateforme de BI.

26.4.1 Création d'un connecteur dans SAP NetWeaver Enterprise Search

Vous pouvez utiliser un connecteur d'objet de type OpenSearch pour intégrer les fournisseurs de recherche externes offrant une fonction de recherche disponible par le biais d'OpenSearch.

Pour créer un connecteur dans SAP NetWeaver Enterprise Search, vous devez remplir les prérequis suivants :

1. L'URL du service de description OpenSearch.
2. Le service de description OpenSearch doit être disponible en format RSS ou ATOM uniquement.

Suivez la procédure suivante pour créer un connecteur dans SAP NetWeaver Enterprise Search :

1. Lancez le cockpit d'administration et choisissez Créer.

2. Sélectionnez OpenSearch comme type de connecteur d'objet de recherche.
3. Sélectionnez *Suivant*.
4. Saisissez l'URL du service de description OpenSearch du fournisseur OpenSearch.
5. Sélectionnez un des paramètres d'authentification suivants pour lancer l'URL du service de description :
   - Aucune authentification : aucune authentification n'a lieu.
   - SAP Authentication Assertion Ticket (Ticket d'assertion d'authentification SAP) : cet utilisateur est utilisé pour l'authentification par connexion unique.
   - User/Password (Utilisateur/Mot de passe) : un utilisateur prédéfini est utilisé pour l'authentification
6. Sélectionnez Launch Search URL (Démarrer l'URL de recherche) dans les paramètres d'URL OpenSearch. Le service de description OpenSearch est alors validé pour un service de recherche correspondant. Le système entre automatiquement une valeur pour le modèle d'URL de recherche et la description associée.
7. Sélectionnez un des paramètres d'authentification suivants pour configurer un connecteur :
   - Aucune authentification : aucune authentification n'a lieu.
   - SAP Authentication Assertion Ticket (Ticket d'assertion d'authentification SAP) : cet utilisateur est utilisé pour l'authentification par connexion unique.
   - User/Password (Utilisateur/Mot de passe) : un utilisateur prédéfini est utilisé pour l'authentification
8. Sélectionnez *Suivant*.
   Une boîte de dialogue de résumé apparaît, affichant les valeurs entrées pour ce connecteur d'objet de recherche.
9. Sélectionnez *Précédent* pour modifier les paramètres ou *Annuler* pour refuser les données entrées.
10. Sélectionnez *Terminer* pour enregistrer les paramètres.

26.4.2 Importation du rôle d'un utilisateur dans la plateforme de BI

Procédez comme suit pour importer le rôle d'un utilisateur dans la plateforme de BI :

> **Remarque**
>
> L'administrateur doit disposer des renseignements relatifs à l'utilisateur, des informations système, des informations d'hôte de l'application et des références de connexion de l'utilisateur.

1. Accédez à la zone *Authentification* de la CMC.
2. Sélectionnez *SAP*.
3. Dans l'onglet *Systèmes d'autorisation*, spécifiez les éléments suivants :
   - Système
   - Client
   - Serveur d'applications
   - Numéro du système
   - Nom d'utilisateur
   - Mot de passe
   - Langue
4. Sélectionnez *Mettre à jour*.

5. Cliquez sur l'onglet *Importation de rôle* et importez les rôles d'utilisateur.
6. Sélectionnez *Mettre à jour*.
7. Sélectionnez *Gérer* > *Sécurité de l'utilisateur* dans la CMC pour affecter les droits d'utilisateur appropriés.

26.5 Recherche depuis SAP NetWeaver Enterprise Search

Pour effectuer une recherche parmi les résultats depuis SAP NetWeaver Enterprise Search, procédez comme suit :

1. Connectez-vous à l'application SAP NetWeaver Enterprise Search.
2. Sélectionnez *Recherche avancée*.
3. Sélectionnez le connecteur créé pour la recherche de plateformes.
4. Recherchez un mot clé.

   Les résultats réunis pour le mot clé contiennent les résultats de la recherche de plateformes s'il existe une correspondance pour le mot clé.

26.6 Audit

Tous les événements de requêtes de recherche envoyées depuis une application client utilisant le service de recherche de plateformes et la réponse de la recherche sont audités. Pour la recherche de plateformes, l'audit est implémenté au niveau du service.

Le service de recherche de plateformes doit s'exécuter avec un service du proxy de l'audit client sur le même serveur afin d'envoyer les événements d'audit.

Il existe un ID de type d'événement 1009 pour la recherche de plateformes et quatre ID de type de détail d'événement spécifiques à la recherche de plateformes :

- Keyword searched (Mot clé recherché) (ID: 19)
- Number of Search Results (Nombre de résultats de la recherche) (ID: 63)
- Facet Search (Recherche de facettes) (ID: 20)
- Search Exception (Exception de recherche) (ID: 1)

En dehors des détails d'événement, il existe quelques détails d'événement standard tels que le CUID de session et le CUID d'utilisateur qui sont pris en charge pour tout audit de tout module de la plateforme de BI.

Le fonctionnement de l'audit dans la recherche de plateformes est illustré ci-dessous par un exemple.

Si vous recherchez un mot clé comme "Ventes", le nombre total de résultats de la recherche pourrait être 5. Dans ce cas, les événements suivants sont audités :

- ID de type d'événement : 1009
- ID du type de détails d'événement 19 avec la valeur ventes
- ID du type de détails d'événement 63 avec la valeur 5

- CUID de session
- CUID d'utilisateur
- Statut avec la valeur 0, qui consiste en l'état de réussite
- Heure de début
- Durée
- ID objet avec la valeur 0 car il s'agit de l'audit côté service

Lorsque les facettes sont générées et que vous sélectionnez une ou plusieurs facettes, les événements suivants sont audités :

- ID de type d'événement : 1009
- ID du type de détails d'événement 19 avec la valeur ventes
- ID du type de détails d'événement 63 avec la valeur 5
- ID de type de détails d'événement 20 avec chaîne de facettes séparées par des virgules
- CUID de session
- CUID d'utilisateur
- Statut avec la valeur 0, qui consiste en l'état de réussite
- Heure de début
- Durée
- ID objet avec la valeur 0 car il s'agit de l'audit côté service

S'il existe une exception de recherche en raison d'une entrée non valide (telle que *"a"), les détails d'événement suivants sont audités :

- ID de type d'événement : 1009
- ID du type de détails d'événement 19 avec la valeur ventes
- ID de type de détails d'événement 63 avec la valeur 0
- ID de type de détails d'événement 1 avec le message d'exception
- CUID de session
- CUID d'utilisateur
- Statut avec la valeur 1, qui consiste en l'état d'échec
- Heure de début
- Durée
- ID objet avec la valeur 0 car il s'agit de l'audit côté service

26.7 Dépannage

26.7.1 Auto-guérison

La recherche de plateformes possède son propre mécanisme d'auto-guérison. Elle surveille en continu l'utilisation de la mémoire du service de recherche et arrête automatiquement l'indexation lorsque l'utilisation de la mémoire dépasse la valeur seuil. Elle démarre automatiquement une fois que l'utilisation de la mémoire est ramenée à une limite raisonnable. Cependant, les utilisateurs peuvent poursuivre la recherche durant ce processus mais ne peuvent effectuer d'indexation pendant un certain temps. Par défaut, la recherche de

plateformes configure le nombre de documents pouvant être indexés à tout instant, en se basant sur le type de document. L'indexation est lancée en fonction des ressources système telles que la CPU et la mémoire.

26.7.2 Scénarios de problèmes

Cette section fournit des solutions détaillées à un vaste éventail de problèmes pouvant survenir lors de l'extraction des résultats de la recherche avec la recherche de plateformes.

Impossible d'extraire les résultats de la recherche du document récemment ajouté contenant le mot clé

- Vérifiez que la recherche de plateformes prend en charge le type du document soumis. Si le type de document n'est pas pris en charge, le document n'est pas indexé.
  Pour en savoir plus sur les types de documents pris en charge, voir la rubrique *Types de contenus pouvant être recherchés* dans les rubriques associées répertoriées ci-dessous.
- Vérifiez l'option sélectionnée pour la *Fréquence de l'analyse*. Si la *Fréquence de l'analyse* est définie sur *Analyse continue*, les documents sont immédiatement sélectionnés pour être indexés. Si la *Fréquence de l'analyse* est définie sur *Analyse planifiée*, l'indexation n'est exécutée que lors de la période planifiée.
  Pour en savoir plus sur la *Fréquence de l'analyse*, reportez-vous à la rubrique *Configuration des propriétés de l'application* dans les rubriques associées répertoriées ci-dessous.
- Consultez la liste d'échecs d'indexation pour vérifier que le document a été correctement indexé. Si le document s'affiche dans la liste, vous devez le modifier et l'envoyer à nouveau afin que la recherche de plateformes l'utilise pour l'indexer.

  > **Remarque**
  >
  > Vous pouvez modifier le document en ajoutant ou en supprimant un champ, puis en l'enregistrant à nouveau. Cela permet d'actualiser l'horodatage du document dans le référentiel de la plateforme de BI et de lancer la réindexation du document.

  Pour en savoir plus sur les documents dont l'indexation a échoué, reportez-vous à la rubrique *Liste d'échecs d'indexation* dans les rubriques associées répertoriées ci-dessous.
- Vérifiez les journaux des événements du serveur de traitement adaptatif contenant des informations sur l'échec d'indexation.
  1. Accédez au répertoire `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\logging\`, qui contient le journal de suivi de serveur de traitement adaptatif avec une extension .glf.
  2. Ouvrez le fichier journal de traces et recherchez le document SI_ID à indexer.

     > **Remarque**
     >
     > Vous pouvez rechercher le SI_ID du document à partir des propriétés du document.

Impossible d'extraire des documents Crystal Reports

La recherche de plateformes indexe le contenu Crystal Reports uniquement pour Crystal Reports 2020. Elle n'indexe pas le contenu associé à Crystal Reports pour Entreprise.

Cependant, avec Crystal Reports pour Entreprise, vous pouvez rechercher des métadonnées de document telles qu'un titre, une description et un mot clé, qui sont des propriétés de document.

Si le document contient du contenu indexable, vous devez suivre le processus repris dans la section ci-dessus *Impossible d'extraire les résultats de la recherche du document récemment ajouté contenant le mot clé*.

L'application SAP NetWeaver Enterprise Search ne peut pas extraire les résultats du référentiel de la plateforme de BI

- Vérifiez si la recherche de plateformes extrait les résultats de recherche à l'aide de la zone de lancement BI pour déterminer si le problème est dû à l'intégration de la recherche de plateformes et SAP NetWeaver Enterprise Search.
- Vérifiez si OpenSearch est déployé correctement dans le serveur d'applications Web. Les étapes propres à la validation du déploiement OpenSearch dépendent du type de serveur d'applications Web utilisé.
- Vérifiez si le connecteur est créé ou configuré correctement dans la configuration SAP NetWeaver Enterprise Search. Vous devez utiliser le bon connecteur pour que SAP NetWeaver Enterprise Search fédère les résultats de la recherche de plateformes.
- Vérifiez si la communication est correcte entre les ordinateurs exécutant respectivement SAP NetWeaver Enterprise Search et la plateforme de BI. En cas de problèmes de réseau dans un environnement distribué, SAP NetWeaver Enterprise Search risque de ne pas parvenir à fédérer les résultats.
- Vérifiez si le ou les utilisateurs SAP NetWeaver Enterprise Search sont ajoutés à la plateforme de BI avec les droits appropriés. Pour valider les droit des utilisateurs, accédez à la zone *Authentification* de la CMC et sélectionnez *SAP*.

Informations associées

Liste d'échecs d'indexation [page 967]
Configuration des propriétés de l'application dans la CMC [page 958]
Types de contenus pouvant être recherchés [page 969]

27 Fédération

27.1 Fédération

Fédération est un outil de réplication intersites pour l'utilisation de plusieurs déploiements de la plateforme de BI au sein d'un environnement international.

Vous pouvez créer et gérer le contenu depuis un déploiement de la plateforme de BI et le répliquer dans d'autres déploiements de la plateforme de BI situés sur d'autres sites géographiques selon une planification régulière. Vous pouvez réaliser des tâches de réplication unidirectionnelle et bidirectionnelle.

Les avantages offerts par Fédération incluent la possibilité de :

- Réduire le trafic réseau
- Créer et gérer du contenu à partir d'un site unique
- Augmenter les performances pour les utilisateurs finaux

Lorsque vous répliquez du contenu à l'aide de Fédération, vous pouvez :

- Simplifier les tâches administratives requises pour plusieurs déploiements
- Mettre en place des droits d'accès cohérents dans les nombreux bureaux des multinationales
- Obtenir des informations plus rapidement et traiter les rapports sur les sites distants sur lesquels les données résident
- Gagner du temps en extrayant plus rapidement les données locales et disséminées
- Synchroniser le contenu issu de plusieurs déploiements sans écrire de code personnalisé

Fédération vous offre des modèles de sécurité, des cycles de vie, ainsi que des plannings de test et de déploiement distincts variant en fonction des titulaires et des administrateurs. Par exemple, vous pouvez déléguer des fonctions d'administration qui empêchent l'administrateur de l'application de ventes de changer l'application des ressources humaines.

Vous pouvez répliquer différents objets avec Fédération, comme le décrit le tableau suivant.

Catégorie	Types d'objets que vous pouvez répliquer	Remarques supplémentaires
Vues d'entreprise	Gestionnaire de vues d'entreprise, connexions de données, listes de valeurs, fondation de données, etc.	Tous les objets sont pris en charge, bien qu'ils ne le soient pas au niveau individuel.
Rapports	Crystal Reports, Web Intelligence et Dashboard Design	Le module complémentaire et les modèles Full Client sont pris en charge.
Objets tiers	Fichiers Excel, PDF, PowerPoint, Word, texte, texte enrichi et ShockWave	
Utilisateurs	Utilisateurs, groupes, boîtes de réception, favoris et catégorie personnelle	
Plateforme de Business Intelligence	Dossiers, événements, catégories, calendriers, niveaux d'accès, liens	

Catégorie	Types d'objets que vous pouvez répliquer	Remarques supplémentaires
	hypertexte, raccourcis, programmes, profils, lots d'objets, objets agnostiques	
Univers	Univers, connexions et surcharges d'univers	

Les scénarios suivants présentent deux exemples d'utilisation de Fédération.

Scénario 1 : Distribution (conception centralisée)

La chaîne de magasins ACME souhaite envoyer un rapport de ventes mensuel à ses différents points de vente à l'aide de la méthode de réplication unidirectionnelle. L'administrateur du site d'origine crée un rapport que les administrateurs de chaque site de destination répliquent et exécutent sur la base de données du point de vente.

> → Conseil
>
> Les instances localisées peuvent être renvoyées au site d'origine qui gère les informations répliquées de chaque objet. Par exemple, le site d'origine applique le logo approprié, les informations de connexion à la base de données, etc.

Scénario 2 : Planification distante (accès distribué)

Les données sont situées sur le site d'origine. Les tâches de réplication en attente sont envoyées au site d'origine pour exécution. Les tâches de réplication terminées sont renvoyées aux sites de destination pour consultation. Par exemple, les données d'un rapport peuvent ne pas être disponibles sur le site de destination, auquel cas l'utilisateur peut configurer les rapports de sorte qu'ils s'exécutent sur le site d'origine avant que le rapport complété soit renvoyé au site de destination.

27.2 Terminologie Fédération

La liste de termes suivante contient des mots et expressions relatifs à Fédération et peut vous aider dans le cadre de votre utilisation de cette fonctionnalité.

Application BI	Regroupement logique des contenus de Business Intelligence destiné à un public spécifique dans un but précis. Une application BI n'est pas un objet. Un déploiement de la plateforme de BI peut héberger plusieurs applications BI, chacune d'elle pouvant avoir un modèle de sécurité, un cycle de vie, un calendrier de tests et de déploiement, ainsi que des propriétaires et des administrateurs distincts.
Site de destination	Système de la plateforme de BI recevant un contenu de la plateforme de BI répliqué à partir d'un site d'origine.
Local	Système local auquel un utilisateur ou un administrateur est connecté. Par exemple, l'administrateur d'un site de destination est considéré comme « local » pour le site de destination.

Instances finalisées exécutées localement	Instances traitées sur le site de destination, puis retransmises au site d'origine.
Sites d'origine multiples	Site d'origine constitué de plusieurs sites. Par exemple, les centres de développement multiples possèdent généralement des sites d'origine multiples. Toutefois, il ne peut y avoir qu'un seul site d'origine par réplication.
Réplication unidirectionnelle	Les objets ne sont répliqués que dans un seul sens : du site d'origine vers le site de destination. Toute mise à jour effectuée sur un site de destination se limite à ce site de destination.
Site d'origine	Système de la plateforme de BI d'où provient le contenu.
Distant	Système non local pour un utilisateur. Le site d'origine, par exemple, est considéré comme « distant » pour les utilisateurs et administrateurs du site de destination.
Connexion à distance	Objet qui contient des informations utilisées pour se connecter à un déploiement de la plateforme de BI, notamment le nom d'utilisateur et le mot de passe, le nom du CMS, l'URI du service Web et les options de nettoyage.
Planification à distance	Demandes de planification transmises à partir du site de destination vers le site d'origine. Les rapports se trouvant sur les sites de destination peuvent être planifiés à distance, et l'instance du rapport est donc renvoyée vers le site d'origine pour traitement. L'instance finalisée est ensuite renvoyée vers le site de destination.
Réplication	Processus permettant de copier le contenu d'un système de la plateforme de BI vers un autre.
Travail de réplication	Objet contenant des informations sur la planification des réplications et sur le contenu à répliquer ainsi que toute condition spécifique devant être appliquée lors de la réplication du contenu.
Liste de réplication	Liste des objets à répliquer. Une liste de réplication fait référence à d'autres contenus tels que des utilisateurs, des groupes, des rapports, etc., du déploiement de la plateforme de BI à répliquer ensemble.
Objet de réplication	Objet répliqué d'un site d'origine vers un site de destination. Tous les objets répliqués sur un site de destination seront marqués par une icône de réplication. En cas de conflit, les objets seront marqués par une icône de conflit.
Lot de réplications	Créé lors du transfert, le lot de réplications contient les objets d'un travail de réplication. Il peut contenir tous les objets définis dans la liste de réplication, comme dans le cas d'un environnement évoluant rapidement ou d'une réplication initiale. Il peut également contenir un sous-ensemble de la liste de réplication si les objets ne changent pas fréquemment par rapport à la planification du travail de réplication. Le lot de réplications est implémenté sous la forme d'un fichier BIAR (BI Application Resource).
Actualisation de la réplication	Tous les objets d'une liste de réplication sont actualisés, quelle que soit la date de la dernière version modifiée.
Réplication bidirectionnelle	Similaire à la réplication unidirectionnelle, à la différence que cette réplication permet l'envoi des modifications dans les deux sens. Les mises à jour apportées au site d'origine sont répliquées sur chaque site de destination. Les mises à jour et les nouveaux objets du site de destination sont envoyés au site d'origine.

27.3 Gestion des droits de sécurité

Fédération réplique des contenus entre des déploiements distincts et implique une collaboration avec d'autres administrateurs ; il est donc nécessaire de comprendre comment fonctionne la sécurité avant de commencer à utiliser cette fonctionnalité.

Les administrateurs des différents déploiements doivent effectuer un travail de coordination avant d'activer Fédération. Une fois le contenu répliqué, les administrateurs peuvent le modifier.

Pour accomplir certaines tâches, des droits spécifiques sont requis sur les déploiements d'origine et de destination :

- Droits requis sur le site d'origine
- Droits requis sur le site de destination
- Droits requis sur les objets spécifiques à Fédération
- Scénarios de Fédération

> → Conseil
>
> Il est conseillé de lire ce chapitre avant d'activer Fédération.

27.3.1 Droits requis sur le site d'origine

Cette section décrit les actions effectuées sur le site d'origine et les droits requis pour le compte utilisateur qui se connecte au site d'origine. Il s'agit du compte que vous avez saisi dans l'objet Connexion à distance sur le site de destination.

Action	Description	Droits requis
Réplication unidirectionnelle	Effectue des réplications uniquement à partir du site d'origine vers le site de destination. **ⓘ Remarque** Les droits « Visualiser » et « Répliquer » sont requis pour tous les objets en cours de réplication, notamment les objets qui sont automatiquement répliqués par des calculs de dépendance.	• Droits de « Visualiser » et « Répliquer » sur tous les objets à répliquer • Droit de « visualisation » sur la liste de réplication
Réplication bidirectionnelle	Effectue des réplications à partir du site d'origine vers le site de destination, et du site de destination vers le site d'origine.	• Droits de « Visualiser » et « Répliquer » sur tous les objets à répliquer • Droit de « visualisation » sur la liste de réplication

Action	Description	Droits requis
		• Droit « Modifier les droits » sur les objets personnels afin de pouvoir répliquer les changements de mot de passe
Planification	Autorise l'exécution de la planification à distance sur le site d'origine à partir du site de destination.	• Droit de « Planifier » pour tous les objets devant être planifiés à distance

Informations associées

Droits requis sur le site de destination [page 984]

27.3.2 Droits requis sur le site de destination

Cette section décrit les actions appliquées au site de destination et les droits requis pour le compte utilisateur qui exécute le travail de réplication. Il s'agit du compte de l'utilisateur ayant créé le travail de réplication.

> ⓘ Remarque
>
> Tout comme d'autres objets planifiables, vous pouvez planifier le travail de réplication à la place d'un autre utilisateur.

Action	Description	Droits requis
Tous les objets	Réplique les objets, que la réplication soit unidirectionnelle ou bidirectionnelle.	• Droits de « Visualisation », « Ajout », « Modification » et « Modification des droits » sur tous les objets • Droit de « Modifier le mot de passe utilisateur » pour tous les objets de l'utilisateur
Première réplication	Lors de la première exécution d'un travail de réplication, aucun objet n'existe encore sur le site de destination. Par conséquent, le compte utilisateur sous lequel le travail de réplication est exécuté doit disposer de droits sur tous les dossiers et objets de niveau supérieur auxquels du contenu sera ajouté.	• Droits de « Visualiser », « Ajouter »,« Modifier » et « Modifier des droits » sur tous les dossiers de niveau supérieur et objets par défaut

Informations associées

Droits requis sur le site d'origine [page 983]

27.3.3 Droits spécifiques à Fédération

Cette section répertorie les scénarios spécifiques à Fédération.

Action	Description	Droits requis
Nettoyage des objets	Le nettoyage des objets supprime les objets sur le site de destination.	• Le compte sous lequel s'exécute le travail de réplication requiert des droits de « Suppression » sur les objets susceptibles d'être supprimés.
Désactivez le nettoyage pour certains objets	Lorsque certains objets sont répliqués à partir du site d'origine, vous ne souhaiterez peut-être pas les supprimer du site de destination s'ils sont supprimés du site d'origine. Dans ce cas, vous pouvez utiliser ce droit. Par exemple, vous pouvez choisir cette option lorsque des utilisateurs du site de destination commencent à utiliser un objet indépendamment des utilisateurs du site d'origine. Par exemple, dans un univers répliqué dans lequel les utilisateurs du site de destination créent leurs propres rapports locaux à l'aide de cet univers, vous ne souhaiterez peut-être pas perdre cet univers sur le site de destination s'il est supprimé du site d'origine.	• Refusez les droits de « suppression » sur les objets que vous souhaitez pouvoir conserver pour le compte utilisateur sous lequel s'exécute le travail de réplication.
Réplication bidirectionnelle, sans modifications sur le site d'origine	Dans certains cas, il se peut que vous choisissiez une réplication bidirectionnelle tout en souhaitant que certains objets sur le site d'origine ne soient pas modifiés, même s'ils le sont sur le site de destination. Plusieurs raisons peuvent justifier ce choix : s'il s'agit d'objets spéciaux devant être modifiés uniquement par les utilisateurs sur le site d'origine, ou si vous souhaitez activer la planification à	• Refusez les droits « Modifier » pour le compte utilisateur utilisé pour se connecter à l'objet Connexion à distance.

Action	Description	Droits requis
	distance mais que vous ne voulez pas que les modifications apportées soient répercutées sur le site d'origine. **Remarque** Dans le cas d'une planification à distance, vous pouvez créer un travail qui gère uniquement les objets destinés à la planification à distance. Toutefois, dans ce cas, les objets d'ascendants continuent à être répliqués, notamment le rapport, le dossier contenant ce rapport et le dossier parent de ce dossier. Toutes les modifications effectuées sur le site de destination sont répliquées sur le site d'origine, et les modifications effectuées sur le site d'origine sont répliquées sur le site de destination.	

27.3.4 Réplication de la sécurité sur un objet

Pour conserver les droits de sécurité d'un objet, vous devez répliquer à la fois l'objet et l'utilisateur ou le groupe de cet objet. Sinon, ils doivent déjà exister sur le site vers lequel vous effectuez la réplication et posséder les mêmes identificateurs uniques sur chaque site.

Si un objet est répliqué mais que l'utilisateur ou le groupe de celui-ci ne l'est pas, ou s'il n'existe pas sur le site vers lequel vous effectuez la réplication, leurs droits seront supprimés.

Exemple

Les groupes A et B ont des droits affectés à l'objet A. Le groupe A possède les droits « Visualiser » et le groupe B les droits « Refuser la visualisation ». Si le travail de réplication ne réplique que le groupe A et l'objet A, sur le site de destination, l'objet A ne disposera que des droits « Visualiser » pour le groupe A qui lui est associé.

Lorsque vous répliquez un objet, il existe un risque potentiel de sécurité si vous ne répliquez pas tous les groupes disposant de droits explicites sur l'objet. L'exemple précédent souligne un risque de sécurité potentiel. Si l'utilisateur A appartient à la fois au groupe A et au groupe B, l'utilisateur n'aura pas le droit de visualiser l'objet A sur le site d'origine. Toutefois, l'utilisateur A sera répliqué sur le site de destination, car il appartient aux deux groupes. Ensuite, étant donné que le groupe B n'a pas été répliqué, l'utilisateur A aura le droit de visualiser l'objet A sur le site de destination mais pas sur le site d'origine.

Les objets qui font référence à d'autres objets non inclus dans un travail de réplication ou les objets n'existant par encore sur le site de destination sont affichés dans le fichier journal. Le fichier journal montre que l'objet a référencé l'objet non répliqué et a supprimé sa référence.

La sécurité sur un objet définie pour un utilisateur ou un groupe particulier n'est répliquée que du site d'origine vers le site de destination. Vous pouvez définir des paramètres de sécurité sur les objets répliqués sur le site de destination, mais ces paramètres ne seront pas répliqués sur le site d'origine.

27.3.5 Réplication de la sécurité à l'aide des niveaux d'accès.

Pour être maintenus, les droits doivent être définis par niveau d'accès. L'objet, l'utilisateur ou le groupe et le niveau d'accès doivent être répliqués en même temps, ou ils doivent déjà exister sur le site vers lequel vous effectuez la réplication.

Les objets qui affectent à un utilisateur ou à un groupe des droits explicites qui ne sont pas inclus dans le travail de réplication ou qui ne figurent pas encore sur le site de destination sont affichés dans le fichier journal, qui indique que des droits non répliqués étaient affectés à l'objet et que ces droits ont été supprimés.

De plus, vous pouvez choisir de répliquer automatiquement les « Niveaux d'accès » utilisés dans un objet importé. Cette option est disponible dans la liste de réplication.

> ⓘ Remarque
>
> Les niveaux d'accès par défaut ne sont pas répliqués mais les références sont conservées.

27.4 Options de types et de mode de réplication

Selon le type et le mode de réplication sélectionnés, vous pouvez choisir pour votre travail de réplication l'une des quatre options suivantes :

- Réplication unidirectionnelle
- Réplication bidirectionnelle
- Actualiser à partir du site d'origine
- Actualiser à partir de la destination

27.4.1 Réplication unidirectionnelle

La réplication unidirectionnelle ne permet de répliquer un contenu que dans un seul sens, du site d'origine vers un site de destination. Les modifications apportées aux objets du site d'origine figurant dans la liste de réplication sont transmises au site de destination. Toutefois, les modifications apportées aux objets d'un site de destination ne sont pas retransmises au site d'origine.

La réplication unidirectionnelle est idéale pour les déploiements comportant un déploiement de la plateforme de BI centralisé dans lequel les objets sont créés, modifiés et gérés. Les autres déploiements utilisent le contenu de ce déploiement centralisé.

Pour créer une réplication unidirectionnelle, sélectionnez les options suivantes :

- Type de réplication = Réplication unidirectionnelle
- Mode de réplication = Réplication normale

27.4.2 Réplication bidirectionnelle

La réplication bidirectionnelle permet de répliquer un contenu dans les deux sens, entre le site d'origine et les sites de destination. Les modifications apportées aux objets du site d'origine sont transmises aux sites de destination et les modifications apportées aux objets d'un site de destination sont transmises au site d'origine.

> **Remarque**
>
> Pour effectuer une planification à distance et répliquer des instances exécutées localement vers le site d'origine, vous devez sélectionner le mode Réplication bidirectionnelle.

Si vous disposez de plusieurs déploiements de la plateforme de BI dans lesquels des contenus sont créés, modifiés, gérés et utilisés sur les sites d'origine et de destination, la réplication bidirectionnelle est la plus appropriée. Cette option permet également de synchroniser les déploiements.

Pour créer une réplication bidirectionnelle, sélectionnez les options suivantes :

- Type de réplication = Réplication bidirectionnelle
- Mode de réplication = Réplication normale

Informations associées

Planification à distance et instances exécutées localement [page 1013]

27.4.3 Actualiser à partir du site d'origine ou Actualiser à partir de la destination

Lorsque vous répliquez du contenu en mode unidirectionnel ou en mode bidirectionnel, les objets figurant dans la liste de réplication sont répliqués sur un site de destination. Cependant, tous les objets ne peuvent pas être répliqués à chaque exécution du travail de réplication.

Fédération possède un moteur d'optimisation conçu pour vous aider à terminer vos travaux de réplication plus rapidement. Il utilise une combinaison de la version et de l'horodatage de l'objet pour déterminer si l'objet a été modifié depuis la dernière réplication. Cette vérification est effectuée sur les objets spécialement sélectionnés dans la liste de réplication ainsi que sur tout objet répliqué pendant la vérification des dépendances.

Cependant, dans certains cas, il peut manquer des objets au moteur d'optimisation, et par conséquent, ces objets ne seront pas répliqués. Dans ce cas, vous pouvez utiliser « Actualiser à partir du site d'origine » et « Actualiser à partir de la destination » pour forcer le travail de réplication à répliquer le contenu et ses dépendances, quel que soit l'horodatage.

L'option "Actualiser à partir du site d'origine" transmet simplement le contenu du site d'origine aux sites de destination. L'option "Actualiser à partir de la destination" transmet seulement le contenu des sites de destination au site d'origine.

Exemple

Les trois exemples suivants décrivent des scénarios utilisant les options « Actualiser à partir du site d'origine » et « Actualiser à partir de la destination » et dans lesquels certains objets sont ignorés en raison de l'optimisation.

Scénario 1 : Ajout d'objets contenant d'autres objets dans une zone répliquée.

Le dossier A est répliqué à partir du site d'origine sur le site de destination. Il existe à présent sur les deux sites. Un utilisateur déplace ou copie le dossier B avec le rapport B dans le dossier A sur le site d'origine. Lors de la réplication suivante, Fédération verra que l'horodatage du dossier B a changé et répliquera la modification sur le site de destination. Cependant, l'horodatage du rapport B ne change pas. Par conséquent, il sera ignoré dans un travail de réplication unidirectionnel ou bidirectionnel standard.

Pour s'assurer que le contenu du dossier B est correctement répliqué, un travail de réplication avec l'option « Actualiser à partir du site d'origine » doit être utilisé immédiatement. Après cette opération, le travail de réplication unidirectionnel ou bidirectionnel standard s'exécutera correctement. Si cet exemple est inversé et que le dossier B est déplacé ou copié sur le site de destination, utilisez l'option « Actualiser à partir de la destination ».

Scénario 2 : Ajout de nouveaux objets à l'aide de LifeCycle Manager ou de la ligne de commande BIAR.

Lorsque vous ajoutez des objets dans une zone répliquée à l'aide de LifeCycle Manager ou de la ligne de commande BIAR, l'objet peut ne pas être recueilli par un travail de réplication unidirectionnel ou bidirectionnel standard. Cela se produit car les horloges internes des systèmes source et de destination peuvent ne plus être synchronisées lors de l'utilisation de LifeCycle Manager ou de la ligne de commande BIAR.

> ⓘ Remarque
>
> Après l'importation de nouveaux objets dans une zone en cours de réplication sur le site d'origine, il est recommandé d'exécuter un travail de réplication avec l'option « Actualiser à partir du site d'origine ». Après l'importation de nouveaux objets dans une zone en cours de réplication sur le site de destination, il est recommandé d'exécuter un travail de réplication avec l'option « Actualiser à partir de la destination ».

Scénario 3 : Entre les heures de réplication planifiées.

Si vous ajoutez des objets dans une zone en cours de réplication et que vous ne pouvez pas attendre la prochaine heure de réplication planifiée, vous pouvez utiliser les travaux de réplication « Actualiser à partir du site d'origine » et « Actualiser à partir de la destination ». En sélectionnant la zone dans laquelle les objets ont été ajoutés, vous pouvez répliquer rapidement le contenu.

> ⓘ Remarque
>
> Ce scénario peut s'avérer onéreux si les listes de réplication sont importantes ; il est donc conseillé de ne pas utiliser très souvent cette option. Par exemple, il n'est pas nécessaire de créer des travaux de

réplication qui s'exécutent en mode d'actualisation du site d'origine vers les sites de destination toutes les heures. Ces modes doivent être utilisés pour l'« exécution immédiate » ou pour des planifications peu fréquentes.

> ⓘ Remarque
>
> Dans certains cas, vous ne pouvez pas utiliser la résolution de conflit, par exemple : « Actualiser à partir du site d'origine » : l'option Le site de destination l'emporte est bloquée, ou « Actualiser à partir de la destination » : l'option Le site d'origine l'emporte est bloquée.

27.5 Réplication d'utilisateurs et de groupes tiers

Fédération permet de répliquer des utilisateurs et des groupes tiers, en particulier les utilisateurs et groupes Active Directory (AD) et LDAP.

> → Conseil
>
> Lisez cette section si vous envisagez de répliquer ces types d'utilisateur et de groupe ou leur contenu personnel, tel que les dossiers favoris ou les boîtes de réception.

Mappage d'utilisateurs et de groupes

1. Vous devez mapper les utilisateurs et les groupes sur le site d'origine afin que Fédération puisse les répliquer correctement.
2. Répliquez les utilisateurs et groupes mappés sur le site de destination.

> ⓘ Remarque
>
> Ne mappez pas les groupes et les utilisateurs séparément sur le site de destination. Autrement, ils se verront affecter des identificateurs uniques (CUID) différents sur les sites de destination et d'origine, et Fédération ne parviendra pas à mettre en correspondance l'utilisateur ou les groupes.

Exemple

L'administrateur mappe le groupe A à l'utilisateur A sur les sites d'origine et de destination. Le groupe A et l'utilisateur A auront tous deux des identificateurs uniques différents sur les sites d'origine et de destination. Lors de la réplication, Fédération ne parvient pas à effectuer la mise en correspondance, et le groupe A ou l'utilisateur A se sont pas répliqués en raison d'un conflit d'alias.

> ⓘ Remarque
>
> Le site de destination doit être configuré pour utiliser l'authentification Active Directory ou LDAP avant la réplication des utilisateurs et des groupes tiers. Toutefois, vous devez également configurer le site de

destination de manière à ce qu'il utilise AD ou LDAP pour communiquer avec le serveur d'annuaire ou le contrôleur de domaine.

> **Remarque**
>
> Après la toute première réplication d'un groupe AD ou LDAP, les utilisateurs de ce groupe ne peuvent plus se connecter tant que le diagramme de groupe AD/LDAP n'a pas été actualisé. Cela se produit automatiquement toutes les 15 minutes environ. Pour actualiser manuellement le diagramme de groupe AD/LDAP, ouvrez la page *Authentification* de la CMC, cliquez deux fois sur *Windows AD* ou sur *LDAP*, puis sur *Mettre à jour*.

> **Remarque**
>
> Soyez prudent lorsque vous répliquez des groupes tiers. Si vous ajoutez des utilisateurs à un groupe sur le serveur d'annuaire, ces utilisateurs pourront se connecter au site d'origine et au site de destination. Ce problème de sécurité de l'authentification AD ou LDAP ne dépend pas de Fédération.
>
> Si vous vous connectez aux sites d'origine et de destination séparément, ou si l'appartenance au groupe est mise à jour sur les deux sites à l'aide du bouton de mise à jour figurant sur la page d'authentification de la CMC, un compte utilisateur est créé sur les deux sites. Les comptes auront donc des identificateurs uniques différents et Fédération ne pourra pas les répliquer correctement.
>
> Il est important de ne créer le compte que sur un seul site, puis de le répliquer sur l'autre site.

27.6 Réplication des univers et des connexions d'univers

Il est important de planifier à l'avance si vous utilisez Fédération pour répliquer des univers entre les déploiements de la plateforme de BI. Un objet d'univers ne peut fonctionner sans une connexion d'univers sous-jacente.

Les objets Connexion d'univers contiennent des informations requises pour la connexion à une base de données de reporting. Pour fonctionner efficacement, les objets de connexion d'univers doivent contenir des informations valides et autoriser l'implantation d'une connexion à la base de données.

> **Remarque**
>
> Si vous utilisez la réplication bidirectionnelle et que vous répliquez un univers à partir du site d'origine sur le site de destination sans sa connexion d'univers associée, la relation entre l'univers du site d'origine et la connexion d'univers sur le site d'origine pourrait être écrasée ou supprimée dans les réplications suivantes. Pour éviter cela, répliquez toujours les connexions d'univers en même temps que les univers.

Afin de vous assurer que les connexions d'univers dépendantes sont répliquées avec les univers, sélectionnez systématiquement les options suivantes lorsque vous créez ou modifiez la liste de réplication qui contient les univers :

- *Inclure les connexions utilisées par les univers sélectionnés*
- *Inclure les univers requis par les univers sélectionnés*

> **Remarque**
>
> Si la relation d'un univers avec sa connexion d'univers a été écrasée ou supprimée, ouvrez l'univers dans Universe Designer, et sous *Fichier* > *Paramètres* >, modifiez les informations de connexion.

Les deux exemples suivants illustrent le processus de réplication d'univers et de leurs connexions d'univers associées.

Exemple

Lors de la réplication d'univers et de connexions d'univers, vous devez vous assurer que l'environnement de connectivité sur le site d'origine correspond à celui du site de destination.

Par exemple, si la connexion d'univers utilise une connexion ODBC appelée « TestODBC », une connexion ODBC bien configurée appelée « TestODBC » doit exister dans l'environnement de destination. La connexion ODBC peut se résoudre sous la forme de la même base de données ou d'une base de données différente. Pour s'assurer que les univers utilisant cette connexion ne rencontrent aucun problème de connectivité, les schémas de la base de données doivent être identiques.

Exemple

Si vous souhaitez que l'univers répliqué sur le site de destination utilise une autre base de données que celle utilisée par l'univers sur le site d'origine, répliquez la connexion d'univers mais faites pointer les informations de connectivité sur le site de destination vers la base de données souhaitée.

Par exemple, si la connexion d'univers sur le site d'origine utilise une connexion ODBC appelée « Test » pointant vers la « BasededonnéesA », vous devez vous assurer d'avoir une connexion ODBC sur le site de destination également appelée « Test » mais pointant vers la « BasededonnéesB ».

27.7 Gestion des listes de réplication

Les listes de réplication contiennent du contenu tel que des utilisateurs, des groupes et des rapports du déploiement de la plateforme de BI qui peuvent être répliqués ensemble. Les listes de réplication sont accessibles depuis la CMC.

Les types de contenu pouvant être répliqués sont répertoriés dans le tableau suivant.

Catégorie	Objets pris en charge
Objets du référentiel	Objets tels que les vues d'entreprise, les connexions de données, les listes de valeurs, les fondations de données, etc.

Catégorie	Objets pris en charge
	Remarque Tous les objets sont pris en charge, bien qu'ils ne le soient pas au niveau individuel.
Rapports	Rapports Crystal, documents Web Intelligence et objets Dashboards. **Remarque** Le module complémentaire et les modèles Full Client sont pris en charge.
Objets tiers	Fichiers Excel, PDF, PowerPoint, Word, texte, texte enrichi et ShockWave.
Utilisateurs	Utilisateurs, groupes, boîtes de réception, favoris, catégorie personnelle.
Plateforme de Business Intelligence	Dossiers, événements, catégories, calendriers, rôles personnalisés, liens hypertexte, raccourcis, programmes, profils, lots d'objets, objets agnostiques.
Univers	Univers, connexions, surcharges d'univers.

Remarque

Les objets suivants doivent être créés sur le site d'origine, puis répliqués sur le site de destination. Si vous créez ces objets sur le site de destination, puis que vous les répliquez sur le site d'origine, ils ne fonctionneront pas sur le site d'origine.

- Vues d'entreprise
- éléments d'entreprise
- Fondations de données
- Connexions de données
- Listes de valeurs
- Surcharges d'univers

27.7.1 Création de listes de réplication

Les listes de réplication se trouvent dans la zone Listes de réplication de la CMC. Vous pouvez organiser les listes de réplication dans des dossiers et des sous-dossiers que vous créez.

27.7.1.1 Pour créer un dossier Liste de réplication

1. Accédez à la zone *Listes de réplication* de la CMC.

2. Cliquez sur *Listes de réplication*.
3. Cliquez sur *Gérer* > *Nouveau* > *Dossier*.
   La boîte de dialogue *Créer un dossier* s'affiche.
4. Saisissez un nom de dossier et cliquez sur *OK*.
   Vous pouvez désormais créer des listes de réplication dans ce dossier

27.7.1.2 Pour créer une liste de réplication

1. Accédez à la zone *Listes de réplication* de la CMC.
2. Sélectionnez le dossier dans lequel vous souhaitez enregistrer votre nouvelle liste de réplication.
3. Cliquez sur *Gérer* > *Nouveau* > *Nouvelle liste de réplication*.
   La boîte de dialogue *Nouvelle liste de réplication* s'affiche.
4. Saisissez le titre et la description de la liste de réplication.
5. Pour afficher les options avancées, cliquez sur le lien *Propriétés de la liste de réplication*.

   Cela vous permet d'indiquer quelles sont les dépendances du site d'origine à répliquer automatiquement sur le site de destination.
6. Sélectionnez les options requises selon la description du tableau.

Options des objets de dépendance	Définition
Inclure les dossiers personnels des utilisateurs sélectionnés	Réplique les dossiers personnels d'un utilisateur sélectionné avec leur contenu.
Inclure les catégories personnelles des utilisateurs sélectionnés	Réplique les catégories personnelles d'un utilisateur sélectionné.
Inclure les univers des rapports sélectionnés	Réplique tout univers dont les objets du rapport sélectionné dépendent.
Inclure les membres des groupes d'utilisateurs sélectionnés	Réplique les utilisateurs d'un groupe sélectionné.
Inclure les univers requis par les univers sélectionnés	Réplique tout univers dépendant d'autres univers.
Inclure les boîtes de réception des utilisateurs sélectionnés	Réplique la boîte de réception d'un utilisateur sélectionné et son contenu.
Inclure les groupes d'utilisateurs des univers sélectionnés	Réplique les groupes d'utilisateurs associés aux surcharges d'un univers.
Inclure les niveaux d'accès définis sur les objets sélectionnés	Réplique tout niveau d'accès utilisé sur un objet sélectionné.
Inclure les documents des catégories sélectionnées	Réplique tout document, notamment Word, Excel et PDF inclus dans les catégories sélectionnées.
Inclure les profils des utilisateurs et des groupes d'utilisateurs sélectionnés	Réplique tout profil associé aux utilisateurs ou groupes sélectionnés.
Inclure les connexions utilisées par les univers sélectionnés	Réplique tout objet de connexion d'univers utilisé par les objets sélectionnés.

> **Remarque**
>
> Certains objets de la plateforme de BI dépendent d'autres objets. Par exemple, un document Web Intelligence dépend de l'univers sous-jacent pour sa structure et son contenu. Si vous répliquez un document Web Intelligence mais que vous ne sélectionnez pas l'univers qu'il utilise, la réplication échouera sur le site de destination à moins que l'univers n'ait déjà été répliqué à cet emplacement. Cependant, si vous activez *Inclure les univers des rapports sélectionnés*, Fédération réplique automatiquement les univers dont dépend le rapport.

7. Cliquez sur *Suivant*.
8. Sélectionnez un ou plusieurs objets à ajouter à votre liste de réplication.
   - Utilisez les boutons flèches pour ajouter ou supprimer des objets dans le dossier *Objets disponibles*.
   - Vous pouvez également cliquer sur *Objets du référentiel* sous *Tout répliquer* pour répliquer tous les objets Vue d'entreprise, Éléments d'entreprise, Fondation de données, Connexion de données, Liste de valeurs et les objets du référentiel, y compris les images et les fonctions des rapports.

> **Remarque**
>
> Il est impossible de répliquer les dossiers de niveau supérieur qui se trouvent dans le dossier *Objets disponibles*.

9. Cliquez sur *Enregistrer et fermer*.

27.7.2 Modification des listes de réplication

Une fois la liste de réplication créée, vous pouvez modifier ses propriétés ou ses objets.

27.7.2.1 Pour modifier les propriétés d'une liste de réplication

1. Accédez à la zone *Listes de réplication* de la CMC.
2. Sélectionnez la *liste de réplication* que vous souhaitez modifier.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés générales* s'affiche.
4. Modifiez le titre et la description. Vous pouvez également modifier les autres zones d'une liste de réplication pendant que la boîte de dialogue *Propriétés* est ouverte.
5. Pour modifier des options de dépendance, cliquez sur *Propriétés de la liste de réplication* dans la liste de navigation.
6. Cliquez sur *Enregistrer et fermer*.

Informations associées

Création de listes de réplication [page 993]

27.7.2.2 Pour modifier les objets d'une liste de réplication

1. Accédez à la zone *Listes de réplication* de la CMC.
2. Sélectionnez une *liste de réplication*.
3. Cliquez sur *Actions* > *Gérer la liste de réplication*.
   La boîte de dialogue *Gérer la liste de réplication* s'affiche avec une liste d'objets compris dans la liste de réplication.
4. Ajoutez ou supprimez des objets en fonction des besoins.
5. Cliquez sur *Enregistrer et fermer*.

Informations associées

Création de listes de réplication [page 993]

27.8 Gestion des connexions à distance

Les objets Connexion à distance contiennent les informations nécessaires pour se connecter à un déploiement distant de la plateforme de BI.

> **Remarque**
>
> L'objet Connexion à distance est créé sur un déploiement de la plateforme de BI du site de destination. La connexion à distance est le site d'origine.

Vous pouvez visualiser les connexions à distance dans la zone *Fédération* de la CMC.

27.8.1 Création de connexions à distance

Dans Fédération, une connexion à distance s'effectue avec un déploiement de la plateforme de BI distant. Pour établir une connexion au site d'origine sur lequel se trouve le contenu à répliquer, vous devez d'abord créer une connexion à distance sur le site de destination.

Vous pouvez créer des dossiers et des sous-dossiers pour organiser vos connexions à distance.

27.8.1.1 Création d'un dossier Connexion à distance

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur *Connexions à distance*.

3. Cliquez sur *Gérer* > *Nouveau* > *Dossier*.
   La boîte de dialogue *Créer un dossier* s'affiche.
4. Saisissez le nom du dossier et cliquez sur *OK*.
   Vous pouvez désormais créer des connexions à distance dans ce dossier.

27.8.1.2 Pour créer une connexion à distance

Pour vous connecter à un déploiement distant de la plateforme de BI, vous devez créer une connexion à distance dans Fédération.

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur *Connexions à distance*.
3. Cliquez sur *Gérer* > *Nouvelle* > *Nouvelle connexion à distance*.
   La boîte de dialogue *Nouvelle connexion de système distant* s'affiche.
4. Saisissez un titre et une description, et renseignez les champs associés le cas échéant :

> **Remarque**
>
> Tous les champs sont obligatoires, à l'exception de « Description » et « Limiter le nombre d'objets de nettoyage ».

Champ	Description
Titre	Nom de l'objet Connexion à distance.
Description	Description de l'objet Connexion à distance. (Facultatif)
URI de Service Web du système distant	URL des services Web de Fédération qui est automatiquement déployée sur votre serveur d'applications Java. Vous pouvez utiliser n'importe quel service Web de Fédération dans la plateforme de BI, que ce service se trouve sur le site d'origine ou le site de destination, ou encore dans un autre déploiement. Utilisez ce format : `http://<nom_ordinateur_votreserveur_application>:<port>/dswsbobje` Exemple : `http://<monordinateur.mondomaine.com>:<8080>/dswsbobje`
CMS de système distant	Nom du CMS auquel vous souhaitez vous connecter et qui est accessible via les services Web de Fédération. Il sera considéré comme CMS du site d'origine. Voici le format : `CMS_Name:port`. Exemple : `<monordinateur>:6400` **Remarque** Si vous utilisez le port 6400 par défaut, l'indication du port est facultative.

Champ	Description
Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion au site d'origine. **Remarque** Assurez-vous que le nom d'utilisateur utilisé possède les droits de consultation de la liste de réplication dans le déploiement sur le site d'origine.
Mot de passe	Mot de passe du compte utilisateur nécessaire à la connexion au site d'origine.
Authentification	Type d'authentification de compte pour la connexion au site d'origine. Les options sont les suivantes : Enterprise, AD ou LDAP.
Fréquence de nettoyage (en heures)	Fréquence à laquelle les travaux de réplication utilisant cet objet Connexion à distance effectuent un nettoyage des objets. Saisissez uniquement des nombres entiers positifs. L'unité est l'heure. La valeur par défaut est 24.
Limiter le nombre d'objets de nettoyage à	Nombre d'objets qui doivent être nettoyés par le travail de réplication. (Facultatif)

5. Cliquez sur *OK*.

27.8.2 Modification des connexions à distance

Une fois la connexion à distance créée, vous pouvez modifier ses propriétés et sa sécurité.

Pour modifier une connexion à distance :

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur *Connexions à distance*.
3. Cliquez deux fois sur la connexion à distance à modifier.
   La boîte de dialogue *Propriétés de la connexion à distance* s'affiche. Vous pouvez modifier les propriétés suivantes :
   - *Titre*
   - *Description*
   - *URI de Service Web du système distant*
   - *CMS de système distant*
   - *Nom d'utilisateur*
   - *Mot de passe*
   - *Authentification*
   - *Fréquence de nettoyage (en heures)*
   - *Limiter le nombre d'objets de nettoyage à*
4. Spécifiez vos modifications.
5. Cliquez sur *Enregistrer et fermer*.

27.9 Gestion des travaux de réplication

Un travail de réplication est un type d'objet exécuté selon une planification et utilisé pour répliquer du contenu entre deux déploiements de la plateforme de BI dans Fédération.

> **Remarque**
>
> Les objets répliqués sur un site de destination seront signalés par une icône de réplication, comme illustré ici : . En cas de conflit, un objet sera signalé par une icône de conflit, comme illustré ici :

Vous pouvez visualiser une liste des travaux de réplication dans le dossier *Connexion à distance* dans la zone *Fédération* de la CMC.

27.9.1 Création de travaux de réplication

Dans Fédération, un travail de réplication est nécessaire pour répliquer du contenu entre deux déploiements de la plateforme de BI. Chaque travail de réplication doit être associé à une seule connexion à distance et à une liste de réplication.

27.9.1.1 Pour créer un travail de réplication

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur *Connexions à distance*.
3. Sélectionnez la *Connexion à distance* qui contiendra le nouveau travail de réplication.

   > **Attention**
   >
   > La CMC doit pouvoir se connecter aux services Web dans l'URI de la connexion à distance pour continuer à l'aide de l'Assistant d'importation.

4. Cliquez sur *Gérer* > *Nouveau* > *Nouveau travail de réplication*.
   Une boîte de dialogue *Nouveau travail de réplication* s'affiche.
5. Saisissez un titre et une description du travail de réplication.
6. Cliquez sur *Suivant*.
   La liste des listes de réplication disponibles sur le site d'origine s'affiche.
7. Sélectionnez la *Liste de réplication* que vous souhaitez utiliser pour votre travail de réplication.
8. Cliquez sur *Suivant*.
9. Sélectionnez les options de configuration comme décrit dans le tableau ci-dessous.

Option	Description
Activer le nettoyage des objets sur la destination	Force le travail de réplication à supprimer tout objet répliqué sur le site de destination, lorsque l'objet d'origine a été supprimé sur le site d'origine. **Remarque** Le nettoyage des objets ne supprime pas les objets répliqués à l'aide de dépendances ou d'objets sélectionnés dans la liste de réplication.
Réplication unidirectionnelle	Indique qu'un objet est uniquement répliqué à partir du site d'origine sur le site de destination. Toute modification effectuée après la réplication de l'objet sur le site d'origine est répliquée sur le site de destination, mais les modifications apportées sur le site de destination ne seront pas répliquées sur le site d'origine.
Réplication bidirectionnelle	Indique que les objets sont répliqués dans les deux sens : du site d'origine vers le site de destination et du site de destination vers le site d'origine. Les modifications apportées à ces objets après la réplication sur un site sont ensuite répliquées sur l'autre site.
Le site d'origine est prioritaire	Indique que lorsqu'un conflit est détecté entre un objet sur le site d'origine et sa version répliquée sur le site de destination, la version du site d'origine est prioritaire.
Pas de résolution automatique de conflit	Indique qu'aucune action n'est prise pour résoudre les conflits détectés.
Le site de destination est prioritaire (uniquement disponible avec la réplication bidirectionnelle)	Indique que lorsqu'un conflit est détecté entre un objet sur le site d'origine et sa version répliquée sur le site de destination, la version du site de destination est prioritaire.
Réplication normale	Indique que le travail de réplication est exécuté normalement.
Actualiser à partir du site d'origine	Réplique tout le contenu du site d'origine sur le site de destination, que ce contenu ait été modifié ou non. Vous pouvez répliquer l'intégralité de la liste de réplication ou uniquement une partie.
Actualiser à partir de la destination (uniquement disponible avec la réplication bidirectionnelle)	Réplique tout le contenu du site de destination sur le site d'origine, que ce contenu ait été modifié ou non. Vous pouvez répliquer l'intégralité de la liste de réplication ou uniquement une partie.
Répliquer tous les objets (disponible uniquement avec la réplication bidirectionnelle)	Réplique l'intégralité de la liste de réplication. **Remarque** Il s'agit de l'option la plus complète, mais aussi de la plus longue en termes de temps d'exécution.
Répliquer les planifications distantes (disponible uniquement avec la réplication bidirectionnelle)	Réplique les instances distantes en suspens du site de destination vers le site d'origine et force la réplication

Option	Description
	des instances finalisées du site d'origine vers le site de destination.
Répliquer les modèles de document	Réplique tous les objets qui ne sont pas des instances (instances exécutées localement ou rapports vérifiés dans le cadre d'une planification à distance). Sont inclus les utilisateurs, les groupes, les dossiers, les rapports, etc.
Répliquer les instances finalisées exécutées localement	Réplique les instances finalisées uniquement du site de destination vers le site d'origine.

10. Cliquez sur *OK*.

27.9.2 Planification de travaux de réplication

Une fois un travail de réplication créé, vous pouvez le planifier de façon à ce qu'il s'exécute une seule fois ou de manière périodique. Vous pouvez également planifier plusieurs travaux de réplication sur un site de destination à partir d'un site d'origine.

> **Remarque**
>
> Si vous avez planifié plusieurs travaux de réplication sur un site de destination, un seul travail de réplication peut se connecter au site d'origine à la fois. Tous les autres travaux de réplication essayant de se connecter seront placés en suspens et le resteront jusqu'à ce qu'ils puissent se connecter automatiquement au site d'origine.

27.9.2.1 Pour planifier un travail de réplication

1. Accédez à la zone *Fédération* de la CMC.
2. Sélectionnez le *Travail de réplication* que vous souhaitez planifier.
3. Cliquez sur *Actions* > *Planifications*.
4. Sélectionnez les options de planification souhaitées.

27.9.3 Modification des travaux de réplication

Après la création d'un travail de réplication dans Fédération, vous pouvez modifier ses propriétés.

27.9.3.1 Pour modifier un travail de réplication

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur le dossier *Connexions à distance*.
3. Sélectionnez l'objet *Connexion à distance* contenant le *travail de réplication* à modifier.
4. Sélectionnez le *travail de réplication* que vous souhaitez modifier.
5. Cliquez sur *Gérer* > *Gérer les propriétés de l'objet*.
6. Visualisez et modifiez selon les besoins les éléments suivants : *Propriétés*, *Planification*, *Historique*, *Liste de réplication* et *Sécurité de l'utilisateur*.

Sections	Description
Propriétés	Permet de modifier le nom, la description et d'autres propriétés et options générales du travail de réplication.
Planification	Permet de définir le travail de réplication de façon à ce qu'il s'exécute selon une planification régulière.
Historique	Permet de visualiser et d'administrer toutes les instances du travail de réplication.
Liste de réplication	Permet de modifier la liste de réplication sélectionnée.
Sécurité de l'utilisateur	Permet de définir les droits sur le travail de réplication.

27.9.4 Visualisation d'un journal après un travail de réplication

A chaque exécution d'un travail de réplication, Fédération crée automatiquement un fichier journal sur le site de destination. Les fichiers journaux utilisent les normes XML 1.1 et nécessitent un navigateur Web prenant en charge XML 1.1.

Pour visualiser un journal de réplication :

1. Accédez à la zone *Fédération* de la CMC.
2. Cliquez sur *Tous les travaux de réplication*.
3. Sélectionnez un *Travail de réplication* dans la liste.
4. Cliquez sur *Propriétés*.
   La page *Propriétés* du travail de réplication s'ouvre.
5. Cliquez sur *Historique*.
6. Cliquez sur l'*Heure de l'instance* du fichier journal pour visualiser les travaux de réplication réussis ou cliquez sur le statut *Echec* pour visualiser un fichier journal des travaux de réplication ayant échoué.
7. Sélectionnez l'instance souhaitée pour visualiser le fichier journal.
   Le fichier journal est généré au format XML et utilise un formulaire XSL pour formater les informations sur une page HTML.

   Vous pouvez accéder au journal XML à partir de l'ordinateur qui exécute le Server Intelligence Agent contenant le serveur Adaptative Job Server. Le fichier journal se trouve à cet emplacement :

- Sous Windows : `<RepInstall>\SAP BusinessObjects XI 4.0\logging`
- Sous Unix : `<RepInstall>/sap_bobj/logging`

27.10 Gestion du nettoyage des objets

Dans Fédération, vous devez effectuer un nettoyage des objets durant le cycle de vie de votre processus de réplication afin de vous assurer que tous les objets que vous supprimez du site d'origine sont également supprimés de chaque site de destination.

Le nettoyage des objets implique deux éléments : une connexion à distance et un travail de réplication. Un objet Connexion à distance définit les options générales de nettoyage, et un travail de réplication effectue le nettoyage à la fin de l'intervalle approprié.

27.10.1 Utilisation du nettoyage des objets

Les différents travaux de réplication qui utilisent la même connexion à distance fonctionnent ensemble lors du nettoyage des objets. Autrement dit, votre travail de réplication nettoie les objets qui figurent dans sa liste de réplication, ainsi que les objets qui figurent dans les autres listes de réplication utilisant la même connexion à distance. Une connexion à distance n'est considérée comme identique que si le parent du travail de réplication est le même objet Connexion à distance.

Exemple

Les travaux de réplication A et B répliquent les objets A et B. Ces deux travaux effectuent la réplication à partir du même site d'origine et utilisent la même connexion à distance. Si le site d'origine supprime l'objet B, le travail de réplication A verra que cet objet a été supprimé. Même si la réplication est effectuée par le travail de réplication B, l'objet B sera également supprimé du site de destination. Pendant l'exécution du travail de réplication B, aucun nettoyage d'objet ne sera nécessaire.

> **Remarque**
>
> Seuls les objets du site de destination sont supprimés lors du nettoyage des objets. Si vous supprimez un objet faisant partie de la réplication du site d'origine, l'objet sera également supprimé du site de destination. Toutefois, lorsqu'un objet est supprimé du site de destination, il n'est pas supprimé du site d'origine lors de la phase de nettoyage, même si le travail de réplication fonctionne en mode bidirectionnel.
>
> Les objets qui sont supprimés ou déplacés de la liste de réplication ne sont pas supprimés du site de destination. Pour supprimer correctement un objet spécifié dans une liste de réplication, vous devez le supprimer à la fois sur le site de destination et sur le site d'origine. Les objets qui sont répliqués via des calculs de dépendances ne sont pas supprimés.

27.10.2 Limites du nettoyage des objets

L'objet Connexion à distance permet de définir le nombre d'objets qu'un travail de réplication peut nettoyer en une fois. Fédération suit automatiquement l'emplacement où se termine le travail de nettoyage. De cette façon, à la prochaine exécution d'un travail de réplication, le travail de nettoyage suivant reprend à partir de cet emplacement.

> → Conseil
>
> Pour effectuer plus rapidement un travail de réplication, limitez le nombre d'objets à nettoyer.

Exemple

Les travaux de réplication A et B répliquent les objets A et B. Ces deux objets sont répliqués à partir du même site d'origine et utilisent la même connexion à distance.

Si le site d'origine supprime l'objet B et que la limite d'objet est définie sur 1, à la prochaine exécution du travail de réplication A, seule la suppression de l'objet A sera vérifiée. Ainsi, l'objet B ne sera ni vérifié ni supprimé.

Le travail de réplication B s'exécute ensuite et démarre le nettoyage des objets à l'emplacement où le travail de réplication A s'est arrêté. Il vérifie si l'objet B a été supprimé, puis le supprime du site de destination. Cette option se trouve dans la propriété « Limiter le nombre d'objets de nettoyage à : » de l'objet Connexion à distance.

> ⓘ Remarque
>
> Si vous ne sélectionnez pas cette option, tous les travaux de réplication utilisant cette connexion à distance rechercheront si un nettoyage potentiel doit être effectué pour tous les objets.

27.10.3 Fréquence de nettoyage des objets

Vous pouvez définir la fréquence à laquelle un travail de réplication effectue le nettoyage des objets dans le champ « Fréquence de nettoyage » de la connexion à distance.

> ⓘ Remarque
>
> Vous devez saisir un nombre entier positif représentant le nombre d'heures à attendre entre chaque traitement de nettoyage des objets.

Exemple

Les travaux de réplication A et B répliquent les objets A et B. Ces deux objets sont répliqués à partir du même site d'origine et utilisent la même connexion à distance.

Si l'objet B est supprimé du site d'origine et que toutes les conditions suivantes sont vérifiées, le travail de réplication A vérifiera si l'objet A a été supprimé.

- La limite des objets est 1.
- La fréquence de nettoyage est 150 heures.
- Le travail de réplication A s'exécute ensuite.

La limite des objets étant 1, l'objet B ne sera ni vérifié ni supprimé sur le site de destination.

Le nettoyage suivant se produit 150 heures après la vérification initiale du travail de réplication A. Bien que les travaux de réplication A et B puissent s'exécuter de nombreuses fois avant la fin du délai de 150 heures, aucun d'eux n'essaiera d'effectuer un nettoyage des objets. Ce dernier sera effectué par le travail de réplication suivant à l'expiration des 150 heures. Il va ensuite déterminer que l'objet B a été supprimé sur le site d'origine et le supprimera sur le site de destination.

Activation et désactivation des options

Chaque travail de réplication peut participer au nettoyage des objets. Utilisez l'option « Activer le nettoyage des objets sur la destination » pour un travail de réplication pour indiquer s'il doit exécuter ou non un nettoyage des objets. Dans certains cas, comme par exemple des travaux de réplication à priorité élevée, vous ne souhaiterez pas effectuer de nettoyage des objets afin de ne pas ralentir leur exécution. Pour ce faire, désactivez le nettoyage des objets.

Informations associées

Limites du nettoyage des objets [page 1004]

27.11 Gestion de la détection et de la résolution des conflits

Dans Fédération, un conflit peut se produire lorsque les propriétés d'un objet sont modifiées à la fois sur le site d'origine et sur le site de destination. Les conflits sont recherchés à la fois dans les propriétés de niveau supérieur et les propriétés imbriquées d'un objet. Par exemple, un conflit peut se produire si un rapport ou le nom d'un rapport est modifié à la fois sur les sites d'origine et de destination.

Certaines instances ne créent pas de conflit. Par exemple, si le nom d'un rapport est modifié sur le site d'origine et la description de la version répliquée est modifiée sur le site de destination, les modifications sont fusionnées et aucun conflit ne se produit.

27.11.1 Résolution des conflits de réplication unidirectionnelle

Dans le cas d'une réplication unidirectionnelle, vous avez deux façons de résoudre les conflits.

Le site d'origine est prioritaire

Si un conflit se produit lors d'une réplication unidirectionnelle, l'objet site d'origine est prioritaire. Toute modification apportée aux objets sur un site de destination est remplacée par les informations du site d'origine. Par exemple, si un rapport est modifié à la fois sur le site d'origine et le site de destination, la modification de ce dernier sera remplacée par la version du site d'origine après le prochain travail de réplication.

> ⓘ Remarque
>
> Etant donné que le conflit est résolu automatiquement, il n'est pas généré dans le fichier journal et il ne figure pas non plus dans la liste des objets en conflit.

Pas de résolution automatique de conflit

Si un conflit se produit et que vous sélectionnez « Pas de résolution automatique de conflit », le conflit n'est pas résolu, aucun fichier journal n'est généré et le conflit ne figure pas dans la liste des objets en conflit.

Les administrateurs peuvent accéder à une liste de tous les objets répliqués en conflit dans la zone Fédération de la CMC. Les objets en conflit sont regroupés selon la connexion à distance qu'ils utilisent avec le site d'origine. Pour accéder à ces listes, ouvrez le dossier Erreurs de réplication dans la zone Fédération de la CMC, puis sélectionnez la connexion à distance souhaitée. Tous les objets répliqués sur un site de destination seront signalés par une icône de réplication. En cas de conflit, les objets seront signalés par une icône de conflit. Un message d'avertissement s'affiche également dans la page *Propriétés*.

> ⓘ Remarque
>
> La liste est mise à jour lorsqu'un travail de réplication utilisant une connexion à distance est terminé. Elle contient tous les objets en conflit pour tous les travaux de réplication utilisant sa connexion à distance.

> ⓘ Remarque
>
> Tout utilisateur disposant d'un accès à la CMC et aux instances de travaux de réplication peut accéder au journal XML enregistré dans le répertoire des fichiers journaux. Une icône d'un objet du site de destination possède un indicateur pour signaler le conflit. Lors du traitement, un journal de conflit est créé.

Abdul modifie le rapport A sur le site d'origine. Maria modifie la version répliquée sur le site de destination. La prochaine fois que le travail de réplication sera exécuté, un conflit se produira, car le rapport a été modifié sur les deux sites, et ce conflit ne sera pas résolu.

Le rapport du site de destination sera conservé et les modifications apportées au rapport du site d'origine ne seront pas répliquées. Les travaux de réplication suivants se comporteront de la même manière jusqu'à ce que le conflit soit résolu. Toutes les modifications effectuées sur le site d'origine ne seront répliquées que lorsque le conflit aura été manuellement résolu.

> ⓘ Remarque
>
> Dans ce cas, c'est la totalité de l'objet qui n'est pas répliqué. Aucune autre modification, même si elle ne crée aucun conflit, n'est répliquée.

Pour résoudre manuellement un conflit, vous avez le choix entre trois possibilités :

1. Créez un travail de réplication qui réplique uniquement les objets en conflit. Il doit utiliser le même objet Connexion à distance et la même liste de réplication.
   Pour conserver les modifications du site d'origine, créez un travail de réplication. Définissez ensuite le mode de réplication sur « Actualiser à partir du site d'origine » et la résolution automatique de conflit sur « Le site d'origine est prioritaire ».
   Pour conserver les modifications du site de destination, créez un travail de réplication avec le type de réplication « Réplication bidirectionnelle », le mode de réplication « Actualiser à partir de la destination » et la résolution automatique de conflit « Le site de destination est prioritaire ».

   > ⓘ Remarque
   >
   > En mode de réplication, définissez « Actualiser à partir du site d'origine » ou « Actualiser à partir de la destination » pour sélectionner uniquement les objets en conflit dans la liste de réplication. De cette façon, les autres objets ne seront pas répliqués. Ensuite, planifiez le travail de réplication à exécuter afin de répliquer les objets sélectionnés et de résoudre le conflit comme indiqué.

2. Créez un travail de réplication qui réplique uniquement les objets en conflit. Il devra utiliser le même objet Connexion à distance. Cependant, contrairement à l'option 1, vous pouvez créer une liste de réplication sur le site d'origine. Utilisez uniquement les objets en conflit et créez un travail de réplication qui utilisera cette liste de réplication ciblée.
   Pour conserver les modifications du site d'origine, définissez la résolution automatique de conflit sur « Le site d'origine est prioritaire ».
   Pour conserver les modifications du site de destination, définissez la résolution automatique de conflit sur « Le site de destination est prioritaire » et le type de réplication sur « Réplication bidirectionnelle ».
3. Pour les travaux de réplication unidirectionnelle, vous pouvez simplement supprimer l'objet sur le site de destination. A la prochaine exécution du travail de réplication, l'objet est répliqué à partir du site d'origine sur le site de destination.

   > ⓘ Remarque
   >
   > Faites attention lorsque vous supprimez un objet car les autres objets qui en dépendent peuvent également être supprimés, cesser de fonctionner ou ne plus être sécurisés. Les options 1 et 2 sont recommandées.

27.11.2 Résolution des conflits de réplication bidirectionnelle

Dans un conflit de réplication bidirectionnelle, vous avez le choix entre trois possibilités pour la détection de conflit :

- Le site d'origine est prioritaire
- Le site de destination est prioritaire
- Pas de résolution automatique de conflit

Le site d'origine est prioritaire

Si un conflit se produit, le site d'origine est prioritaire et toutes les modifications du site de destination sont remplacées par celles du site d'origine.

Exemple

Lily modifie le nom d'un rapport en rapport A. Malik modifie le nom de la version répliquée sur le site de destination en rapport B. Après l'exécution du travail de réplication suivant, la version répliquée sur le site de destination redeviendra rapport A.

Aucun conflit ne sera généré dans le fichier journal et cela ne figurera pas dans la liste des objets en conflit, car le conflit a été résolu selon les instructions de l'utilisateur sur le site d'origine.

Le site de destination est prioritaire

Si un conflit se produit, le site de destination conserve ses modifications et les applique sur le site d'origine.

Exemple

Kamal modifie le nom d'un rapport en rapport A. Peter modifie le nom de la version répliquée sur le site de destination en rapport B. A l'exécution du travail de réplication, un conflit est détecté. Le nom du rapport sur le site de destination demeure rapport B.

Dans les réplications bidirectionnelles, les modifications sont retransmises au site d'origine. Dans ce scénario, le site d'origine est mis à jour et son nom de rapport est modifié en rapport B. Aucun conflit n'est généré dans le fichier journal et cela ne figure pas non plus dans la liste des objets en conflit car le conflit a été résolu selon les instructions de l'utilisateur.

Pas de résolution automatique de conflit

Si l'option « Pas de résolution automatique de conflit » est sélectionnée, aucun conflit ne sera résolu. Il sera consigné dans un fichier journal destiné à l'administrateur, lequel pourra le résoudre manuellement.

> ⓘ Remarque
>
> L'icône d'un objet comporte un indicateur pour signaler qu'il existe un conflit.

> ⓘ Remarque
>
> Bien que les modifications soient répercutées à la fois sur le site d'origine et le site de destination dans les réplications bidirectionnelles, seules les versions du site de destination comporteront une icône de conflit.

> **Remarque**
>
> Tout utilisateur disposant d'un accès à la CMC et aux instances de travaux de réplication peut accéder au journal XML enregistré dans le répertoire des fichiers journaux. Une icône d'un objet du site de destination possède un indicateur pour signaler le conflit. Lors du traitement, un journal de conflit est créé.

L'administrateur peut accéder à une liste de tous les objets répliqués en conflit dans la zone Fédération de la CMC. Les objets en conflit sont regroupés selon la connexion à distance qu'ils utilisent avec le site d'origine.

Pour accéder à ces listes, sélectionnez *CMC* > *Fédération* > *Erreurs de réplication* > *Connexion à distance*.

> **Remarque**
>
> La liste est mise à jour lorsqu'un travail de réplication utilisant une connexion à distance est terminé. Elle contient tous les objets en conflit pour tous les travaux de réplication utilisant sa connexion à distance. Tous les objets répliqués sur un site de destination seront marqués par une icône de réplication. En cas de conflit, les objets seront marqués par une icône de conflit.

Exemple

Michael modifie le rapport A sur le site d'origine. Damien modifie la version répliquée sur le site de destination. La prochaine fois que le travail de réplication sera exécuté, un conflit se produira, car le rapport a été modifié à la fois sur le site d'origine et sur le site de destination ; ce conflit ne sera pas résolu.

Le rapport du site de destination est conservé et les modifications apportées au rapport du site d'origine ne sont pas répliquées. Les travaux de réplication suivants se comporteront de la même manière jusqu'à ce que le conflit soit résolu. Les modifications effectuées sur le site d'origine ne seront pas répliquées tant que le conflit ne sera pas résolu manuellement par l'administrateur ou l'administrateur délégué.

> **Remarque**
>
> Dans ce cas, c'est la totalité de l'objet qui n'est pas répliqué. Aucune autre modification, même si elle ne crée aucun conflit, n'est répliquée.

> **Remarque**
>
> Tout utilisateur disposant d'un accès à la CMC et aux instances de travaux de réplication peut accéder au journal XML enregistré dans le répertoire des fichiers journaux. Une icône d'un objet du site de destination possède un indicateur pour signaler le conflit. Lors du traitement, un journal de conflit est créé.

L'administrateur peut accéder à une liste de tous les objets répliqués en conflit dans la zone Fédération de la CMC. Les objets en conflit sont regroupés selon la connexion à distance qu'ils utilisent avec le site d'origine.

Pour accéder à ces listes, sélectionnez *CMC* > *Fédération* > *Erreurs de réplication* > *Connexion à distance*.

> **Remarque**
>
> La liste est mise à jour lorsqu'un travail de réplication utilisant une connexion à distance est terminé. Elle contient tous les objets en conflit pour tous les travaux de réplication utilisant sa connexion à distance. Tous les objets répliqués sur un site de destination seront marqués par une icône de réplication. En cas de conflit, les objets seront marqués par une icône de conflit.

Pour résoudre manuellement un conflit, vous avez le choix entre trois possibilités :

1. Créez un travail de réplication qui réplique uniquement les objets en conflit. Il doit utiliser le même objet Connexion à distance et la même liste de réplication.
   Pour conserver les modifications du site d'origine, créez un travail de réplication. Définissez ensuite le mode de réplication sur « Actualiser à partir du site d'origine » et la résolution automatique de conflit sur « Le site d'origine est prioritaire ».
   Pour conserver les modifications du site de destination, créez un travail de réplication et définissez le type de réplication sur « Réplication bidirectionnelle », le mode de réplication sur « Actualiser à partir de la destination » et la résolution automatique de conflit sur « Le site de destination est prioritaire ».

   > **Remarque**
   >
   > En mode de réplication, définissez « Actualiser à partir du site d'origine » ou « Actualiser à partir de la destination » pour sélectionner uniquement les objets en conflit dans la liste de réplication. De cette façon, les autres objets ne seront pas répliqués. Ensuite, planifiez le travail de réplication à exécuter afin de répliquer les objets sélectionnés et de résoudre le conflit comme indiqué.

2. Créez un travail de réplication qui réplique uniquement les objets en conflit. Il devra utiliser le même objet Connexion à distance. Cependant, contrairement à l'option 1, vous pouvez créer une liste de réplication sur le site d'origine. Utilisez uniquement les objets en conflit et créez un travail de réplication qui utilisera cette liste de réplication ciblée.
   Pour conserver les modifications du site d'origine, définissez la résolution automatique de conflit sur : « Le site d'origine est prioritaire ».
   Pour conserver les modifications du site de destination , définissez la résolution automatique de conflit sur : « Le site de destination est prioritaire » et le type de réplication : « Réplication bidirectionnelle »
3. Supprimez l'objet sur le site souhaité.

> **Remarque**
>
> Faites attention lorsque vous supprimez un objet car les autres objets qui en dépendent peuvent également être supprimés, cesser de fonctionner ou ne plus être sécurisés. Les options 1 et 2 sont recommandées.

Pour conserver les modifications effectuées sur le site de destination, vous pouvez supprimer l'objet sur le site d'origine. A la prochaine exécution du travail de réplication, l'objet est répliqué à partir du site de destination sur le site d'origine.

> **Remarque**
>
> Faites attention lorsque vous supprimez une copie du site d'origine car d'autres sites de destination répliquant cet objet peuvent exécuter leur travail de réplication avant que la copie n'ait été répliquée sur l'autre site. Cela entraînerait la suppression de la copie sur les autres sites de destination ainsi que son indisponibilité tant que la copie n'aura pas été renvoyée.

Pour conserver les modifications du site d'origine, vous pouvez supprimer l'objet sur le site de destination.

27.12 Utilisation des services Web dans Fédération

Fédération utilise les services Web pour transférer des objets et leurs modifications entre le site d'origine et les sites de destination. Les services Web spécifiques à Fédération sont automatiquement installés et déployés

dans votre installation de la plateforme de BI. Cependant, vous souhaiterez peut-être modifier des propriétés ou personnaliser des déploiements dans les services Web afin d'améliorer les fonctionnalités, comme décrit dans cette section.

> → Conseil
>
> Afin d'améliorer la gestion des fichiers ainsi que les fonctionnalités, activez la mise en cache des fichiers dans Fédération.

27.12.1 Variables de session

Si vous transférez de nombreux fichiers de contenu dans un même travail de réplication, vous souhaiterez peut-être augmenter le délai d'expiration de la session des services Web Fédération.

La propriété se trouve dans le fichier `dsws.properties` :

```
<Répertoire d'installation du serveur d'applications>\dswsbobje\Web-INF\classes
```

Par exemple :

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes
```

Pour activer une variable de session, saisissez :

```
session.timeout = x
```

Où « x »représente le délai souhaité ; « x » est mesuré en secondes. Si aucune valeur n'est spécifiée, la valeur par défaut est 1 200 secondes, soit 20 minutes.

Les nouvelles propriétés s'appliquent uniquement lorsque l'application Web modifiée est redéployée sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

27.12.2 Mise en cache des fichiers

La mise en cache des fichiers permet aux services Web de gérer des pièces jointes très volumineuses sans avoir à les placer dans une mémoire tampon. Si elle n'est pas activée lors des transferts de taille volumineuse, toute la mémoire de la JVM peut être utilisée et la réplication peut échouer.

> ⓘ Remarque
>
> La mise en cache des fichiers diminue les performances lorsque les services Web effectuent le traitement dans les fichiers et non dans la mémoire. Vous pouvez utiliser une combinaison des deux options et envoyer les transferts volumineux vers un fichier et les plus petits dans la mémoire.

Pour activer la mise en cache des fichiers, modifiez le fichier `Axis2.xml` qui se trouve à l'emplacement suivant :

```
<Répertoire d'installation du serveur d'applications>\dswsbobje\Web-Inf\conf
```

Par exemple :

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
```

Saisissez les informations suivantes :

```
<parameter name="cacheAttachments" locked="false">true</parameter>
```

```
<parameter name="attachmentDIR" locked="false">temp directory</parameter>
```

```
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> **Remarque**
>
> La taille du seuil est mesurée en octets.

Les nouvelles propriétés s'appliquent uniquement lorsque l'application Web modifiée est redéployée sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

27.12.3 Déploiement personnalisé

Les services Web de Fédération peuvent être déployés automatiquement et les services « federation », « biplatform » et « session » doivent être activés. Pour désactiver Fédération, ou tout autre service Web, modifiez le fichier `service.xml` des services Web correspondants.

Les services Web de la plateforme de BI se trouvent dans :

```
<Répertoire d'installation du serveur d'applications>\dswsbobje\WEB-INF\services
```

Exemple :

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\services
```

Pour désactiver les services Web :

- Ajoutez la propriété « activate » à la balise du nom de service dans le fichier `service.xml` et définissez-la sur false.
- Redémarrez votre serveur d'applications Java.

Par exemple, pour désactiver Fédération :

Le fichier `services.xml` est à l'emplacement suivant :

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Changez le nom du service de :

```
<service name="Federator">
```

en :

```
<service name="Federator" activate="false">
```

Les nouvelles propriétés s'appliquent uniquement lorsque l'application Web modifiée est redéployée sur l'ordinateur exécutant le serveur d'applications Web. Utilisez WDeploy pour redéployer le fichier WAR sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

27.13 Planification à distance et instances exécutées localement

Cette section décrit la planification à distance, les instances exécutées localement et le partage d'instances. Ces fonctionnalités permettent d'exécuter les rapports à l'endroit où résident les données et d'envoyer les instances finalisées vers les emplacements appropriés.

27.13.1 Planification à distance

Fédération permet de planifier un rapport sur le site de destination, puis de le traiter sur le site d'origine. L'instance finalisée est ensuite renvoyée vers le site de destination.

Pour activer la planification à distance, planifiez un rapport de type normal et activez l'option « Exécuter sur le site d'origine ». Pour activer cette option, cliquez sur *Planifier* > *Groupe de serveurs de planification* > *Exécuter sur le site d'origine*. Une fois que les instances planifiées ont été créées, elles prennent le statut En suspens.

Lors de la planification à distance, les informations envoyées au site de destination sont ignorées et l'instance du rapport conserve le statut En suspens.

Lorsque le travail de réplication suivant qui gère le rapport est activé pour la planification à distance, il copie l'instance sur le site d'origine afin qu'elle y soit traitée. L'instance conserve le statut En suspens jusqu'à ce qu'elle soit traitée par le planificateur. Pendant ce temps, le travail de réplication ayant copié l'instance sur le site d'origine renvoie les éventuels objets modifiés et instances finalisées précédemment.

Un fois l'instance traitée sur le site d'origine, le statut finalisé lui est affecté. Lorsque le travail de réplication suivant gérant le rapport est activé pour la planification à distance, il utilise l'instance finalisée pour mettre à jour la copie sur le site de destination. Une fois mise à jour, l'instance du site de destination est finalisée.

> **Remarque**
>
> Un travail de réplication doit être exécuté pour renvoyer une instance finalisée.

Exemple

1. Tom planifie un rapport A pour la planification à distance.
2. L'instance de rapport A est créée sur le site de destination et le statut En suspens lui est affecté.

3. Le travail de réplication A s'exécute. Tout d'abord, il réplique les modifications à partir du site d'origine vers le site de destination (notamment les instances finalisées précédemment). Il copie ensuite l'instance en suspens sur le site d'origine, ainsi que les modifications devant être répliquées à partir du site de destination vers le site d'origine.
4. Sur le site d'origine, le planificateur envoie l'instance en suspens vers le Job Server approprié pour qu'elle y soit traitée. L'instance est ensuite traitée et prend le statut finalisé sur le site d'origine.
5. Le travail de réplication A s'exécute à nouveau. Lorsqu'il réplique le contenu à partir du site d'origine vers le site de destination, l'instance finalisée du rapport A est recueillie et les modifications sont appliquées à la version du site de destination.
6. Une fois cette tâche effectuée, la version du site de destination est complète.

La planification à distance fonctionne uniquement avec un travail de réplication bidirectionnel. Vous devez activer l'option « Répliquer les planifications distantes ». Cette option se trouve sur la page « Propriétés du travail de réplication » dans la zone *Filtres de réplication*. Dans certains cas, il se peut que vous souhaitiez répliquer les travaux planifiés à distance plus fréquemment que d'autres objets de votre liste de réplication. Pour ce faire, créez deux travaux de réplication. Activez le premier à l'aide de l'option « Répliquer les planifications distantes » pour un travail de réplication uniquement axé sur la planification à distance. Activez le second à l'aide de l'option « Répliquer les modèles de documents » ou « Répliquer tous les objets (pas de filtre) ».

> **Remarque**
>
> Lorsque vous activez la planification à distance, les instances finalisées et celles ayant échoué apparaissent à la fois sur le site de destination et sur le site d'origine.
>
> Si un utilisateur d'un site de destination, inexistant sur le site d'origine, exécute une planification à distance d'un rapport, l'instance du site d'origine échouera. Le propriétaire de l'instance ayant échoué sera le compte utilisateur de l'objet Connexion à distance utilisé pour se connecter au site d'origine.
>
> Bien qu'un travail de réplication puisse être configuré pour la planification à distance uniquement, il réplique toujours les objets des ascendants de l'instance du rapport. Ce qui signifie que si des modifications sont apportées entre des réplications, il réplique le rapport réel, le dossier de rapports réels, etc. Si vous ne souhaitez pas que les modifications du site de destination soient répliquées sur le site d'origine, vous pouvez utiliser des droits de sécurité pour piloter le choix des modifications à répliquer.

Informations associées

Gestion des droits de sécurité [page 983]

27.13.2 Instances exécutées localement

Les instances exécutées localement sont des instances d'un rapport qui sont traitées à partir de rapports du site de destination. Fédération permet de répliquer les instances finalisées du site de destination vers le site d'origine.

Pour permettre à un travail de réplication d'effectuer la réplication des instances finalisées et ayant échoué du site de destination vers le site d'origine, cliquez sur *Propriétés du travail de réplication* > *Filtres de réplication* > *Répliquer les instances finalisées exécutées localement*.

Dans certains cas, vous souhaiterez peut-être qu'un travail de réplication réplique uniquement les instances exécutées localement. Pour ce faire, activez l'option « Répliquer les instances finalisées exécutées localement ».

> **Remarque**
>
> Lorsque vous activez les instances exécutées localement dans un travail de réplication, les instances finalisées et ayant échoué sont répliquées sur le site d'origine. Cela signifie que des copies se trouveront à la fois sur le site d'origine et sur le site de destination.
>
> Les instances en suspens ne sont jamais répliquées.
>
> Si le propriétaire d'une instance exécutée localement n'existe pas sur le site d'origine, le propriétaire est le compte utilisateur utilisé pour se connecter à l'objet Connexion à distance.

27.13.3 Partage d'instances

Lorsque vous activez la planification à distance et les instances exécutées localement dans un travail de réplication, un partage d'instances peut se produire si un site d'origine et plusieurs sites de destination répliquent le même rapport.

Exemple

Le rapport A provient du site d'origine, tandis que les sites de destination A et B en créent des réplications. Le partage d'instances s'effectue sur les deux sites de destination :

- Travaux de réplication activés avec « Répliquer les planifications distantes » et/ou « Répliquer les instances finalisées exécutées localement ». Répliquez le rapport A avec le même travail de réplication que ci-dessus.
- Planifiez le rapport A sur le site de destination pour l'« exécuter sur le site d'origine » et/ou l'exécuter localement

Si les deux sites de destination A et B répliquent le rapport A et que les travaux de réplication correspondants répliquent des planifications à distance et/ou répliquent des instances localement, alors toute instance traitée sur le site de destination A et/ou sur le site d'origine à la place du site de destination A sera partagée avec le site de destination B.

De même, toute instance traitée sur le site de destination B et/ou sur le site d'origine sera également partagée avec le site de destination A. Enfin, le site d'origine et les sites de destination A et B possèderont un ensemble d'instances identique.

Le partage d'instances est idéal dans de nombreuses situations. Par exemple, lorsque les utilisateurs d'autres sites ont besoin d'accéder à des informations provenant de déploiements apparentés. Dans ce cas, veillez à ce que les droits de sécurité soient définis de manière appropriée afin que les instances ne puissent pas être visualisées par les utilisateurs du site local. Par exemple, dans un objet rapport, appliquez les droits de façon à ce que les utilisateurs ne puissent afficher que les instances dont ils sont propriétaires.

> **Remarque**
>
> Tous les objets sont régis par les règles de sécurité de la plateforme de BI. Afin que les utilisateurs et les groupes ne puissent visualiser que les instances applicables, il est recommandé de définir les droits de sorte qu'ils ne puissent afficher que les instances dont ils sont propriétaires. Par exemple, dans un objet rapport, appliquez les droits de façon à ce que les utilisateurs ne puissent afficher que les instances dont ils sont propriétaires.

Informations associées

Gestion des droits de sécurité [page 983]

27.14 Importation et promotion de contenu répliqué

Dans certains cas, vous pouvez choisir d'importer ou de promouvoir du contenu répliqué d'un système de la plateforme de BI vers un autre. Cette section est consacrée à ces fonctionnalités dans Fédération.

> **Remarque**
>
> Les migrations d'objet sont mieux exécutées par des membres du groupe d'administrateurs, en particulier du groupe d'utilisateurs Administrateur. Pour migrer un objet, il se peut qu'un grand nombre d'objets liés doivent également être migrés. Dans le cas d'un compte administrateur délégué, il ne sera peut-être pas possible d'obtenir les droits de sécurité requis pour l'ensemble des objets.

27.14.1 Importation de contenu répliqué

Si vous utilisez LifeCycle Manager pour importer le contenu d'un déploiement de la plateforme de BI vers un autre, LifeCycle Manager n'importera aucune information spécifique sur la réplication associée aux objets répliqués en cours d'importation. Cela signifie qu'après l'importation, l'objet agira comme s'il n'avait jamais été répliqué. Ce comportement est spécifique aux objets répliqués sur un site de destination et est décrit dans le scénario suivant.

Exemple

La plateforme de BI A est un site de destination dans un processus Fédération. Le rapport A, rapport répliqué sur le système A, est importé du système A vers la plateforme de BI B à l'aide de LifeCycle Manager.

Résultat : lorsque le rapport A est copié sur la plateforme de BI B, il ne contient aucune information répliquée. Le rapport A ne comportera plus d'icône de réplication. Si l'objet était en conflit sur la plateforme de BI A, il ne le sera plus sur la B. Il est en fait traité comme un objet issu du système B.

> **Remarque**
>
> Le CUID peut être identique ou différent selon les choix d'importation que vous avez sélectionnés dans LifeCycle Manager.

27.14.2 Importation de contenu répliqué et réplication continue

Après l'importation du contenu répliqué, vous souhaiterez peut-être inclure les objets importés dans un processus Fédération. Deux scénarios sont possibles : utiliser le système sur lequel les objets importés résident comme site d'origine, ou utiliser le système comme site de destination. Pour utiliser ce système comme site d'origine, continuez la procédure habituelle dans Fédération.

Pour utiliser le système comme site de destination et répliquer les objets importés à partir du site d'origine, vous devez :

- Vous assurer que le CUID des objets est conservé lors de l'utilisation de LifeCycle Manager.
- Vous assurer que la résolution du conflit du premier travail de réplication est définie sur « Le site d'origine l'emporte » ou sur « Le site de destination l'emporte ».

> **→ Conseil**
>
> Au lieu d'importer l'objet à l'aide de LifeCycle Manager d'un site de destination vers un autre, il est plus efficace et vivement recommandé d'utiliser Fédération uniquement pour répliquer l'objet.

Exemple

Le rapport A a été créé sur le système de la plateforme de BI A. Le système X a utilisé Fédération pour répliquer le rapport A du système A vers le système X. LifeCycle Manager a ensuite importé le rapport A du système X vers le système Y.

Plan : le système Y souhaite configurer Fédération sur le système A et conserver le rapport A en tant que partie de la réplication. Le système Y est le système de destination et le système A est le système d'origine.

Action : lors de l'importation du rapport A à partir du système X vers le système Y, le CUID du rapport A doit être conservé. De plus, lorsque le premier travail de réplication s'exécute, il essaiera de répliquer le rapport A. Etant donné que l'objet existe déjà sur le système Y, la réplication générera un conflit. Pour préciser quelle version utiliser, vous devez définir le mode de résolution de conflit sur « Site d'origine » ou sur « Site de destination ».

> **Remarque**
>
> Dans cet exemple, il est recommandé au lieu d'importer l'objet à l'aide de LifeCycle Manager d'un site de destination vers un autre de n'utiliser Fédération que pour répliquer l'objet. Le rapport A effectuera les réplications du système A vers le système Y, et il est inutile d'utiliser LifeCycle Manager pour effectuer les importations du système X vers le système Y.

27.14.3 Promotion de contenu à partir d'un environnement de test

Dans n'importe quelle organisation, des tests sont souvent réalisés avant de placer un élément dans un environnement de production. Il semble donc normal de tester Fédération entre plusieurs systèmes de la plateforme de BI dans un environnement de développement ou de test avant de configurer Fédération sur vos ordinateurs de production. Une fois que vous avez créé votre site d'origine et vos sites de destination ainsi que le contenu dans un environnement de test, vous pouvez promouvoir cette configuration sur vos ordinateurs de production à l'aide de la procédure suivante :

1. Utilisez LifeCycle Manager pour promouvoir votre contenu du site d'origine de l'environnement de test sur l'ordinateur de production qui agira en tant que site d'origine.

   > ⓘ Remarque
   >
   > Il est impossible de sélectionner l'objet Liste de réplication lors de l'utilisation de LifeCycle Manager.

2. Créez la liste de réplication sur le site d'origine dans l'environnement de production et ajoutez le contenu souhaité.
3. Choisissez l'une des deux options suivantes :
   - A) Créez un objet Connexion à distance avec les travaux de réplication appropriés sur les ordinateurs de production qui agiront en tant que sites de destination.
   - B) Utilisez LifeCycle Manager pour importer la connexion à distance et les travaux de réplication à partir du site de destination des environnements de développement et de contrôle qualité sur les ordinateurs de production qui agiront en tant que sites de destination. Modifiez ensuite les connexions à distance importées afin qu'elles pointent vers l'ordinateur de production qui agira en tant que site d'origine.

27.14.4 Redirection d'un site de destination

Actuellement, après réplication d'un objet à partir de son site d'origine, il doit toujours être répliqué à partir de ce site d'origine et ne peut pas l'être à partir d'une autre plateforme de BI si l'objet Connexion à distance est modifié pour pointer vers un nouveau système, toute tentative de réplication d'un objet répliqué à partir d'un système de la plateforme de BI différent de celui de l'objet Connexion à distance échouera. Pour répliquer un objet à partir d'un autre site d'origine, supprimez-le d'abord du site de destination.

> ⓘ Remarque
>
> Une fois que vous avez copié un objet répliqué, le CUID de la copie est modifié et la copie ne contiendra aucune information répliquée.

27.15 Meilleures pratiques

La Fédération permet d'optimiser les performances d'un travail de réplication.

Si un seul travail de réplication contient un grand nombre d'objets, vous pouvez effectuer des étapes supplémentaires pour garantir la réussite de son exécution. En règle générale, vous devriez pouvoir répliquer jusqu'à 32 000 objets dans chaque travail de réplication. Cependant, certains déploiements peuvent requérir des configurations incluant des tailles de réplication inférieures ou supérieures.

1) Obtenir un fournisseur de services Web dédié

Dans Fédération, le contenu répliqué est envoyé via les services Web. Dans une installation par défaut de la plateforme de BI, tous les services Web utilisent le même fournisseur de services Web. Les travaux de réplication de grande taille peuvent utiliser le fournisseur de services Web plus longtemps et ralentir ses réponses aux autres requêtes de services Web, ainsi que toutes les applications qu'il sert.

Si vous prévoyez de répliquer un grand nombre d'objets en une seule fois ou d'exécuter plusieurs travaux de réplication les uns après les autres, vous pouvez envisager de déployer les services Web Fédération sur leur propre serveur d'applications Java à l'aide de votre propre fournisseur de services Web.

Pour ce faire, utilisez la plateforme de BI pour installer les services Web. Vous devez disposer d'un serveur d'applications Java en cours d'exécution. Si ce n'est pas le cas, choisissez l'option complète Composants de niveau Web, qui installe les services Web, ainsi que Tomcat.

> **Remarque**
>
> Vous devez fournir des informations sur un CSM existant (par exemple, le nom d'hôte, le port et le mot de passe administrateur).

> **Remarque**
>
> Vous devrez utiliser l'URI de ce nouveau fournisseur de services Web dans le champ URI de votre connexion à distance.

2) Augmenter la mémoire disponible du serveur d'applications Java

Augmentez la mémoire disponible de votre serveur d'applications Java si votre unique travail de réplication réplique de nombreux objets ou si vous partagez le serveur d'applications avec d'autres applications.

Si vous avez déployé la plateforme de BI et Tomcat, la mémoire disponible par défaut est de 1 Go. Pour augmenter la mémoire disponible pour Tomcat :

Sous Windows :

1. Cliquez sur *Démarrer* > *Programmes* > *Tomcat* > *Configuration Tomcat*.
2. Sélectionnez *Java*.
3. Dans la zone *Options Java*, recherchez `-Xmx1024M`
4. Augmentez la valeur `-Xmx1024M` pour définir la taille voulue.

Exemple

Pour augmenter la mémoire à 2 Go, saisissez la valeur suivante : `-Xmx2048M`

Sous Unix :

1. Dans le répertoire `<Rep_Install_BOE>/setup/`, ouvrez le fichier `env.sh` dans votre éditeur de texte préféré. Augmentez la valeur du paramètre `-Xmx1024m` pour définir la taille voulue.

2. Recherchez les lignes suivantes :

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

> **Remarque**
>
> Dans BI 4.2 Support Package 5, vous pouvez utiliser le paramètre MaxMetaspaceSize pour définir la taille de la mémoire du méta-espace, ce qui n'est pas le cas du paramètre MaxPermSize.
>
> - Si vous procédez à la mise à niveau à partir de versions antérieures à BI 4.2 Support Package 5 vers BI 4.2 Support Package 5, vous devez modifier manuellement le paramètre pour tous les serveurs existants.
> - Si vous procédez à une nouvelle installation de BI 4.2 Support Package 5, le paramètre est remplacé par défaut.

3. Augmentez la valeur du paramètre `-Xmx1024m` pour définir la taille voulue.

Exemple

Pour augmenter la mémoire à 2 Go, saisissez la valeur suivante : `-Xmx2048m`

> **→ Conseil**
>
> Pour les autres serveurs d'applications Java, reportez-vous à la documentation du serveur pour augmenter la mémoire disponible.

3) Réduire la taille des fichiers BIAR créés

Fédération utilise les services Web pour répliquer le contenu entre le site d'origine et le site de destination. Les objets sont regroupés et compressés dans des fichiers BIAR pour permettre un transfert plus efficace.

Lorsque vous répliquez un grand nombre d'objets, configurez votre serveur d'applications Java pour créer des fichiers BIAR de plus petite taille. Fédération va regrouper et compresser les objets dans plusieurs fichiers BIAR de plus petite taille, si bien que le nombre d'objets à répliquer ne sera pas limité.

Pour réduire la taille des fichiers BIAR créés, ajoutez les paramètres Java suivants à votre serveur d'applications Java :

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

`bobj.biar.suggestSplit` suggère une taille de fichier BIAR appropriée, qu'il va essayer de respecter. La nouvelle valeur suggérée est 90 Mo.

`bobj.biar.forceSplit` va forcer un fichier BIAR à s'arrêter à une taille donnée. La nouvelle valeur suggérée est 100 Mo.

> **Remarque**
>
> Vous ne devez modifier les paramètres de taille des fichiers BIAR par défaut que si la mémoire de votre serveur d'applications est saturée et que vous ne pouvez plus augmenter la taille maximale des segments de mémoire.

Pour Tomcat sous Windows :

1. Pour ouvrir l'outil *Configuration Tomcat*, cliquez sur *Démarrer* > *Programmes* > *Tomcat* > *Configuration Tomcat* >.
2. Sélectionnez *Java*.
3. Dans la zone *Options Java*, ajoutez les lignes suivantes à la fin :

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

Pour Tomcat sous Unix/Linux :

1. Ouvrez le fichier env.sh dans votre éditeur de texte préféré. Il se trouve dans le répertoire `<Rep_Install_BOE>/setup/`
2. Recherchez les lignes suivantes :

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Ajoutez les paramètres de taille des fichiers BIAR voulus.

Par exemple : `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

Pour les autres serveurs d'applications Java, consultez la documentation du serveur pour ajouter des propriétés système Java.

4) Augmenter le délai d'attente du socket

Le serveur Adaptative Job Server est responsable de l'exécution du travail de réplication. Pendant l'exécution du travail de réplication, le serveur Adaptative Job Server établit une connexion avec le site d'origine. Lors de la réception de gros volumes d'informations en provenance du site d'origine, il est important que le délai d'attente du socket que le serveur Adaptative Job Server utilise pour recevoir les informations n'expire pas.

La valeur par défaut est 90 minutes. Vous pouvez augmenter le délai du socket si besoin.

Pour augmenter le délai d'attente du socket sur le serveur Adaptative Job Server :

1. Ouvrez la Central Management Console (CMC).
2. Naviguez jusqu'à la section *Serveur* et sélectionnez *Adaptative Job Server*.
3. Cliquez sur *Propriétés*.

4. Ajoutez les « paramètres de ligne de commande » à la fin de la ligne suivante :
   - **Windows :** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<délai d'attente en minutes>`
   - **UNIX :** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<délai d'attente en minutes>`

Informations associées

Dépannage des messages d'erreur [page 1023]
Utilisation des services Web dans Fédération [page 1010]
Limites de la version actuelle [page 1022]

27.15.1 Limites de la version actuelle

Fédération est un outil flexible ; certaines limitations peuvent cependant affecter ses performances en production. Cette section présente les points que vous pouvez modifier pour optimiser le fonctionnement de Fédération.

- Nombre maximal d'objets
  Chaque travail de réplication réplique des objets entre plusieurs déploiements de la plateforme de BI. Le nombre maximal recommandé d'objets à répliquer dans un seul travail de réplication est 100 000. Bien qu'un travail de réplication puisse fonctionner avec plus de 100 000 objets, Fédération prend uniquement en charge la réplication de 100 000 objets au maximum.
- Droits
  Dans Fédération, les droits sont uniquement répliqués du site d'origine vers le site de destination. Il est recommandé de définir les droits utilisateur communs aux deux déploiements sur le site d'origine et de les répliquer sur les sites de destination à l'aide d'une réplication bidirectionnelle. Les droits de l'utilisateur d'un site spécifique seront gérés comme habituellement dans un déploiement de la plateforme de BI sur le site où réside l'utilisateur.
- Vues d'entreprise et objets associés
  La plateforme de BI peut stocker des vues d'entreprise, des éléments d'entreprise, des fondations de données, des connexions de données et des listes de valeurs. Ces objets permettent d'améliorer les fonctionnalités de Crystal Reports.
  Si ces objets sont d'abord créés sur le site de destination, puis répliqués sur le site d'origine à l'aide d'une réplication bidirectionnelle, ils risquent de ne pas fonctionner correctement et leurs données risquent de ne pas apparaître dans Crystal Reports.
  Il est recommandé de créer les vues d'entreprise, éléments d'entreprise, fondations de données, connexions de données et listes de valeurs sur le site d'origine, puis de les répliquer sur le site de destination. Effectuez les mises à jour de ces objets sur le site de destination ou sur le site d'origine (en fonction des droits) et les modifications seront correctement répliquées.
- Surcharges d'univers
  La plateforme de BI peut stocker des surcharges d'univers. Si les surcharges d'univers sont créées sur le site de destination, puis répliquées sur le site d'origine à l'aide d'une réplication bidirectionnelle, elles risquent de ne pas fonctionner correctement.

Pour résoudre ce problème, créez d'abord les surcharges d'univers sur le site d'origine, puis répliquez-les sur le site de destination. Ensuite, définissez des paramètres de sécurité sur les surcharges d'univers sur le site d'origine, puis répliquez-les sur le site de destination.

- Nettoyage des objets
  La fonction de nettoyage des objets supprime les objets qui ont été supprimés sur l'autre site. Le nettoyage des objets est actuellement uniquement effectué du site d'origine vers le site de destination.
- Fichiers journaux de Fédération
  Les fichiers journaux de Fédération sont écrits dans des fichiers XML utilisant les normes XML 1.1. Pour visualiser les fichiers journaux à l'aide d'un navigateur, ce dernier doit prendre en charge XML 1.1.

Informations associées

Gestion du nettoyage des objets [page 1003]

27.15.2 Dépannage des messages d'erreur

Cette section contient les messages d'erreur que vous pouvez rencontrer dans de rares circonstances lors de l'utilisation de Fédération. Ces messages s'afficheront dans les journaux des travaux de réplication ou dans la zone des fonctionnalités d'un rapport.

1) GUID non valide

Exemple d'erreur : `ERREUR 2008-01-10T00:31:08.234Z Le GUID ASXOOFyvy0FJnRcD0dZNTZg (trouvé dans la propriété SI_PARENT_CUID de l'objet numéro 1285) n'est pas un GUID valide`.

Cette erreur signifie que vous répliquez un objet dont le parent n'est pas répliqué simultanément et qui n'existe pas encore sur le site de destination. Par exemple, vous répliquez un objet, mais pas le dossier qui le contient. Il est possible que l'objet parent ne puisse pas être répliqué car le compte répliquant les objets ne dispose pas des droits suffisants sur cet objet parent.

2) Rapports Crystal ne présentant aucune donnée sur le site d'origine

Cette erreur peut se produire si le rapport Crystal utilise une vue d'entreprise, un élément d'entreprise, une fondation de données, une connexion de données ou une liste de valeurs initialement créés sur le site de destination, puis répliqués sur le site d'origine.

3) Les surcharges d'univers ne sont pas appliquées correctement

Cette erreur peut se produire si le rapport utilise un univers qui contient une surcharge d'univers créée sur le site de destination, puis répliquée sur le site d'origine.

4) Mémoire Java saturée

Exemple d'erreur : `java.lang.OutOfMemoryError`.

Cette erreur peut se produire si la mémoire de votre serveur d'applications Java est saturée lors du traitement d'un travail de réplication. Votre travail de réplication est peut-être trop gros ou votre serveur d'applications Java ne dispose pas de suffisamment de mémoire.

Augmentez la mémoire disponible de votre serveur d'applications Java en déplaçant les services Web Fédération vers un ordinateur dédié ou réduisez le nombre d'objets répliqués dans un travail de réplication.

5) Délai d'attente du socket

Exemple d'erreur : `Erreur de communication avec le site d'origine. Délai de lecture expiré.`

Les informations envoyées depuis le site d'origine au serveur Adaptative Job Server sur le site de destination dépassent le délai d'attente autorisé. Augmentez le délai d'attente du socket sur le serveur Adaptative Job Server ou réduisez le nombre d'objets répliqués dans votre travail de réplication.

6) Limite de requête

Exemple d'erreur : `Une erreur liée au SDK s'est produite sur le site de destination. La requête n'est pas valide. (FWB 00025) …...La chaîne de la requête dépasse la limite de longueur de requête.`

Cette erreur peut se produire si vous répliquez trop d'objets simultanément et que Fédération envoie une requête trop volumineuse pour que le CMS puisse la traiter. Les objets du site d'origine seront validés sur le site de destination. Cependant, les modifications devant être validées sur le site d'origine ne le seront pas. Les conflits sont résolus comme indiqué, cependant, aucun indicateur de conflit demandant une résolution manuelle ne sera défini sur l'objet. Les objets validés sur le site de destination continueront de fonctionner correctement.

Pour résoudre ce problème, réduisez le nombre d'objets répliqués dans un travail de réplication.

7) Expiration du travail de réplication

Exemple d'erreur : `Impossible de planifier l'objet avec l'intervalle d'heures spécifié`.

Vous pouvez recevoir ce message si votre travail de réplication a expiré alors qu'il attendait la fin d'un autre travail de réplication. Cela peut se produire si vous avez plusieurs travaux de réplication qui se connectent simultanément au même site d'origine. Une nouvelle exécution du travail de réplication ayant échoué va être tentée à l'heure planifiée suivante.

Pour résoudre ce problème, planifiez le travail de réplication ayant échoué à une heure où il ne sera pas en conflit avec d'autres travaux de réplication se connectant au même site d'origine.

8) Limite de réplication

Exemple d'erreur : `Une erreur liée au SDK s'est produite sur le site de destination. Erreur d'accès à la base de données. …. Erreur du processeur de requête interne : espace de pile du processeur de requête saturé lors de l'optimisation de la requête. Erreur lors de l'exécution de la requête dans ExecWithDeadlockHandling.`

Vous pouvez recevoir ce message si vous avez dépassé le nombre d'objets pris en charge pouvant être répliqués simultanément. Pour résoudre ce problème, réduisez le nombre d'objets répliqués dans votre travail de réplication et exécutez-le à nouveau.

9) Objet supprimé

Exemple d'erreur : `Erreur lors de la vérification des droits de sécurité` ou `Erreur lors de la compression de l'objet`.

Ce message peut s'afficher si un objet est supprimé du package de réplication. Cela peut se produire lorsque Fédération demande un objet nécessitant une réplication, mais avant la vérification des droits et la création du package de l'objet.

10) Adaptive Processing Server

Exemple d'erreur : `Une erreur s'est produite dans le Job Processing Server`.

Cette erreur peut se produire lorsque trop de classes sont chargées par Fédération et que la mémoire est insuffisante pour traiter le travail de réplication.

Pour résoudre ce problème, vous devez exécuter les deux étapes suivantes :

1. Dans les arguments de ligne de commande du serveur de traitement adaptatif, ajoutez la ligne suivante : `-javaArgs "XX:MaxMetaspaceSize=256m"`.

> **Remarque**
>
> Dans BI 4.2 Support Package 5, vous pouvez utiliser le paramètre MaxMetaspaceSize pour définir la taille de la mémoire du méta-espace, ce qui n'est pas le cas du paramètre MaxPermSize.
>
> - Si vous procédez à la mise à niveau à partir de versions antérieures à BI 4.2 Support Package 5 vers BI 4.2 Support Package 5, vous devez modifier manuellement le paramètre pour tous les serveurs existants.
> - Si vous procédez à une nouvelle installation de BI 4.2 Support Package 5, le paramètre est remplacé par défaut.

2. Ajoutez les paramètres suivants au serveur d'applications Java auquel vous vous connectez pour l'utilisation de Fédération afin de réduire la taille des fichiers BIAR que vous utilisez :
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

11) Installation des serveurs de traitement adaptatifs

Un nouvel argument Java `-XX:MetaspaceSize` a été ajouté à la ligne de commande APS en combinaison avec l'argument `-XX:MaxMetaspaceSize` existant pour améliorer l'expérience d'initialisation et éviter le Full Garbage Collection non souhaité dans le processus Java lié aux serveurs de traitement adaptatifs.

Le test sur une machine virtuelle avec des ressources RAM minimales, un APS par défaut et Tous les services, y compris ces valeurs pour MetaSpace et MaxMetaSpace, semble permettre à l'APS de se lancer et de s'initialiser un peu plus rapidement qu'avec les paramètres prêts à l'emploi. Aucun "Full GC" n'est signalé.

Pour en savoir plus sur les *options Java des serveurs de traitement adaptatifs pour éviter les Full GC (Full Garbage Collections) avec MetaSpace*, consultez la note SAP 3001317.

12) Espace du Gestionnaire d'objets

Exemple d'erreur : `Impossible de générer le package de publication. Exception d'entrée ou de sortie : "Plus d'espace sur le périphérique."`

Cela se produit lorsque le répertoire temporaire utilisé par Fédération ne dispose plus d'assez d'espace disque. Pour résoudre ce problème, créez un espace supplémentaire dans le répertoire temporaire ou utilisez un autre emplacement pour le répertoire temporaire.

Pour spécifier un autre emplacement pour le répertoire temporaire sur le site d'origine, ajoutez la ligne suivante aux fichiers de configuration du serveur d'applications Java : `-Dbobj.tmp.dir=<TempDir>`.

Pour spécifier un autre emplacement pour le répertoire temporaire sur le site de destination, ajoutez la ligne suivante aux arguments de la ligne de commande du serveur de traitement adaptatif : `-javaArgs « -Dbobj.tmp.dir=<TempDir> »`.

Dans les exemples ci-dessus, `<RépTemp>` représente l'emplacement du répertoire temporaire que vous souhaitez utiliser.

13) Erreur d'univers

Exemple d'erreur : `Une erreur interne s'est produite lors de l'appel de l'API processDPCommands`.

Cela se produit lorsque la relation de connexion Univers-à-Univers d'un univers répliqué n'est pas valide ou manquante. Pour résoudre ce problème, exécutez le travail de réplication en sélectionnant l'option *Actualiser à partir du site d'origine* et vérifiez que la connexion d'univers est répliquée.

Vous pouvez également ouvrir l'univers dans Universe Designer, modifier la connexion de l'univers et revalider l'univers.

Informations associées

Meilleures pratiques [page 1018]
Limites de la version actuelle [page 1022]

28 Configurations supplémentaires pour les environnements Enterprise Resource Planning

28.1 Configurations pour l'intégration SAP NetWeaver

28.1.1 Intégration avec SAP Business Warehouse (BW)

28.1.1.1 Présentation

Cette section explique comment configurer BW pour activer et gérer la publication des rapports à partir de l'application SAP Business Warehouse sur la plateforme de BI.

Avant de lire cette section, assurez-vous que vous avez terminé la configuration du plug-in d'authentification SAP dans la CMC.

Informations associées

Configuration de l'authentification SAP [page 342]

28.1.1.1.1 Configuration des dossiers et de la sécurité sur la plateforme de BI

Lorsque vous définissez un système d'autorisation sur la plateforme de BI, le système crée une structure de dossiers logique correspondant à votre système SAP. Lorsque vous importez des rôles et publiez du contenu sur la plateforme de BI, des dossiers correspondants sont créés. En tant qu'administrateur, vous n'avez pas à créer ces dossiers. Ils sont créés suite à la définition d'un système d'autorisation, lors de la configuration du plug-in d'authentification SAP en important des rôles dans la CMC et en publiant du contenu sur la plateforme de BI.

> **Remarque**
>
> Il incombe à l'administrateur de la plateforme de BI d'attribuer les droits d'accès appropriés à ces dossiers :
>
> - *Dossier SAP de niveau supérieur*
> Assurez-vous que le groupe Tout le monde a un accès limité au dossier SAP de niveau supérieur.
> - *Dossiers d'ID système*
> Affectez les droits suivants à l'éditeur principal dans la CMC :

> **Remarque**
>
> Le groupe Editeur principal n'est disponible qu'une fois le contenu publié.
>
> - Ajouter les objets au dossier
> - Visualiser les objets
> - Modifier les objets
> - Modifier les droits des utilisateurs sur les objets
> - Supprimer les objets

> **→ Conseil**
>
> Pour faciliter l'administration des droits, vous pouvez créer un niveau d'accès Editeur personnalisé qui inclut ces droits, puis accorder ce niveau d'accès à l'utilisateur ou groupe Editeur principal pour les dossiers d'ID système nécessaires.

Informations associées

Utilisation des niveaux d'accès [page 143]
Fonctionnement des droits sur la plateforme de BI [page 128]

28.1.1.1.2 Paramètres de sécurité par défaut des dossiers

Lors d'une publication de contenu sur la plateforme de BI à partir de SAP, la plateforme crée automatiquement le reste de la hiérarchie des rôles, des dossiers et des rapports. Le système organise vos rapports dans des dossiers nommés d'après l'ID système, le numéro du client et le nom du rôle :

- Le système crée les dossiers de niveau supérieur, c'est-à-dire les dossiers SAP, 2.0 et système (`<SID>`), lorsque vous définissez un système d'autorisation.
- Le système crée des dossiers de rôle (importés sous forme de groupes sur la plateforme de BI) en fonction des besoins, lorsqu'un rôle est publié à partir de BW.
- Le système crée un dossier Contenu pour chaque rôle dans lequel est publié du contenu.
- La sécurité étant définie pour chaque objet rapport, les utilisateurs peuvent avoir accès uniquement aux rapports appartenant à leur rôle.

L'administrateur est chargé d'assigner des droits aux membres des différents rôles. Le Workbench d'administration de contenu sert à gérer la fonctionnalité de publication de rapports à partir de SAP BW. Vous pouvez identifier des rôles du système SAP BW pour des systèmes particuliers de la plateforme de BI, publier des rapports et synchroniser des rapports entre SAP BW et un déploiement de la plateforme de BI.

Dossiers Contenu

La plateforme de BI importe un groupe pour chaque rôle défini dans la CMC et ajouté au système d'autorisation.

Afin que les droits par défaut appropriés soient affectés à tous les membres d'un rôle portant le contenu, vous devez attribuer les droits appropriés dans le Workbench d'administration de contenu pour chaque système d'autorisation défini sur la plateforme de BI. Pour lancer le Workbench d'administration de contenu, exécutez la transaction /CRYSTAL/RPTADMIN :

1. Dans le Workbench d'administration de contenu, développez *Système Enterprise*, puis *Systèmes disponibles*.
2. Cliquez deux fois sur le système souhaité.
3. Cliquez dans l'onglet *Présentation*.
4. Définissez *Système de sécurité par défaut pour rapports* sur *Visualiser*.
5. Définissez *Système de sécurité par défaut pour dossiers de rôles* sur *Visualiser à la demande*.
6. Cliquez sur *OK*.

Ces paramètres sont appliqués sur la plateforme de BI pour tous les rôles de contenu. Il s'agit des rôles pour lesquels du contenu est publié. Les membres de ces rôles peuvent à présent afficher les instances planifiées des rapports publiés dans d'autres rôles et actualiser les rapports publiés dans des rôles auxquels ils appartiennent.

> **Remarque**
>
> Nous vous recommandons fortement de distinguer les activités des rôles. Par exemple, alors qu'il est possible de réaliser une publication à partir du rôle d'un administrateur, il est préférable de publier uniquement à partir de rôles d'éditeurs. En outre, la fonction des rôles de publication consiste uniquement à définir les utilisateurs pouvant publier du contenu. Ainsi, les rôles de publication ne doivent pas contenir de contenu ; les éditeurs doivent publier vers des rôles portant le contenu qui sont accessibles aux membres de rôle standard.

28.1.1.1.3 Planification basée sur les événements BW

Vous pouvez maintenant planifier des objets basés sur des événements BW dans la plateforme de BI. Vous établissez un canaux de communication de confiance entre un système SAP NetWeaver Business Warehouse (BW) et la plateforme de BI pour activer la planification basée sur les événements BW.

28.1.1.1.3.1 Pour créer et configurer des événements BW

Suivez les étapes ci-dessous pour créer un événement BW :

1. Connectez-vous à la CMC.
2. Accédez à *Événements* > *Événements BW*.

3. Sélectionnez pour créer un nouvel événement.
4. Saisissez un *Nom d'événement* et une *Description*.
5. Sélectionnez *Créer*.
   Vous venez de créer un événement BW.

28.1.1.1.3.2 Pour ajouter des événements BW lors de la planification d'un rapport

Suivez les étapes ci-dessous pour ajouter un événement BW lorsque vous planifiez des rapports :

1. Dans la CMC, accédez à *Dossiers* et sélectionnez un rapport.
2. Dans le menu contextuel du rapport, sélectionnez *Planifier*.
3. Dans le panneau *Navigation*, accédez à *Événements* > *Événements BW*.
4. Sélectionnez un événement dans la section *Événements disponibles*.
5. Ajoutez-le aux événements en attente d'utilisation >>.
6. Dans le panneau *Navigation*, accédez à *Récurrence*.
7. Spécifiez les paramètres *Exécuter l'objet*, *Nombre de tentatives autorisées* et *Intervalle entre les tentatives exprimé en secondes*.
8. Sélectionnez *Planifier*.

   Une fois l'événement déclenché, le statut de planification du rapport passe de **En suspens** à **En cours d'exécution**.

   > **Remarque**
   >
   > Le statut de planification continue d'être défini sur **En suspens** si l'un des événements définis sous *Événements à attendre* n'est pas déclenché.

28.1.1.1.3.3 Pour intégrer la plateforme de BI et le système ABAP

Cette rubrique explique comment activer la planification basée sur les événements BW.

Suivez la procédure ci-dessous :

1. Configurez HTTPS/SSL pour tout serveur d'applications pris en charge dans la plateforme de BI et ajoutez la clé de secret partagé sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`. Voir la rubrique Pour configurer HTTPS/SSL [page 534] pour WACS et Configuration SSL dans Tomcat [page 416] pour Tomcat.

> **Remarque**
>
> Vous pouvez vous référer à la SAP Product Availability Matrix (PAM) pour plus d'informations sur les serveurs d'applications pris en charge.

2. Exportez le certificat de serveur de la plateforme de BI depuis un navigateur vers un système local. Vous pouvez télécharger les certificats depuis le navigateur Chrome en procédant comme suit.
1. Accédez à l'adresse http://<hostname>:<port_number>/biprws. Pour plus d'informations sur le numéro de port spécifique à chaque application, reportez-vous à la rubrique Pour configurer l'URL de base pour les services Web de type RESTful [page 547].
2. Ouvrez les outils développeur du navigateur Chrome en appuyant sur la touche F12.
3. Cliquez sur l'onglet *Security* (Sécurité) et sélectionnez *View Certificate* (Afficher le certificat).
   L'assistant `Certificate` (Certificat) s'affiche.
4. Dans l'assistant `Certificate` (Certificat), accédez à l'onglet *Details* (Détails) et sélectionnez *Copy to File* (Copier dans un fichier).
   L'assistant d'exportation de certificats *Certificate Export Wizard* s'affiche
5. Sélectionnez *Next* (Suivant).
6. À la page *Export File Format* (Format d'exportation du fichier), sélectionnez le format *Base-64 encoded X.509 (.CER)* (X.509 avec codage base 64 (.CER), puis cliquez sur *Next* (Suivant).
7. Attribuez un nom au fichier de certificat et enregistrez-le localement.
3. Téléchargez le certificat du système SAP NetWeaver BW.
1. Lancez SAP NetWeaver BW.
2. Accédez à la transaction *STRUSTSSO2*.
3. Sélectionnez ▶ *PSE système* ▶ *Sujet* ▶ *Propre certificat* ▶.
4. Sélectionnez *Télécharger*.
5. Spécifiez le chemin d'accès et définissez le format de fichier sur *Base64*.
6. Sélectionnez ✔.

Le certificat du système SAP NetWeaver BW est téléchargé à l'emplacement spécifié.

4. Importez le certificat de la plateforme de BI dans le système SAP NetWeaver BW.
1. Accédez à la transaction *STRUSTSSO2*.
2. Basculez vers le mode *Édition*.
3. Sélectionnez le dossier *Client SSL (standard)*.
4. Sélectionnez *Importer*.
5. Chargez le certificat du système SAP NetWeaver BW et sélectionnez *Ajouter à la liste de certificats*.
   Le certificat est ajouté à la *Liste de certificats*.
6. Enregistrez la transaction.
5. Importez le certificat du système SAP NetWeaver BW dans la plateforme de BI. Reportez-vous à l'étape 12 dans la rubrique Pour configurer HTTPS/SSL [page 534] pour plus d'informations sur l'importation de certificats.
6. Créez un utilisateur dans la plateforme de BI.

> **Remarque**
>
> Vous devez vous assurer que le nom d'utilisateur dans la plateforme de BI est identique à celui dans le système SAP NetWeaver BW. Par exemple, si le nom du système SAP NetWeaver BW est MySystem, vous devez attribuer le nom MySystem à l'utilisateur que vous créez dans la plateforme de BI.

7. Créez une destination HTTP dans le système SAP NetWeaver BW.
1. Accédez à la transaction *SM59*.
2. Sélectionnez *Connexions HTTP au serveur externe*.
3. Sélectionnez .
4. Dans la fenêtre *Destination RFC*, basculez vers l'onglet Paramètres techniques et entrez l'*Hôte*, le *Port* et le *Préfixe de chemin d'accès* comme `<hostname>`, `<port_number>` et `/biprws` respectivement.
5. Accédez à l'onglet *Connexion et sécurité* et sélectionnez *Actif* en regard de *SSL*.
6. Sélectionnez *Client SSL par défaut (standard)* au niveau de l'option *Certificat SSL*.
7. Sélectionnez *Enregistrer*.
8. Cliquez sur Tester la connexion Connection Test pour tester la connexion à la destination HTTP. Le résultat du test de la connexion s'affiche et indique OK au niveau de l'option Texte de statut.

> **Remarque**
>
> La connexion HTTP entre SAP NetWeaver BW et la plateforme de BI n'est pas possible si les conditions mentionnées ci-dessous ne sont pas remplies.
>
> - Le système BW doit être mis à jour pour prendre en charge TLS versions 1.1 et 1.2.
> - Le système BW doit prendre en charge les mêmes suites de chiffrement que celles prises en charge dans la plateforme de BI.

9. Créez une chaîne de processus dans le système SAP NetWeaver BW.
1. Accédez à la transaction *RSPC*.
2. Ouvrez le menu contextuel *Chaînes de processus* et sélectionnez *Créer un composant d'affichage*.
3. Dans la fenêtre *Création d'un regroupement*, spécifiez un *Composant applicatif* et une *Description longue*.
   Un composant SAP NetWeaver BW est créé.
4. Dans le menu contextuel du composant applicatif, sélectionnez *Créer une chaînes de processus*.
5. Entrez le nom et la description, puis cliquez sur .
   Une fois que vous avez spécifié le nom de la nouvelle chaîne de processus, la boîte de dialogue `Insérer un process de lancement` s'affiche. Vous pouvez alors insérer un process de lancement pour la chaîne de processus.
6. Spécifiez la *Variante de processus* et la *Description longue*, puis cliquez sur .
   La fenêtre Maintenir le process de lancement s'affiche.
7. Sélectionnez *Modifier les conditions*, puis *Immédiat* pour exécuter la chaîne de processus immédiatement.
8. Sélectionnez *Enregistrer* dans la fenêtre `Heure de début`.
9. Sélectionnez *Enregistrer* dans la fenêtre `Maintenir le process de lancement`.
10. Dans la fenêtre `Insérer un process de lancement`, cliquez sur .
    La chaîne de processus est créée.
10. Configurez le type de processus dans la chaîne de processus.
1. Dans la colonne *Chaînes de processus*, sélectionnez la chaîne de processus créée à l'étape précédente.
2. Développez le dossier *Charger le processus et le post-traitement* et sélectionnez *Modification des données du déclencheur d'événements dans la plateforme de BI SAP BOBJ pour BW*.
   La boîte de dialogue `Modification des données d'insertion d'un déclencheur d'événements dans la plateforme de BI SAP BOBJ pour BW` s'ouvre.

3. Dans la boîte de dialogue *Modification des données d'insertion d'un déclencheur d'événements dans la plateforme de BI SAP BOBJ pour BW*, sélectionnez .
4. Entrez les *Variantes de processus* et la *Description longue*.
5. Sélectionnez .
   La fenêtre `Maintenance des processus` s'affiche.
6. Cliquez sur en regard de *Destination* pour sélectionner une destination.
7. Cliquez sur en regard de *Événement* pour sélectionner un événement.
8. Enregistrez les modifications.
9. Sélectionnez dans la boîte de dialogue `Modification des données d'insertion d'un déclencheur d'événements dans la plateforme de BI SAP BOBJ pour BW`.
   Le type de processus est créé.
11. Activez la chaîne de processus et exécutez-la.

L'action déclenche l'événement BW mentionné dans le type de processus.

28.1.1.2 Configuration de BW Publisher

BW Publisher permet de publier des rapports Crystal (fichiers .rpt) individuellement ou par lots de BW vers la plateforme de BI.

Sous Windows, vous pouvez configurer BW Publisher de deux manières différentes :

- Lancez BW Publisher en utilisant un service sur un ordinateur hébergeant la plateforme de BI. Le service BW Publisher démarre des instances de BW Publisher comme requis.
- Lancez BW Publisher en utilisant une passerelle SAP locale pour créer des instances de BW.

Vous devez sélectionner la méthode de configuration en fonction des besoins de votre site, après avoir pris en compte les avantages et les inconvénients de chaque configuration. Une fois que vous avez configuré BW Publisher sur la plateforme de BI, vous devez configurer la publication dans le Workbench d'administration de contenu.

28.1.1.3 Configuration de BW Publisher en tant que service

Cette section explique comment activer la publication de rapports depuis BW sur la plateforme de BI, en utilisant BW Publisher comme service.

28.1.1.3.1 Distribution de l'installation de BW Publisher

Cette section décrit la distribution du service BW Publisher et explique comment séparer BW Publisher des autres composants de la plateforme de BI.

Vous pouvez équilibrer la charge de publication à partir de BW en installant les services BW Publisher sur deux ordinateurs distincts du même système de la plateforme de BI.

Lorsque vous installez BW Publisher sur les ordinateurs hébergeant la plateforme de BI, vous devez configurer chaque ordinateur pour utiliser les mêmes ID programme, hôte passerelle SAP et service de passerelle. Une fois que vous avez créé une destination RFC utilisant cet ID programme, BW équilibre les charges de publication entre les ordinateurs hébergeant la plateforme de BI. En outre, si un composant BW Publisher devient indisponible, l'autre BW Publisher est utilisé.

Vous pouvez ajouter un niveau de redondance système supplémentaire à toute configuration incluant plusieurs serveurs d'applications BW. Configurez chaque serveur d'applications BW pour exécuter une passerelle SAP. Pour chacun d'eux, installez un service BW Publisher distinct sur un ordinateur hébergeant la plateforme de BI. Configurez chaque service BW Publisher pour qu'il utilise l'hôte passerelle et le service de passerelle d'un serveur d'applications BW distinct. Avec cette configuration, la publication à partir de BW reste possible même si un BW Publisher ou un serveur d'applications tombe en panne.

Si vous souhaitez séparer BW Publisher des autres composants de la plateforme de BI, installez BW sur une passerelle SAP autonome.

Dans ce cas, vous devez installer une passerelle SAP locale sur le même ordinateur que BW Publisher. En outre, BW Publisher requiert l'accès au SDK de la plateforme de BI et au moteur d'impression de SAP Crystal Reports. Si vous installez BW Publisher et la passerelle SAP locale sur un ordinateur dédié, vous devez également installer le serveur SIA.

28.1.1.3.2 Démarrage de BW Publisher : UNIX

Exécutez le script de BW Publisher pour créer une ou plusieurs instances d'éditeur afin de répondre aux requêtes de publication. Il est recommandé de démarrer une instance d'éditeur.

Une fois lancé, BW Publisher établit une connexion au service de passerelle SAP que vous avez spécifié lors de l'exécution du programme d'installation de la plateforme de BI.

28.1.1.3.3 Démarrage de BW Publisher : Windows

Sous Windows, utilisez le CCM (Central Configuration Manager)™ pour démarrer le service BW Publisher. Lorsque vous démarrez le service BW Publisher, ce dernier crée une instance d'éditeur pour répondre aux requêtes de publication émanant de votre système BW. Si le volume des requêtes de publication augmente, BW Publisher génère automatiquement des éditeurs supplémentaires pour faire face à la demande.

28.1.1.3.4 Configuration d'une destination pour le service BW Publisher

Pour activer BW Publisher, vous devez configurer une destination RFC sur le serveur BW afin de communiquer avec le service BW Publisher. Si vous possédez un cluster BW, vous devez configurer la destination RFC sur chaque serveur, en utilisant l'instance centrale de BW comme hôte passerelle dans chaque cas.

Si vous souhaitez réaliser des publications sur plusieurs systèmes de la plateforme de BI à partir de BW, créez une destination RFC distincte pour le service BW Publisher sur chaque déploiement de la plateforme de BI.

Vous devez utiliser des ID programme uniques pour chaque destination, mais le même hôte passerelle et le même service de passerelle.

28.1.1.3.5 Configuration de BW Publisher avec une passerelle SAP locale

> **Remarque**
>
> N'utilisez pas cette configuration si la plateforme de BI est installée sous UNIX. L'utilisation de cette méthode sous UNIX peut entraîner un comportement inattendu du système.

Pour activer la publication de rapports à partir de BW sur la plateforme de BI en utilisant une passerelle SAP locale, procédez comme suit :

- Installation d'une passerelle SAP locale [page 1036].
- Configuration d'une destination pour BW Publisher [page 1036].

28.1.1.3.6 Installation d'une passerelle SAP locale

Une passerelle SAP locale doit être installée sur la machine sur laquelle vous avez installé BW Publisher. Il est recommandé qu'un administrateur SAP BASIS exécute l'installation de l'une de ces passerelles SAP.

Pour obtenir des instructions actuelles sur l'installation d'une passerelle SAP locale, reportez-vous aux instructions sur l'installation SAP incluses dans le CD de présentation SAP.

Vous trouverez la liste détaillée des environnements testés dans la PAM (Product Availability Matrix) à l'adresse http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540. Cette matrice spécifie la version et le Service Pack requis pour les serveurs d'applications, les systèmes d'exploitation, les composants SAP, etc.

Une fois que vous avez installé la passerelle SAP, utilisez `regedit` pour vérifier les entrées de registre `TMP` et `TEMP` de la sous-clé `HKEY_CURRENT_USER\Environment`. Les deux entrées de registre doivent contenir la même valeur de chaîne : le chemin absolu d'un répertoire. Si une des valeurs d'entrée contient la variable `%USERPROFILE%`, remplacez-la par un chemin de répertoire absolu. En règle générale, les deux entrées de registre sont `C:\WINDOWS\TEMP`.

28.1.1.4 Configuration d'une destination pour BW Publisher

Pour activer BW Publisher, vous devez configurer une destination RFC pour fournir à BW l'emplacement de l'ordinateur sur lequel vous avez installé la passerelle SAP et BW Publisher.

28.1.1.5 Configuration de la publication dans le Workbench d'administration de contenu

Le Workbench d'administration de contenu sert à gérer la fonctionnalité de publication de rapports à partir de SAP BW. Vous pouvez identifier des rôles du système SAP BW pour des systèmes particuliers de la plateforme de BI, publier des rapports et synchroniser des rapports entre SAP BW et un déploiement de la plateforme de BI. Une fois que vous avez configuré l'authentification SAP et BW Publisher, exécutez les fonctions décrites dans cette section pour activer la publication. Ces instructions vous permettent :

- de définir les autorisations appropriées pour différents utilisateurs du Workbench d'administration de contenu
- de configurer des connexions à la plateforme de BI sur laquelle le contenu est publié
- de définir les rôles qui peuvent publier sur chaque plateforme de BI
- de publier du contenu à partir de BW sur la plateforme de BI

28.1.1.6 Utilisateurs pouvant accéder au Workbench d'administration de contenu

Trois types d'utilisateur peuvent accéder au Workbench d'administration de contenu :

- Les utilisateurs de contenu, qui font partie des rôles portant le contenu et qui peuvent visualiser les rapports. Les droits dont ils disposent leur permettent uniquement d'afficher des rapports.
- Les éditeurs de contenu de la plateforme de BI, qui peuvent visualiser, publier, modifier et (de manière facultative) supprimer des rapports à partir de BW.
- Les administrateurs de la plateforme de BI, capables d'effectuer toutes les tâches dans le Workbench d'administration de contenu. Notamment la définition de systèmes de la plateforme de BI, la publication de rapports et la maintenance de rapports.

28.1.1.7 Création des rôles dans BW pour des éditeurs de contenu définis

Lorsque vous configurez BW en vue de l'intégrer à la plateforme de BI, vérifiez si la structure actuelle de vos rôles vous permet de désigner rapidement des utilisateurs BW comme éditeurs de contenu ou administrateurs système pour les systèmes de la plateforme de BI.

Il est recommandé d'attribuer un nom descriptif aux nouveaux rôles que vous créez. Par exemple : `EDITEURS_CONTENU_BOE` et `ADMINISTRATEURS_SYSTEME_BOE`.

> → Conseil
>
> Vous pouvez affecter à un utilisateur administratif tout ou partie des droits d'administration système.

Pour modifier les droits accordés à ces nouveaux rôles (ou à vos rôles existants) dans la plateforme de BI, vous devez d'abord configurer l'authentification SAP et importer les rôles. Vous pouvez alors modifier les droits de chaque rôle importé en utilisant la Central Management Console.

Pour en savoir plus sur la création des rôles, consultez votre documentation SAP. Pour en savoir plus sur l'utilisation des rôles dans l'administration de contenu, voir les sections suivantes :

- Importation de rôles SAP [page 350].
- Configuration des dossiers et de la sécurité sur la plateforme de BI [page 1028].
- Paramètres de sécurité par défaut des dossiers [page 1029].

28.1.1.8 Configuration de l'accès au Workbench d'administration de contenu

Pour chaque type d'utilisateur pouvant accéder au Workbench d'administration de contenu, vous devez appliquer les autorisations appropriées dans BW. Les autorisations sont répertoriées dans les tableaux suivants.

Autorisations réservées aux utilisateurs administratifs

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
S_TCODE	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Exécution (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Modification, affichage (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Exécution (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Création, Modification, Affichage, Suppression (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Création, Suppression (01, 06)
ZCNTADMRPT	ACTVT	Affichage, Suppression, Activation, Maintenance, Vérification (03, 06, 07, 23, 39)

Autorisations réservées aux éditeurs de contenu

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Exécution (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Exécution (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Affichage (03)
ZCNTADMJOB	ACTVT	(Création, Suppression) 01, 06
ZCNTADMRPT	ACTVT	Affichage, Activation, Maintenance, Vérification (03, 07, 23, 39) Suppression (facultatif) (06) Modification (facultatif) (02)

L'octroi des droits de suppression de rapports aux éditeurs de contenu dans le Workbench d'administration de contenu de BW est facultatif. Toutefois, vous devez savoir que la suppression d'un rapport dans BW supprime également le rapport sur la plateforme de BI. Si les éditeurs ne disposent pas des droits suffisants pour supprimer des rapports sur la plateforme, une erreur est générée.

Autorisations réservées aux utilisateurs de contenu

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	Exécution (16)
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Exécution (16)
	RSADMWBOBJ	WORKBENCH

Objet d'autorisation	Champ	Valeurs
	ACTVT	Affichage (03)

28.1.1.9 Définition d'un système de la plateforme de Business Intelligence

Vous devez créer une définition système dans le Workbench d'administration de contenu pour chaque système de la plateforme de BI dans lequel vous souhaitez publier les rapports.

28.1.1.9.1 Pour ajouter un système de la plateforme de BI

1. Exécutez la transaction `/crystal/rptadmin` pour accéder au Workbench d'administration de contenu.
2. Dans le volet *Opérations*, sélectionnez *Système Enterprise*.
3. Cliquez deux fois sur *Ajouter un nouveau système*.
4. Dans l'onglet *Système* :
   - Saisissez un nom descriptif dans le champ *Alias*. Evitez d'utiliser des espaces ou des caractères spéciaux car ces caractères nécessitent un traitement particulier lorsque l'alias est utilisé lors de la configuration des portails Enterprise.
   - Saisissez le nom de l'ordinateur sur lequel s'exécute votre CMS. Si vous avez configuré votre CMS pour écouter un autre port que celui par défaut, saisissez **`CMSNAME:PORT`**.
   - Sélectionnez *Système par défaut* si vous voulez publier des rapports sur ce système à partir d'un rôle qui n'a pas été explicitement affecté à un système de la plateforme de BI. Vous ne pouvez définir qu'un seul système de la plateforme de BI comme système par défaut.
     Dans la liste des systèmes disponibles, le système par défaut est signalé par une coche verte.
5. Cliquez sur *Enregistrer*.
6. Dans l'onglet *Destinations RFC*, ajoutez chaque destination RFC associée à ce système.

   Pour ajouter une destination, cliquez sur le bouton *Insérer ligne*. Dans la liste qui s'affiche, cliquez deux fois sur le nom de la destination RFC.

   > **Remarque**
   >
   > Un système de la plateforme de BI peut avoir plusieurs destinations pour plus de redondance système. Voir « Distribution de l'installation de BW Publisher »

7. Cochez la case en regard du nom de destination ajouté, puis cliquez sur *Vérifier la définition BOE*.

   Ce test vise à vérifier que BW peut contacter BW Publisher spécifié et se connecter à ce système en utilisant le compte utilisateur d'autorisation Crystal.
8. Dans l'onglet *HTTP* :
   - Dans le champ *Protocole*, saisissez **`http`** ou **`https`**, si le serveur Web connecté à la plateforme de BI est configuré pour HTTPS.

- Dans le champ *Hôte et port du serveur Web*, saisissez le nom de domaine complet ou l'adresse IP du serveur Web qui héberge la zone de lancement BI. Dans le cas d'une installation utilisant un serveur d'applications Java, saisissez le numéro du port. Par exemple, saisissez **`boserver01.businessobjects.com:8080`**.
- Dans le champ *Chemin*, saisissez **`SAP`**
  Ce chemin est le chemin virtuel que votre serveur Web utilise lorsqu'il se réfère au sous-dossier `sap` de votre contenu Web de la plateforme de BI. Fournissez une autre valeur uniquement si vous avez personnalisé votre environnement Web et l'emplacement de vos fichiers de contenu Web de la plateforme.
  N'insérez pas de barre oblique au début ou à la fin de cette valeur.
- Dans le champ *Application du visualiseur*, tapez le nom de l'application de votre visualiseur.
  Pour utiliser le visualiseur de la plateforme de BI par défaut qui emploie la version Java de la zone de lancement BI, entrez **`openDocument.jsp`**
  Si la plateforme de BI a été installée sous Windows à l'aide de la configuration `ASP.NET` par défaut, pour utiliser le navigateur par défaut, saisissez **`report/report_view.aspx`**

9. Dans l'onglet *Langues*, sélectionnez les langues des rapports qui seront publiés dans ce système.
10. Dans l'onglet *Rôles*, ajoutez les rôles portant le contenu que vous voulez associer à ce système de la plateforme de BI.

    Voir « Importation de rôles SAP ».
11. Cliquez sur le bouton *Insérer ligne*.

    La liste des rôles disponibles à ajouter à ce système s'affiche.

    > **Remarque**
    >
    > Chaque rôle peut publier sur un seul système de la plateforme de BI. Si les rôles que vous voulez ajouter au système de la plateforme de BI ne figurent pas dans la liste, cliquez sur *Annuler* pour revenir à l'onglet *Rôles*, puis cliquez sur *Réaffecter rôles*.
12. Sélectionnez les rôles à publier sur ce système, puis cliquez sur *OK*.
13. Dans l'onglet *Présentation*, sélectionnez les paramètres de sécurité par défaut pour les dossiers des rapports et des rôles publiés sur ce système de la plateforme de BI.

    > **Remarque**
    >
    > Un dossier est automatiquement créé sur la plateforme de BI pour chaque rôle publié sur ce système. Le dossier contient des raccourcis vers les rapports publiés avec ce rôle.

    > **Remarque**
    >
    > Une fois que vous avez configuré un système de la plateforme de BI, le fait de changer les niveaux de sécurité par défaut ici n'affecte pas les niveaux de sécurité des dossiers ou rapports publiés du rôle. Pour changer les niveaux de sécurité par défaut pour tous les rôles et tous les contenus publiés sur la plateforme, supprimez les dossiers et les raccourcis des rôles du système. (Cela ne supprime pas les rapports eux-mêmes.) Modifiez les paramètres de sécurité ici, puis republiez les rôles et les rapports.
14. Cliquez sur le bouton *OK* situé en bas pour enregistrer vos paramètres et créer le système de la plateforme de BI dans le Workbench d'administration de contenu.

Vous pouvez maintenant publier des rapports depuis BW sur la plateforme de BI.

Informations associées

Distribution de l'installation de BW Publisher [page 1034]
Importation de rôles SAP [page 350]

28.1.1.10 Publication des rapports à l'aide du Workbench d'administration de contenu

Après avoir enregistré un rapport dans BW, vous pouvez le publier à l'aide du Workbench d'administration de contenu. Vous pouvez utiliser le Workbench d'administration de contenu pour publier des rapports individuels ou pour publier tous les rapports enregistrés sur un rôle particulier. Seuls les utilisateurs qui disposent des autorisations octroyées à un éditeur de contenu Crystal (voir Création et application des autorisations [page 1057]) peuvent utiliser le Workbench d'administration de contenu pour publier et gérer des rapports.

28.1.1.11 Publication des rôles ou des rapports

1. Exécutez la transaction `/crystal/rptadmin` pour accéder au Workbench d'administration de contenu.
2. Dans le volet *Opérations*, sélectionnez *Publier les rapports*.
3. Pour rechercher des contenus enregistrés sur votre système BW, cliquez deux fois sur *Sélectionner les rapports et les rôles à publier*.
   Une boîte de dialogue conçue pour vous aider à filtrer les rôles et les rapports disponibles s'ouvre.
4. Dans la liste, sélectionnez le ou les systèmes comportant un contenu que vous voulez afficher.

   > **Remarque**
   >
   > La liste répertorie l'ensemble des systèmes disponibles définis sur le système BW.

5. Ensuite, filtrez vos résultats pour limiter le nombre de rapports et de rôles qui doivent s'afficher. Utilisez les options suivantes :
   - *Version des objets*
     Sélectionnez "A : actif" pour afficher l'ensemble des rapports pouvant être publiés. Cette option laissée vide permet d'afficher tous les rapports. (Les autres options sont des termes SAP réservés.)
   - *Statut des objets*
     Sélectionnez "ACT Actif, exécutable" pour afficher uniquement les rapports qui ont été publiés. Sélectionnez "INA Inactif, non exécutable" pour afficher uniquement les rapports qui n'ont pas été publiés. Laissez le champ vide pour afficher tous les rapports. (Les autres options sont des termes SAP réservés.)
   - *Filtre des rôles*
     Si vous saisissez du texte dans cette zone, seuls les rôles correspondant au texte saisi seront affichés. Utilisez l'astérisque (*) comme caractère générique. Par exemple, pour afficher tous les rôles commençant par la lettre d, tapez "d*".
   - *Description des rapports*
     Si vous saisissez du texte dans cette zone, seuls les rapports dont la description correspond au texte saisi seront affichés. Utilisez l'astérisque (*) comme caractère générique pour remplacer un

nombre non défini de caractères. Utilisez le signe + comme caractère générique pour remplacer 0 ou 1 caractère. Par exemple, pour afficher tous les rapports dont la description contient le mot "revenu", tapez *revenu*.

6. Cliquez sur *OK*.
   La liste des rapports qui répondent aux critères de recherche apparaît dans le panneau de droite.
   Les rapports sont organisés selon la hiérarchie suivante : Système de la plateforme de BI > Rôles sur ce système > Rapports enregistrés pour le rôle.
   Chaque élément de la hiérarchie est accompagné d'un point rouge, jaune ou vert. Les éléments situés à un niveau supérieur de la hiérarchie reflètent le statut des éléments qu'ils contiennent, la condition la moins favorable étant répercutée au sommet de la hiérarchie. Par exemple, si un rôle contient un rapport jaune (actif) et que tous les autres rapports du rôle sont verts (publiés), le rôle apparaît avec un point jaune (actif).
   - Vert : l'élément est entièrement publié. Si l'élément est un système de la plateforme de BI ou un rôle, tous les rapports qu'il contient sont publiés.
   - Jaune : l'élément est actif mais non publié. Si l'élément est un rapport, il est disponible pour la publication. Si l'élément est un rôle ou un système de la plateforme de BI, tout le contenu est actif et au moins un élément du rôle ou du système n'a pas été publié.
   - Rouge : l'élément est un contenu SAP et n'est pas disponible pour la publication par le biais du Workbench d'administration de contenu. Le contenu n'est disponible pour la publication qu'après avoir été activé à l'aide du Workbench d'administration de contenu.
7. Sélectionnez les rapports que vous souhaitez publier.
   Pour publier tous les rapports d'un rôle, sélectionnez le rôle. Pour publier tous les rôles d'un système de la plateforme de BI, sélectionnez le système.

   > **Remarque**
   >
   > Lorsque vous sélectionnez un rôle (ou un système), tous les rapports contenus dans ce rôle (ou système) sont sélectionnés. Pour annuler la sélection, désélectionnez la case correspondant au rôle (ou au système) et cliquez sur Actualiser.

8. Cliquez sur *Publier*.

   > **Remarque**
   >
   > Les rapports publiés en arrière-plan sont traités à mesure que les ressources système se libèrent. Pour utiliser cette option, cliquez sur *En arrière-plan*, et non sur *Publier*.

9. Cliquez sur *Actualiser* pour mettre à jour le statut des systèmes, rôles et rapports de la plateforme de BI dans le Workbench d'administration de contenu.

   > **→ Conseil**
   >
   > Pour visualiser un rapport, cliquez avec le bouton droit de la souris sur le rapport, puis sélectionnez *Visualiser*. Pour voir les requêtes utilisées par le rapport, cliquez avec le bouton droit sur le rapport puis sélectionnez *Requêtes utilisées*.

   > **Remarque**
   >
   > Si vous souhaitez écraser un rapport que vous avez publié sur la plateforme de BI , cliquez sur *Ecraser*.

Informations associées

Planification de la publication en arrière-plan [page 1044]

28.1.1.12 Planification de la publication en arrière-plan

La publication de rapports en arrière-plan, immédiate ou sous forme de tâche planifiée, permet d'économiser les ressources système. Il est recommandé de publier les rapports en arrière-plan afin d'améliorer la réactivité du système.

La publication périodique des rapports en tant que tâches planifiées synchronise les informations de rapport entre BW et votre déploiement de la plateforme de BI. Il est recommandé de planifier tous les rapports (ou les rôles contenant ces rapports). Vous pouvez également synchroniser manuellement les rôles et les rapports à l'aide de l'option Mettre le statut à jour de l'opération Maintenance des rapports. Pour en savoir plus, voir Mise à jour du statut des rapports [page 1044].

28.1.1.13 Mise à jour des informations système pour les rapports publiés

BW Publisher utilise les informations système SAP saisies ici pour mettre à jour la source de données des rapports publiés. Vous pouvez utiliser le serveur d'application BW local ou l'instance BW centrale si vous préférez une configuration avec équilibrage des charges.

28.1.1.14 Maintenance des rapports

Les tâches de maintenance de rapports incluent la synchronisation des informations relatives aux rapports entre la plateforme de BI et BW (Mettre le statut à jour), la suppression des rapports non voulus (Supprimer les rapports) et la mise à jour des rapports migrés depuis les versions antérieures de la plateforme (Post-migration).

28.1.1.14.1 Mise à jour du statut des rapports

Si vous modifiez un rapport publié sur un système de la plateforme de BI (par exemple, si vous changez le rôle sur lequel le rapport est publié), la modification n'est pas répercutée dans BW tant que la plateforme de BI et BW ne sont pas synchronisés. Vous pouvez planifier une tâche de publication de façon à synchroniser la plateforme de BI et BW de manière périodique (voir Planification de la publication en arrière-plan [page 1044]), ou mettre à jour manuellement le statut du rapport à l'aide de l'outil Maintenance des rapports.

28.1.1.14.2 Suppression de rapports

Lorsque vous supprimez un rapport publié à partir de BW, à l'aide du Workbench d'administration de contenu, le rapport est également supprimé de la plateforme de BI. Seuls les utilisateurs disposant des autorisations nécessaires pour supprimer des rapports sur BW et sur le système de la plateforme de BI peuvent supprimer des rapports.

> ⓘ Remarque
>
> Si un utilisateur a le droit de supprimer un rapport sur BW, mais pas sur le système de la plateforme de BI sur lequel le rapport est publié, une erreur risque d'être générée.

28.1.1.15 Configuration du gestionnaire de requêtes http SAP

Pour permettre la visualisation des rapports dans BW, vous devez configurer BW pour utiliser le gestionnaire de requêtes http inclus avec le Workbench d'administration de contenu. Ensuite, lorsqu'un utilisateur WB ouvre un rapport Crystal dans SAPGUI, BW peut router correctement la requête de visualisation via le Web.

Utilisez la transaction SICF pour accéder à la liste des hôtes virtuels et des services actifs sur votre système BW. Créez un nœud appelé `ce_url` sous BW dans la hiérarchie `default_host` et ajoutez `/CRYSTAL/CL_BW_HTTP_HANDLER` à la liste des gestionnaires. Une fois ce service créé, vous devez l'activer manuellement.

28.1.1.16 Configurations pour le traitement de données SAP

28.1.1.16.1 Traitement des rapports planifiés en mode batch SAP

Sous Windows, vous pouvez exécuter des rapports planifiés sur la plateforme de BI en utilisant le mode de traitement par lots de SAP. Les pilotes InfoSet et Open SQL peuvent exécuter des rapports à l'aide du mode batch SAP ou arrière-plan lorsque des variables d'environnement spécifiques sont définies sur 1. Les variables d'environnement appropriées sont les suivantes :

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (pour le pilote InfoSet)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (pour le pilote Open SQL)

Toutefois, il est recommandé d'utiliser cette fonctionnalité uniquement dans le cas d'une installation distribuée de la plateforme de BI. Lorsque ces variables d'environnement sont définies sur 1, les pilotes exécutent les rapports à l'aide du mode batch SAP, quel que soit le composant de reporting exécutant réellement le rapport. Par conséquent, si vous créez ces variables d'environnement sous forme de variables d'environnement système sur un ordinateur exécutant une combinaison de serveurs de la plateforme de BI, les pilotes exécutent tous les rapports en mode batch (par lots) (y compris les requêtes de rapports à la demande à partir du serveur de traitement Crystal Reports et du Report Application Server).

Pour garantir que les pilotes exécutent uniquement vos rapports planifiés en mode batch (les rapports exécutés par l'Adaptive Job Server), évitez de définir des variables d'environnement système sur des

ordinateurs hébergeant des combinaisons de serveurs de la plateforme de BI. Suivez plutôt ces étapes pour personnaliser les variables d'environnement de chaque Adaptive Job Server.

> **Remarque**
>
> Les utilisateurs SAP qui planifient des rapports sur la plateforme de BI peuvent avoir besoin d'autorisations supplémentaires dans SAP.

Informations associées

Planification d'un rapport en mode de traitement par lot à l'aide d'une requête Open SQL [page 1072]

28.1.1.16.2 Pour traiter des rapports planifiés en mode batch SAP

1. Créez un script (fichier `.bat`) dans un éditeur de texte comme le Bloc-notes, contenant les données suivantes :

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   Ce script définit les variables d'environnement sur 1, puis exécute les paramètres transmis au script à partir de la ligne de commande.
2. Enregistrez le fichier sous `jobserver_batchmode.bat` dans un dossier de chaque ordinateur hébergeant l'Adaptive Job Server.
3. Connectez-vous à la CMC (Central Management Console).
4. Choisissez *Serveurs*.
5. Développez le nœud *Catégories de service* et sélectionnez *Analysis Services*.
6. Sélectionnez *Serveur de traitement adaptatif* et choisissez *Propriétés* dans le menu contextuel.
   La page *Propriétés* s'affiche.
7. Sur la page *Propriétés*, localisez le champ *Paramètres de ligne de commande*.

   Il s'agit de la commande de démarrage pour l'Adaptive Job Server. Par exemple :

   ```
   "\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects
   Enterprise\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport -restart
   ```
8. Faites précéder la commande par défaut du chemin d'accès complet au fichier `jobserver_batchmode.bat` que vous avez enregistré sur l'ordinateur hébergeant l'Adaptive Job Server.

   Dans cet exemple, le fichier batch est enregistré sur un ordinateur appelé SERVER01 sous :

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```

La nouvelle commande de démarrage pour l'Adaptive Job Server est :

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$
\Program Files\SAP Business Objects\SAP
BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name
SERVER01.report  -ns SERVER01
-objectType BusinessObjects Enterprise.Report -lib procReport  -restart
```

Cette nouvelle commande de démarrage lance d'abord le fichier batch. Ce dernier définit à son tour les variables d'environnement requises avant l'exécution de la commande de démarrage initiale pour l'Adaptive Job Server. Cela garantit que les variables d'environnement disponibles pour l'Adaptive Job Server sont différentes de celles disponibles pour les serveurs responsables du reporting à la demande (le serveur de traitement Crystal Reports et le Report Application Server).

9. Cliquez sur *Enregistrer et fermer*.
10. Cliquez avec le bouton droit de la souris sur l'Adaptive Job Server et sélectionnez *Démarrer* dans le menu contextuel.

> **Remarque**
>
> Si le démarrage de l'Adaptive Job Server échoue, vérifiez votre nouvelle commande de démarrage.

28.1.1.17 Configurations pour les transports SAP

28.1.1.17.1 Présentation

La plateforme de BI comprend ces transports :

- Transport de connectivité Open SQL
- Transport de connectivité InfoSet
- Transport de définition de la sécurité de niveau ligne
- Transport de définition de clusters
- Transport Workbench d'administration de contenu
- Transport de personnalisation des paramètres BW Query
- Transport MDX
- Transport ODS

Il existe deux ensembles de transport différents : les transports compatibles Unicode et les transports ANSI. Si vous utilisez la version 6.20 du système BASIS ou une version ultérieure, utilisez les transports compatibles Unicode. Si vous utilisez une version du système BASIS antérieure à la version 6.20, utilisez les transports ANSI. Tous les transports sont situés dans le répertoire suivant du support de distribution de votre produit : `\Collaterals\Add-Ons\SAP\Transports\`.

> **Remarque**
>
> Lors de la vérification portant sur la présence d'éventuels conflits au niveau de l'installation, assurez-vous qu'aucun des noms d'objet n'existe déjà dans votre système SAP. Les objets utilisent un espace de noms **`/crystal/`** par défaut. Il est donc inutile de le créer. Si vous créez l'espace de noms **`/crystal/`** manuellement, vous serez invité à indiquer les clés de réparation de licence auxquelles vous n'avez pas accès.

28.1.1.17.2 Configuration des transports

Pour configurer les composants d'accès aux données ou de BW Publisher de la plateforme de BI, vous devez importer les transports appropriés dans votre système SAP. Ces composants utilisent le contenu de ces fichiers de transport lors de la communication avec le système SAP.

Les procédures d'installation et de configuration requises sur le système SAP doivent être effectuées par un spécialiste de BASIS connaissant bien le système de modification et de transport et possédant les droits d'administration sur le système SAP. La procédure exacte pour l'importation des fichiers de transport varie selon la version de BASIS installée sur votre ordinateur. Pour en savoir plus sur la procédure, consultez votre documentation SAP.

Lorsque vous déployez pour la première fois le composant d'accès aux données, tous les utilisateurs peuvent accéder à toutes vos tables SAP par défaut. Pour sécuriser les données SAP auxquelles les utilisateurs peuvent accéder, utilisez l'éditeur de définition de la sécurité.

Une fois les transports importés, vous devez configurer les niveaux d'accès utilisateur appropriés. Créez les autorisations requises et appliquez-les via des profils ou des rôles aux utilisateurs SAP qui concevront, exécuteront ou planifieront les rapports Crystal.

Informations associées

Création et application des autorisations [page 1057]

28.1.1.17.2.1 Types de transport

Il existe deux ensembles de transport différents : les transports compatibles Unicode et les transports ANSI. Si vous utilisez la version 6.20 du système BASIS ou une version ultérieure, utilisez les transports compatibles Unicode. Si vous utilisez une version du système BASIS antérieure à la version 6.20, utilisez les transports ANSI. Tous les transports sont situés dans le répertoire suivant de votre produit : `\Collaterals\Add-Ons\SAP\Transports`. Le fichier `transports.txt` répertorie les fichiers de transport compatibles Unicode et ANSI.

Les types de transport sont décrits ci-dessous :

- Transport de connectivité Open SQL
  Le transport de connectivité Open SQL permet au pilote Open SQL de se connecter au système SAP et de créer des rapports à partir de celui-ci.
- Transport de définition de la sécurité de niveau ligne
  Ce transport fournit l'éditeur de définition de sécurité, un outil qui sert d'interface graphique aux tables /crystal/auth dans le transport de connectivité Open SQL.
- Transport de définition de clusters
  Ce transport fournit l'outil de définition de clusters. Cet outil vous permet de créer un référentiel de métadonnées pour les définitions de clusters de données ABAP. Ces définitions fournissent au pilote Open SQL les informations dont il a besoin pour créer des rapports à partir de ces clusters de données.

> **Remarque**
>
> Les clusters de données ABAP ne sont pas les mêmes que dans les tables de clusters. Les tables de clusters sont déjà définies dans le DDIC.

- Transport de connectivité InfoSet
  Le transport de connectivité InfoSet permet au pilote InfoSet d'accéder aux InfoSets et aux requêtes SAP.
- Transport Workbench d'administration de contenu
  Ce transport fournit des fonctionnalités d'administration de contenu pour les systèmes BW. Il n'est disponible qu'en tant que transport compatible Unicode.
- Transport de personnalisation des paramètres BW Query
  Ce transport fournit une prise en charge des valeurs de paramètre personnalisées et par défaut dans les rapports basés sur des requêtes BW.
- Transport de connectivité MDX BW
  Ce transport permet au pilote MDX Query d'accéder aux cubes et requêtes BW. Il est compatible avec le correctif BW 3.0B 27 ou version(s) ultérieure(s), et le correctif BW 3.1C 21 ou version(s) ultérieure(s).
- Transport de connectivité ODS
  Ce transport permet au pilote ODS Query d'accéder aux données ODS. Il est compatible avec le correctif BW 3.0B 27 ou version(s) ultérieure(s), et le correctif BW 3.1C 21 ou version(s) ultérieure(s).

28.1.1.17.2.2 Vérification de la présence de conflits

Le contenu des fichiers de transport est enregistré automatiquement sous l'espace de nom SAP BusinessObjects lorsque vous importez les fichiers. L'espace de nom SAP BusinessObjects est réservé à cette fin dans les versions récentes de R/3 et de MYSAP ERP. Cependant, il est possible que les noms de certains objets, tels que les objets d'autorisation, les classes d'autorisation et les objets antérieurs ne comportent pas les préfixes qui conviennent. Par conséquent, il est recommandé de vérifier la présence de conflits au niveau de ces types d'objets avant d'importer les fichiers de transport.

Si le groupe de fonctions, l'un des modules de fonction ou tout autre objet existe déjà sur le système SAP, vous devez alors résoudre l'espace de nom avant d'importer les fichiers de transport SAP BusinessObjects. Consultez la documentation de la plateforme technologique SAP NetWeaver pour connaître les procédures appropriées à votre version de SAP.

28.1.1.17.2.3 Importation des fichiers de transport

Lisez le fichier `transports_French.txt` contenu dans le répertoire suivant sur le support de distribution de votre produit : `\Collaterals\Add-Ons\SAP\Transports\`. Ce fichier texte répertorie les noms exacts des fichiers constituant chaque transport. Les répertoires `cofiles` et `data` qui se trouvent sous le répertoire `transports` correspondent aux répertoires .../`trans/cofiles` et .../`trans/data` de votre serveur SAP.

Vous devez importer le transport de connectivité Open SQL avant d'importer le transport de définition de la sécurité de niveau ligne ou le transport de définition de clusters. Vous pouvez importer les autres transports dans n'importe quel ordre.

> **Remarque**
>
> Une fois les fichiers du CD copiés sur le serveur, assurez-vous qu'ils ne sont pas protégés en écriture avant d'importer les transports. L'importation échoue si les fichiers d'importation sont accessibles seulement en lecture.

> **Remarque**
>
> Les transports étant des fichiers binaires, sur les ordinateurs UNIX, vous devez ajouter ces fichiers par FTP en mode binaire (pour éviter qu'ils ne soient corrompus). En outre, vous devez posséder les droits d'écriture sur le serveur UNIX.

28.1.1.17.2.4 Transports

28.1.1.17.2.4.1 Transport de connectivité Open SQL

Le transport de connectivité Open SQL permet aux pilotes de se connecter au système SAP et de créer des rapports à partir de celui-ci.

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/OPENSQL	Groupe de fonctions	Fonctions Open SQL
/CRYSTAL/OSQL_AUTH_FORMS	Programme	Programme d'aide
/CRYSTAL/OSQL_EXECUTE	Programme	Programme d'aide
/CRYSTAL/OSQL_TYPEPOOLPROG	Programme	Programme d'aide
/CRYSTAL/OSQL_TYPEPOOLS	Programme	Programme d'aide
/CRYSTAL/OSQL_UTILS	Programme	Programme d'aide
ZSSI	Classe d'objet d'autorisation	Objets d'autorisation pour le reporting
ZSEGREPORT	Objet d'autorisation	Objet d'autorisation pour le reporting
/CRYSTAL/OSQL_CLU_ACTKEY_ENTRY	Tableau	Métadonnées de cluster
/CRYSTAL/OSQL_FCN_PARAM	Tableau	Métadonnées de fonction
/CRYSTAL/OSQL_FCN_PARAM_FIELD	Tableau	Métadonnées de fonction
/CRYSTAL/OSQL_FIELD_ENTRY	Tableau	Métadonnées de tableau

Objet	Type	Description
/CRYSTAL/OSQL_OBJECT_ENTRY	Tableau	Métadonnées de tableau
/CRYSTAL/OSQL_RLS_CHK_ENTRY	Tableau	Métadonnées de RLS
/CRYSTAL/OSQL_RLS_FCN_ENTRY	Tableau	Métadonnées de RLS
/CRYSTAL/OSQL_RLS_VAL_ENTRY	Tableau	Métadonnées de RLS
ZCLUSTDATA	Tableau	Métadonnées de cluster
ZCLUSTID	Tableau	Métadonnées de cluster
ZCLUSTKEY	Tableau	Métadonnées de cluster
ZCLUSTKEY2	Tableau	Métadonnées de cluster
/CRYSTAL/AUTHCHK	Tableau	Métadonnées de RLS
/CRYSTAL/AUTHFCN	Tableau	Métadonnées de RLS
/CRYSTAL/AUTHKEY	Tableau	Métadonnées de RLS
/CRYSTAL/AUTHOBJ	Tableau	Métadonnées de RLS
/CRYSTAL/AUTHREF	Tableau	Métadonnées de RLS
ZSSAUTHCHK	Tableau	Anciennes métadonnées de RLS
ZSSAUTHOBJ	Tableau	Anciennes métadonnées de RLS
ZSSAUTHKEY	Tableau	Anciennes métadonnées de RLS
ZSSAUTHREF	Tableau	Anciennes métadonnées de RLS
ZSSAUTH FCN	Tableau	Anciennes métadonnées de RLS

28.1.1.17.2.4.2 Transport de connectivité InfoSet

Le transport de connectivité InfoSet permet au pilote InfoSet d'accéder aux InfoSets. Ce transport est compatible avec la version 4.6c et les versions ultérieures de R/3. N'importez pas ce transport si vous disposez de la version R/3 4.6a de SAP ou d'une version antérieure.

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/FLAT	Groupe de fonctions	Fonctions wrapper InfoSet

Objet	Type	Description
/CRYSTAL/QUERY_BATCH	Programme	Exécution du mode batch
/CRYSTAL/QUERY_BATCH_STREAM	Programme	Exécution du mode batch en continu

28.1.1.17.2.4.3 Transport de définition de la sécurité de niveau ligne

Ce transport fournit l'éditeur de définition de sécurité, un outil qui sert d'interface graphique aux tables /CRYSTAL/AUTH dans le transport de connectivité Open SQL.

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/TABMNT	Groupe de fonctions	Groupe de fonctions pour l'affichage de la maintenance des tables pour les restrictions des fonctions
/CRYSTAL/RLSDEF	Programme	Programme principal
/CRYSTAL/RLS_INCLUDE1	Programme	Inclut un programme contenant les définitions du module
/CRYSTAL/RLS_INCLUDE2	Programme	Inclut un programme contenant les définitions des sous-programmes
TDDAT [/CRYSTAL/AUTHFCN]	Contenu de la table	Définition de la maintenance de la table
TVDIR [/CRYSTAL/AUTHFCN]	Contenu de la table	Définition de la maintenance de la table
/CRYSTAL/AUTHFCNS	Définition de l'objet de maintenance et de transport	Définition de la maintenance de la table
/CRYSTAL/RLS	Transaction	Transaction du programme principal
/CRYSTAL/RLSFCN	Transaction	Transaction d'aide appelée de manière interne par le programme principal

28.1.1.17.2.4.4 Transport de définition de clusters

Ce transport fournit l'outil de définition de clusters. Cet outil vous permet de créer un référentiel de métadonnées pour les définitions de clusters de données ABAP. Ces définitions fournissent au pilote Open SQL les informations dont il a besoin pour créer des rapports à partir de ces clusters de données.

> **Remarque**
>
> Les clusters de données ABAP ne sont pas les mêmes que dans les tables de clusters. Les tables de clusters sont déjà définies dans le DDIC.

Objet	Type	Description
ZCIMPRBG	Programme	Programme principal
ZCRBGTOP	Programme	Programme d'inclusion
ZCDD	Transaction	Transaction du programme principal

28.1.1.17.2.4.5 Transport Workbench d'administration de contenu

Ce transport fournit des fonctionnalités d'administration de contenu pour les systèmes BW. Il n'est disponible qu'en tant que transport compatible Unicode.

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/CL_BW_HTTP_HANDLER	Classe	Gestionnaire de requêtes http prenant en compte les CE multiples
/CRYSTAL/OBJECT_STATUS_DOM	Domaine	Activité de rapport
/CRYSTAL/OBJ_POLICY_DOM	Domaine	Sécurité des objets CE
/CRYSTAL/OBJECT_STATUS	Elément de données	Activité de rapport
/CRYSTAL/OBJ_POLICY	Elément de données	Sécurité des objets CE
/CRYSTAL/CE_SYNCH	Groupe de fonctions	Stubs de l'éditeur
/CRYSTAL/CA_MSG	Classe de message	Messages de statut
/CRYSTAL/CE_SYNCH_FORMS	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN	Programme	Composant de programme
/CRYSTAL/CONTENT_AD-MIN_CLASS_D	Programme	Composant de programme
/CRYSTAL/CONTENT_AD-MIN_CLASS_I	Programme	Composant de programme

Objet	Type	Description
/CRYSTAL/CONTENT_ADMIN_CTREE	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_FORMS	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_MODU-LES	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_PAIS	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_PBOS	Programme	Composant de programme
/CRYSTAL/CONTENT_AD-MIN_TAB_FRM	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_TOP	Programme	Composant de programme
/CRYSTAL/PUBLISH_WORKER	Programme	Composant de programme
/CRYSTAL/PUBLISH_WORKER_DISP	Programme	Composant de programme
/CRYSTAL/PUBLISH_WORKER_DISP_I	Programme	Composant de programme
/CRYSTAL/PUBLISH_WOR-KER_FORMS	Programme	Composant de programme
/CRYSTAL/PUBLISH_WORKER_PROC	Programme	Composant de programme
/CRYSTAL/PUBLISH_WOR-KER_PROC_I	Programme	Composant de programme
/CRYSTAL/PUBLISH_WOR-KER_SCREEN	Programme	Composant de programme
/CRYSTAL/CA_DEST	Tableau	Etat d'application
/CRYSTAL/CA_JOB	Tableau	Etat d'application
/CRYSTAL/CA_JOB2	Tableau	Etat d'application
/CRYSTAL/CA_LANG	Tableau	Etat d'application
/CRYSTAL/CA_PARM	Tableau	Etat d'application
/CRYSTAL/CA_ROLE	Tableau	Etat d'application
/CRYSTAL/CA_SYST	Tableau	Etat d'application
/CRYSTAL/MENU_TREE_ITEMS	Structure	Etat d'application
/CRYSTAL/REPORT_ID	Tableau	Etat d'application

Objet	Type	Description
/CRYSTAL/RPTADMIN	Transaction	Transaction du programme principal
/CRYSTAL/EDIT_REPORT	Programme	Wrapper pour la modification de rapports
/CRYSTAL/EDIT_REPORT	Groupe de fonctions	Fonctions pour la modification des rapports
ZSSI	Classe d'objet d'autorisation	Autorisations Crystal
ZCNTADMCES	Objet d'autorisation	Opérations CE
ZCNTADMRPT	Objet d'autorisation	Opérations de rapport
ZCNTADMJOB	Objet d'autorisation	Opérations de tâche en arrière-plan

28.1.1.17.2.4.6 Transport de connectivité ODS

Ce transport permet au pilote ODS Query d'accéder aux données ODS. Il est compatible avec le correctif BW 3.0B 27 ou version(s) ultérieure(s), et le correctif BW 3.1C 21 ou version(s) ultérieure(s).

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/ODS_REPORT	Groupe de fonctions	Fonctions ODS

28.1.1.17.2.4.7 Transport de personnalisation des paramètres BW Query

Ce transport fournit une prise en charge des valeurs de paramètre personnalisées et par défaut dans les rapports basés sur des requêtes BW.

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/PERS_VAR	Structure	Définition des variables
/CRYSTAL/PERS_VALUE	Structure	Définition des valeurs
/CRYSTAL/PERS	Groupe de fonctions	Fonctions de personnalisation

28.1.1.17.2.4.8 Transport de connectivité MDX BW

Ce transport permet au pilote MDX Query d'accéder aux cubes et requêtes BW. Il est compatible avec le correctif BW 3.0B 27 ou version(s) ultérieure(s), et le correctif BW 3.1C 21 ou version(s) ultérieure(s).

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/MDX	Groupe de fonctions	Fonctions MDX
/CRYSTAL/MDX_STREAM_LAYOUT	Définition de table	Structure de jeu de données
/CRYSTAL/CX_BAPI_ERROR	Classe	Exception
/CRYSTAL/CX_METADATA_ERROR	Classe	Exception
/CRYSTAL/CX_MISSING_STREA-MINFO	Classe	Exception
/CRYSTAL/CX_NO_MORE_CELLS	Classe	Exception
/CRYSTAL/CX_NO_MORE_MEMBERS	Classe	Exception
/CRYSTAL/CX_NO_MORE_PROPER-TIES	Classe	Exception
/CRYSTAL/CX_SAVE_SESSION_STATE	Classe	Exception
/CRYSTAL/MDX_APPEND_DATA	Classe	Processeur de jeux de données
/CRYSTAL/MDX_READER_BASE	Classe	Processeur de jeux de données
/CRYSTAL/MDX_READ_DIMENSIONS	Classe	Processeur de jeux de données
/CRYSTAL/MDX_READ_MEASURES	Classe	Processeur de jeux de données
/CRYSTAL/MDX_READ_PROPERTIES	Classe	Processeur de jeux de données
/CRYSTAL/MDX_AXIS_LEVELS	Table	Structure de métadonnées
/CRYSTAL/MDX_PROPERTY_KEYS	Table	Structure de métadonnées
/CRYSTAL/MDX_PROPERTY_VALUES	Table	Structure de métadonnées
/CRYSTAL/ MDX_STREAM_LAYOUT_TAB	Table	Structure de métadonnées

28.1.1.18 Présentation

Cette section contient une liste d'autorisations SAP qui, selon notre expérience et notre environnement de test, sont requises lors de l'exécution de tâches courantes de la plateforme de BI dans un environnement SAP intégré. Des champs ou des objets d'autorisation supplémentaires peuvent être nécessaires, en fonction de votre propre implémentation.

Pour chaque objet d'autorisation, vous devez créer une autorisation et définir les valeurs de champs appropriées. Vous devez ensuite appliquer les autorisations appropriées aux profils (ou rôles) de vos utilisateurs SAP. Les sections suivantes décrivent les autorisations requises et fournissent les valeurs de champ requises. Pour des détails de procédure spécifiques à votre version de SAP, reportez-vous à votre documentation SAP.

> ⓘ Remarque
>
> Les informations contenues dans cette section sont fournies à titre indicatif uniquement.

> ⓘ Remarque
>
> L'objet d'autorisation ZSEGREPORT fait partie de la classe d'objet ZSSI, qui est installée lorsque vous importez les fichiers de transport SAP Integration nécessaires pour prendre en charge les requêtes Open SQL.

28.1.1.18.1 Création et application des autorisations

Vous devez créer et appliquer les autorisations nécessaires à chaque utilisateur pour accéder aux informations par le biais de Desktop Intelligence Integration for SAP. Les procédures exactes de création, de configuration et d'application des autorisations dépendent de la version de SAP que vous avez installée. Cette section contient une liste d'autorisations SAP qui, selon notre expérience et nos environnements de test, sont requises lors de l'exécution de tâches courantes avec la plateforme de BI intégrée dans un environnement SAP NetWeaver ABAP. Des champs ou des objets d'autorisation supplémentaires peuvent être nécessaires, en fonction de votre propre implémentation.

Informations associées

Configuration de la publication dans le Workbench d'administration de contenu [page 1037]

28.1.1.19 Actions dans BW

Cette section contient une liste des actions disponibles dans BW.

28.1.1.19.1 Actions au sein de Crystal Reports

28.1.1.19.1.1 Création d'un rapport à partir d'une requête dans un rôle BW

Objet d'autorisation	Champ	Valeurs
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

<USER_ROLE> désigne le nom du rôle auquel l'utilisateur appartient. Vous pouvez spécifier plusieurs valeurs dans ce champ.

* **<QUERY_OWNER >**représente le nom du propriétaire de la requête. Si vous spécifiez un nom, vous pouvez créer des rapports uniquement à partir de ces requêtes avec ce propriétaire. Saisissez * pour créer des rapports à partir des requêtes d'un propriétaire quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.2 Ouverture d'un rapport existant à partir d'un rôle BW

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.3 Actualisation ou affichage de l'aperçu d'un rapport

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****

Objet d'autorisation	Champ	Valeurs
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.4 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.5 Définition de l'emplacement de la source de données

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.6 Enregistrement d'un rapport dans un rôle BW

Objet d'autorisation	Champ	Valeurs
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** désigne le nom du rôle auquel l'utilisateur appartient. Vous pouvez spécifier plusieurs valeurs dans ce champ.

28.1.1.19.1.7 Préparation d'un rapport pour la traduction lors de l'enregistrement dans BW

Objet d'autorisation	Champ	Valeurs
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

<USER_ROLE> désigne le nom du rôle auquel l'utilisateur appartient. Vous pouvez spécifier plusieurs valeurs dans ce champ.

28.1.1.19.1.8 Enregistrement et publication simultanée d'un rapport sur la plateforme de BI

Objet d'autorisation	Champ	Valeurs
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** ***
	RSINFOCUBE	**<INFO_CUBE>** ***
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** ***
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** ***
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** **
	ACTVT	16

<USER_ROLE> désigne le nom du rôle auquel l'utilisateur appartient. Vous pouvez spécifier plusieurs valeurs dans ce champ.

** **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **< INFO_AREA>, <INFO_CUBE>** ou **<COMP_ID>,** saisissez * afin de représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.1.9 Démarrage de BEx Query Designer™

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** **
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>** saisissez * afin de représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.2 Actions au sein de la zone de lancement BI

28.1.1.19.2.1 Connexion à la plateforme de BI à l'aide des références de connexion SAP

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

28.1.1.19.2.2 Visualisation d'un rapport SAP BW à la demande

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.2.3 Actualisation d'un rapport à partir du visualiseur

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****

Objet d'autorisation	Champ	Valeurs
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>** saisissez * afin de représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.2.4 Planification d'un rapport

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP

Objet d'autorisation	Champ	Valeurs
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** représente le nom du propriétaire de la requête à partir de laquelle vous créez le rapport. Si vous saisissez le nom du propriétaire de la requête, vous pouvez créer des rapports uniquement à partir des requêtes de ce propriétaire. Saisissez * pour désigner un propriétaire de requête quelconque.

** Pour **<INFO_AREA>**, **<INFO_CUBE>** ou **<COMP_ID>**, saisissez * pour représenter une valeur quelconque. Si vous indiquez une valeur spécifique, vous pouvez créer des rapports uniquement à partir de requêtes contenant ces zones d'information, ces cubes et ces ID composant.

28.1.1.19.2.5 Lecture des listes de choix dynamiques dans les paramètres de rapport

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

28.1.1.19.3 Actions au sein de SAP NetWeaver (ABAP)

28.1.1.19.3.1 A partir de Crystal Reports à l'aide du pilote Open SQL

Cette section vous présente une liste des différentes opérations disponibles dans SAP NetWeaver (ABAP) depuis Crystal Report via le pilote Open SQL.

28.1.1.19.3.2 Connexion à un serveur SAP

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.3 Création d'un rapport

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

28.1.1.19.3.4 Ouverture ou affichage de l'aperçu d'un rapport existant

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL

Objet d'autorisation	Champ	Valeurs
	ACTVT	16
ZSEGREPORT	ACTVT	02

28.1.1.19.3.5 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.6 Définition de l'emplacement de la source de données

Objet d'autorisation	Champ	Valeurs
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.4 Actions au sein de Crystal Reports à l'aide du pilote InfoSet et reporting à partir d'InfoSet

28.1.1.19.4.1 Connexion à un serveur SAP

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.4.2 Création d'un rapport à partir d'un InfoSet sur SAP NetWeaver (ABAP)

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

> **Remarque**
>
> Ajoutez également suffisamment d'autorisations pour afficher les lignes de données. Par exemple, P_ORIG ou P_APAP.

Informations associées

Définition de l'emplacement de la source de données [page 1070]

28.1.1.19.4.3 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

28.1.1.19.4.4 Définition de l'emplacement de la source de données

Objet d'autorisation	Champ	Valeurs
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

28.1.1.19.5 Actions au sein de Crystal Reports à l'aide du pilote InfoSet et reporting à partir d'une requête ABAP

28.1.1.19.5.1 Connexion à un serveur SAP

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.5.2 Création d'un rapport à partir d'une requête ABAP sur SAP NetWeaver

Objet d'autorisation	Champ	Valeurs
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_TABU_DIS	ACTVT	03
	GROUP	Nom du groupe de tables

28.1.1.19.5.3 Vérification de la base de données

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

28.1.1.19.5.4 Définition de l'emplacement de la source de données

Objet d'autorisation	Champ	Valeurs
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03

Objet d'autorisation	Champ	Valeurs
	GROUP	Nom du groupe de tables

28.1.1.19.6 Actions au sein de la plateforme de BI

28.1.1.19.6.1 Planification d'un rapport en mode dialogue (à l'aide d'une requête Open SQL)

Objet d'autorisation	Champ	Valeurs
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> **Remarque**
>
> La valeur de CLASS est BLANK (VIDE).

28.1.1.19.6.2 Planification d'un rapport en mode de traitement par lot à l'aide d'une requête Open SQL

Objet d'autorisation	Champ	Valeurs
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A

Objet d'autorisation	Champ	Valeurs
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

> **Remarque**
>
> La valeur de CLASS est BLANK (VIDE).

28.1.1.19.6.3 Système d'autorisation Crystal

Objet d'autorisation	Champ	Valeur
Autorisation d'accès aux fichiers (S_DATASET)	Activité (ACTVT)	Lecture, écriture (33, 34)
	Nom de fichier physique (FILENAME)	* (signifie TOUS)
	Nom de programme ABAP (PROGRAM)	*
Contrôle des autorisations pour accès RFC (S_RFC)	Activité (ACTVT)	16
	Nom de RFC à protéger (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Type d'objet RFC à protéger (RFC_TYPE)	Groupe de fonctions (FUGR)
Maintenance principale des utilisateurs : Groupes d'utilisateurs (S_USER_GRP)	Activité (ACTVT)	Créer ou générer, et afficher (03)
	Groupe d'utilisateurs dans maintenance du fichier utilisateur (CLASS)	* **Remarque** Pour plus de sécurité, vous pouvez répertorier explicitement les groupes d'utilisateurs dont les membres doivent accéder à la plateforme de BI.

28.1.1.19.6.4 Exécution et conception de requêtes BW BEx

Lors de la création d'un rapport à partir d'un univers basé sur une requête BW BEx, si une dimension date est incluse, l'administrateur système doit accorder l'autorisation `S_RS_IOBJ` à la fois à l'utilisateur concevant l'univers et à l'utilisateur exécutant le rapport.

Objet d'autorisation	Champ	Valeurs
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

28.2 Configuration pour l'intégration JD Edwards

28.2.1 Configuration de la connexion unique pour SAP Crystal Reports

Par défaut, la plateforme de BI est configurée pour permettre aux utilisateurs de SAP Crystal Reports d'accéder aux données JD Edwards EnterpriseOne à l'aide de la connexion unique.

28.2.1.1 Pour désactiver la connexion unique pour JD Edwards et SAP Crystal Reports

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sélectionnez *crdb_pseone*.
5. Cliquez sur *Supprimer*.
6. Cliquez sur *Enregistrer et fermer*.
7. Dans la page *Serveurs* de la CMC, sélectionnez *Services Crystal Reports* et cliquez sur *Redémarrer le serveur*.

28.2.1.2 Pour activer la connexion unique pour JD Edwards et SAP Crystal Reports

Si vous avez désactivé la connexion unique pour JD Edwards et SAP Crystal Reports et souhaitez la réactiver.

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sous *Utiliser le contexte de connexion unique pour se connecter à la base de données avec les pilotes suivants*, saisissez *crdb_pseone*.
5. Cliquez sur *Ajouter*.
6. Cliquez sur *Enregistrer et fermer*.
7. Dans la page *Serveurs* de la CMC, sélectionnez *Services Crystal Reports* et cliquez sur *Redémarrer le serveur*.

28.2.2 Configuration de SSL (Secure Sockets Layer) pour les intégrations JD Edwards

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour toutes les communications réseau établies entre clients et serveurs au sein de votre déploiement de la plateforme de BI et JD Edwards EnterpriseOne.

L'utilisation de données JD Edwards EnterpriseOne avec la plateforme de BI nécessite d'apporter des modifications à votre configuration SSL. De même que dans la configuration SSL d'autres serveurs et clients de la plateforme de BI, stockez la clé et les fichiers de certificat suivants dans un emplacement sécurisé (dans le même répertoire), accessible par les ordinateurs de votre déploiement de la plateforme de BI.

- Fichier de certificat approuvé (cacert.der).
- Fichier de certificat serveur généré (servercert.der).
- Fichier de clé serveur (server.key).
- Fichier de phrase de passe (passphrase.txt).

28.2.2.1 Pour activer la connectivité des données avec SSL pour JD Edwards EnterpriseOne

> **Remarque**
>
> Toutes les valeurs décrites dans la procédure suivante sont sensibles à la casse.

1. Copiez vos certificats SSL sous `C:\SSLCert`.
2. Démarrez le Central Configuration Manager (CCM).
3. Arrêtez le Server Intelligence Agent (SIA).
4. Cliquez deux fois sur le SIA pour ouvrir la boîte de dialogue *Propriétés*.

5. Cliquez sur l'onglet *Protocole*.
6. Sélectionnez *Activer SSL*.
7. Comme *Dossier des certificats SSL*, choisissez le répertoire contenant les certificats SSL : `C:\SSLCert`.
8. Pour le *Fichier du certificat SSL du serveur*, sélectionnez `servercert.der`.
9. Pour les *Fichiers des certificats SSL approuvés*, sélectionnez `cacert.der`.
10. Pour le *Fichier de la clé privée SSL*, sélectionnez `server.key`.
11. Pour le *Fichier contenant la phrase de passe de la clé privée SSL*, sélectionnez `passphrase.txt`.
12. Cliquez sur *Appliquer*.
13. Démarrez le Server Intelligence Agent.

Vous devez redémarrer les serveurs de reporting de la plateforme de BI (tels que l'Adaptive Job Server) pour que ces changements prennent effet.

28.2.2.2 Fichier de propriétés de la configuration SSL

Le fichier de propriétés `sslconf.properties` contient toutes les informations pour les certificats et les clés utilisés par la plateforme de BI. Par exemple :

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Le fichier `sslconf.properties` doit être placé dans le dossier où est installée la plateforme de BI, `C:\Program Files\Business Objects\BusinessObjects 13.0` par défaut.

28.3 Configuration pour l'intégration PeopleSoft Enterprise

28.3.1 Configuration de la connexion unique pour SAP Crystal Reports et PeopleSoft Enterprise

Par défaut, la plateforme de BI est configurée pour permettre aux utilisateurs de SAP Crystal Reports d'accéder aux données PeopleSoft Enterprise à l'aide de la connexion unique.

28.3.1.1 Pour désactiver la connexion unique pour PeopleSoft Enterprise et SAP Crystal Reports

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sélectionnez *crdb_psenterprise*.
5. Cliquez sur *Supprimer*.
6. Cliquez sur *Enregistrer et fermer*.
7. Dans la page *Serveurs* de la CMC, sélectionnez *Services Crystal Reports* et cliquez sur *Redémarrer le serveur*.

28.3.1.2 Pour activer la connexion unique pour PeopleSoft Enterprise et SAP Crystal Reports

Si vous avez désactivé la connexion unique pour PeopleSoft Enterprise et SAP Crystal Reports et souhaitez la réactiver.

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sous *Utiliser le contexte de connexion unique pour se connecter à la base de données avec les pilotes suivants*, saisissez *crdb_psenterprise*.
5. Cliquez sur *Ajouter*.
6. Cliquez sur *Enregistrer et fermer*.
7. Dans la page *Serveurs* de la CMC, sélectionnez *Services Crystal Reports* et cliquez sur *Redémarrer le serveur*.

28.3.2 Configuration de la communication Secure Sockets Layer

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour toutes les communications réseau établies entre clients et serveurs au sein de votre déploiement de la plateforme de BI.

De même que dans la configuration SSL d'autres serveurs et clients de la plateforme de BI, stockez la clé et les fichiers de certificat suivants dans un emplacement sécurisé (dans le même répertoire), accessible par les machines de votre déploiement de la plateforme de BI.

- Fichier de certificat approuvé (cacert.der).
- Fichier de certificat serveur généré (servercert.der).
- Fichier de clé serveur (server.key).

- Fichier de phrase de passe (passphrase.txt).

28.3.2.1 Fichier de propriétés de la configuration SSL

Le fichier de propriétés `sslconf.properties` contient toutes les informations pour les certificats et les clés utilisés par les composants de la plateforme de BI. Par exemple :

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Le fichier `sslconf.properties` doit être placé dans le dossier d'installation de la plateforme de BI, par défaut `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

28.3.2.2 Pour activer le serveur de requêtes PeopleSoft avec SSL

> **Remarque**
>
> Toutes les valeurs décrites dans la procédure suivante sont sensibles à la casse.

1. Copiez vos certificats SSL sous `C:\SSLCert`.
2. Démarrez le Central Configuration Manager (CCM).
3. Arrêtez le Server Intelligence Agent (SIA).
4. Cliquez deux fois sur le SIA pour ouvrir la boîte de dialogue *Propriétés*.
5. Cliquez sur l'onglet *Protocole*.
6. Sélectionnez *Activer SSL*.
7. Comme *Dossier des certificats SSL*, choisissez le répertoire contenant les certificats SSL : `C:\SSLCert`.
8. Pour le *Fichier du certificat SSL du serveur*, sélectionnez `servercert.der`.
9. Pour les *Fichiers des certificats SSL approuvés*, sélectionnez `cacert.der`.
10. Pour le *Fichier de la clé privée SSL*, sélectionnez `server.key`.
11. Pour le *Fichier contenant la phrase de passe de la clé privée SSL*, sélectionnez `passphrase.txt`.
12. Cliquez sur *Appliquer*.
13. Démarrez le Server Intelligence Agent.

Vous devez redémarrer les serveurs de reporting de la plateforme de BI (tels que l'Adaptive Job Server) pour que ces changements prennent effet.

28.3.2.3 Pour activer la passerelle de sécurité avec SSL

> **Remarque**
>
> Toutes les valeurs décrites dans la procédure suivante sont sensibles à la casse.

1. Copiez vos certificats SSL sous `C:\SSLCert`.
2. Démarrez le Central Configuration Manager (CCM).
3. Arrêtez le Server Intelligence Agent (SIA).
4. Cliquez deux fois sur le SIA pour ouvrir la boîte de dialogue *Propriétés*.
5. Cliquez sur l'onglet *Protocole*.
6. Sélectionnez *Activer SSL*.
7. Comme *Dossier des certificats SSL*, choisissez le répertoire contenant les certificats SSL : `C:\SSLCert`.
8. Pour le *Fichier du certificat SSL du serveur*, sélectionnez `servercert.der`.
9. Pour les *Fichiers des certificats SSL approuvés*, sélectionnez `cacert.der`.
10. Pour le *Fichier de la clé privée SSL*, sélectionnez `server.key`.
11. Pour le *Fichier contenant la phrase de passe de la clé privée SSL*, sélectionnez `passphrase.txt`.
12. Cliquez sur *Appliquer*.
13. Démarrez le Server Intelligence Agent.

28.3.3 Ajustement des performances pour les systèmes PeopleSoft

Pour garantir des performances optimales lors de la création de rapports à partir de requêtes PeopleSoft, il est important de comprendre comment les requêtes sont exécutées par Crystal Reports et la plateforme de BI.

A chaque actualisation ou exécution d'un rapport basé sur une requête PeopleSoft, une connexion avec un serveur PeopleSoft est établie :

- Dans les environnements PeopleSoft Enterprise (PeopleTools 8.46 ou version ultérieure), une connexion est établie avec le *serveur d'analyse PeopleSoft*.
- Dans les environnements PeopleSoft Enterprise (PeopleTools 8.21 à 8.45), une connexion est établie avec le *serveur d'applications PeopleSoft*.

28.3.3.1 Recommandations

Dans un déploiement optimal, un ou plusieurs serveurs d'analyse ou serveurs d'applications PeopleSoft sont configurés pour gérer uniquement des demandes de rapport. Sur chacun de ces serveurs, les paramètres pour le nombre minimal et maximal d'instances contrôlent le nombre de demandes de rapport pouvant être traitées en une fois, à tout moment. Cette configuration offre les avantages suivants :

- Il n'existe aucun conflit entre les demandes de rapport et d'autres demandes transactionnelles dans le serveur PeopleSoft.

- Il est possible d'exécuter la maintenance sur le serveur qui gère les demandes de rapport sans désactiver le serveur qui gère les demandes transactionnelles.

Dans un environnement où les demandes de rapport et demandes transactionnelles sont gérées par le même serveur d'analyse ou serveur d'applications PeopleSoft, vous devez configurer la plateforme de BI afin qu'il n'exécute qu'un rapport à la fois. Dans le cas contraire, les utilisateurs ne pourront effectuer aucune demande transactionnelle si tous les processus PSANALYTICSRV ou PSAPPSRV sont utilisés pour exécuter des rapports.

> **Remarque**
>
> Pour en savoir plus sur la façon de limiter le nombre de travaux de rapport planifiés et de travaux d'affichage de rapports à la demande, voir "Gestion et configuration des serveurs" dans le *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.

> **Remarque**
>
> Il n'est pas possible de configurer le système pour limiter le nombre d'utilisateurs Crystal Reports qui peuvent essayer d'accéder au serveur simultanément.

Si des problèmes de performance surviennent, utilisez l'outil de configuration Psadmin pour déterminer si les demandes sont mises en file d'attente. Surveillez également les ressources système sur l'ordinateur hébergeant le serveur d'analyse ou le serveur d'applications PeopleSoft. Si la mémoire virtuelle est utilisée en raison d'un manque de mémoire physique, le traitement peut également être ralenti.

28.3.3.2 Serveurs PeopleSoft

Dans un serveur d'analyse PeopleSoft, le processus qui actualise ou exécute les rapports est le processus PSANALYTICSRV. Dans un serveur d'applications PeopleSoft, le processus qui actualise ou exécute les rapports est le processus PSAPPSRV. Le nombre de processus PSANALYTICSRV ou PSAPPSRV disponibles détermine le nombre des rapports que vous pouvez exécuter simultanément.

Un fichier de configuration de serveur d'analyse ou de serveur d'applications PeopleSoft contient généralement les informations suivantes :

```
Min Instances=3
Max Instances=5
```

Dans cet exemple, un minimum de trois processus PSANALYTICSRV ou PSAPPSRV est disponible à tout moment avec la possibilité d'en augmenter le nombre jusqu'à cinq. Les paramètres ne signifient pas nécessairement que cinq rapports peuvent toujours être exécutés simultanément ; les processus peuvent également être utilisés pour gérer d'autres tâches dans le système. Si aucun processus PSANALYTICSRV ou PSAPPSRV n'est disponible pour gérer une demande, cette dernière est mise en file d'attente jusqu'à ce qu'un processus soit disponible.

> **Remarque**
>
> Le fichier de configuration pour les serveurs *d'application* PeopleSoft contient souvent également le paramètre `Service Timeout` qui spécifie le délai d'attente des demandes avant qu'un processus ne soit disponible. Si aucun processus ne se libère dans le temps spécifié pour ce paramètre, le délai d'attente de la demande expire.

28.4 Configuration pour l'intégration Siebel

28.4.1 Configuration de Siebel pour l'intégration à la plateforme SAP BI

L'intégration de la plateforme de BI fournit un lien vers Crystal Reports qui permet d'intégrer la suite SAP BusinessObjects Business Intelligence à une application Siebel. Une fois installé et configuré, le nouvel élément de menu permet aux utilisateurs de lancer la zone de lancement BI depuis l'application Siebel.

Par défaut, les fichiers nécessaires sont installés dans le dossier suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

28.4.1.1 Pour importer un projet d'intégration Siebel de la plateforme de Business Intelligence

1. Démarrez les Outils Siebel.
2. Cliquez sur *Outils* > *Importer depuis l'archive*.
3. Quand une invite vous demande un fichier d'archive, naviguez jusqu'au dossier Siebel Files de votre installation du produit d'intégration.

   Par défaut, il s'agit de : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.
4. Accédez au sous-dossier approprié (Siebel 7.7 ou Siebel 8.0) et sélectionnez le fichier `BusinessObjectsEnterprise.sif`.
   L'Assistant d'importation s'affiche.
5. Cliquez sur *Fusionner la définition d'objet du fichier d'archive avec la définition du référentiel*.
6. Suivez les écrans de l'Assistant pour terminer l'importation du projet d'intégration.
   Le projet d'intégration est ajouté au référentiel.
7. Verrouillez le projet *BusinessObjects Integration*.

28.4.2 Création de l'élément de menu Crystal Reports

1. Dans les Outils Siebel, verrouillez le projet *Menu*.
2. Dans l'Explorateur d'objets, sélectionnez l'objet *Elément de menu*.

   > **Remarque**
   >
   > Si l'objet Menu n'apparaît pas dans l'Explorateur d'objets, cliquez sur *Afficher* > *Options* dans les Outils Siebel, cliquez sur l'onglet *Explorateur d'objets* puis sélectionnez l'objet *Menu*.
3. Dans la liste *Menus*, sélectionnez le menu *Web générique*.

4. Cliquez sur l'en-tête de la liste *Eléments de menu*.
5. Cliquez sur *Modifier* > *Nouvel enregistrement*.
6. Définissez le nouvel élément de menu comme il se doit. Voici les valeurs recommandées :
   - Nom : Visualisation - Crystal Reports
   - Commande : Crystal Reports
   - Commentaires : Menu des rapports intégrés SAP BusinessObjects
   - Inactif : Faux
7. Utilisez un numéro de position pour sélectionner l'emplacement de l'élément de menu dans votre menu d'affichage.

   Pour vous aider à choisir un numéro de position, triez les éléments de menu par position.
8. Vous pouvez à présent ajouter des enregistrements de Paramètres régionaux pour localiser correctement la légende.

Recompilez ensuite votre application Siebel. Voir Recompilation de l'application Siebel [page 1082].

28.4.2.1 Recompilation de l'application Siebel

Une fois que vous avez installé la plateforme de BI et mis ses commandes à disposition des utilisateurs via un élément de menu Siebel, vous devez compiler l'application Siebel en suivant les procédures habituelles. Pour en savoir plus, voir le Bookshelf Siebel.

Lorsque vous avez recompilé l'application Siebel, regénérez ses fichiers JavaScript. Dans les versions Siebel 7.7 et suivantes, il est possible de régénérer automatiquement les fichiers JavaScript lors du processus de recompilation.

Comme les étapes requises pour compiler le référentiel Siebel sont effectuées sur la station de travail des Outils Siebel, vous devez redéployer les fichiers JavaScript en résultant sur votre serveur Siebel depuis la station de travail des Outils Siebel. Habituellement, et selon l'endroit où est installé Siebel, vous trouverez les fichiers JavaScript générés à l'emplacement suivant :

```
C:\sea77\tools\PUBLIC\ENU\<srf1096416329_444>
```

Le nom de dossier exemple `<srf1096416329_444>` est généré par les Outils Siebel et correspond uniquement au fichier du référentiel en résultant.

Les fichiers JavaScript doivent être déployés sur le serveur Siebel, habituellement à l'emplacement suivant, selon l'endroit où Siebel est installé :

```
C:\sea77\SWEApp\PUBLIC\ENU\<srf1096416329_444>
```

Conservez le nom de dossier généré par les Outils Siebel.

De plus, vous devez mettre à jour votre fichier de configuration Siebel sur l'ordinateur du serveur Siebel pour que le service soit pris en charge. Recherchez le fichier de configuration approprié sur l'ordinateur du serveur Siebel. Par exemple, si vous exécutez une version anglaise du Centre d'appels Siebel, utilisez le fichier `uagent.cfg`. Par défaut, ce fichier se trouve sous `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` pour Siebel 7.7.

Ajoutez ensuite la ligne suivante à la fin de la section SWE du fichier de configuration :

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

Les numéros de `ClientBusinessService` sont séquentiels. S'il n'existe aucun autre ClientBusinessService dans la section SWE, définissez **<NUMBER>** sur 0. Sinon, définissez **<NUMBER>** sur la valeur supérieure suivante.

Pour Siebel 8.x ou suivant :

1. Connectez-vous à Outils Siebel et recherchez l'objet d'application *Agent universel Siebel* dans l'Explorateur d'objets.
2. Développez les objets d'application pour faire apparaitre l'objet *Prop. utilisateur d'application*.
3. Créez un enregistrement pour chaque Business Service à déclarer, en définissant les propriétés Nom et Valeur pour chacun comme indiqué :
   - Nom = ClientBusinessServiceX
   - Valeur = BusinessObjects Integration

Créez ensuite l'élément de menu Crystal Reports qui appelle la commande Siebel importée.

28.4.3 Reconnaissance contextuelle

La reconnaissance contextuelle est une fonctionnalité qui présente à l'utilisateur des rapports susceptibles d'être pertinents pour leur tâche en cours. Dans ce cas, les utilisateurs accédant directement à Crystal Reports depuis une application client Siebel verront automatiquement s'afficher des rapports qui ont été conçus pour intégrer des données Siebel.

28.4.3.1 Configuration de la reconnaissance contextuelle

Avant de configurer la sensibilité du contexte, assurez-vous que :

- le produit Siebel Integration est installé
- Siebel est configuré pour s'intégrer à la plateforme de BI

1. Ouvrez la CMC (Central Management Console).
2. Cliquez sur *Authentification*.
3. Cliquez deux fois sur *Siebel*.
   L'interface de mappage Siebel apparaît.
4. Cliquez sur *Domaines*.
   L'interface de mappage des domaines apparaît.
5. Notez le nom de domaine correspondant au serveur Siebel que vous souhaitez utiliser.
6. Fermez l'interface de mappage Siebel
7. Ouvrez la zone de lancement BI.
8. Créez sous `Dossiers publics\Siebel` un dossier ayant le même nom que le domaine Siebel dans la CMC.

9. Placez tous les rapports conçus pour intégrer les informations Siebel dans ce dossier.

28.4.3.2 Spécification de l'URL pour la reconnaissance contextuelle

1. Après avoir régénéré les fichiers JavaScript de l'application, accédez au dossier Siebel Files de votre installation de la plateforme de BI, qui est par défaut : `C:\:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files`.
2. Copiez le fichier `BusinessObjectsEnterpriseServer.html`. Recherchez ensuite le dossier public où le programme genbscript a généré les nouveaux fichiers JavaScript et placez une copie du fichier `BusinessObjectsEnterpriseServer.html` dans le sous-dossier de la langue appropriée.

   Par exemple, si vous avez généré les fichiers JavaScript d'une application dans le dossier `c:\sea752\SWEApp\PUBLIC\ENU` du serveur Siebel, copiez le fichier `BusinessObjectsEnterpriseServer.html` dans le dossier `c:\sea752\SWEApp\PUBLIC\ENU`.
3. Ouvrez le fichier `BusinessObjectsEnterpriseServer.html` du dossier public dans un éditeur de texte comme Notepad et recherchez cette ligne :

   ```
   Var userDomain = "SIEB78"
   ```

   ```
   var destAddr = "http://<serveur SAP BusinessObjects>:8080/BOE/BI/logon/
   siebelStart.do"
   ```

> **Remarque**
>
> Si vous modifiez la variable `<userDomain>` ou `<destAddr>`, vous devez effacer les pages Web du cache de votre navigateur pour vous assurer que le navigateur désignera la bonne adresse de destination.

> **Remarque**
>
> La variable userDomain est sensible à la casse.

28.4.3.3 Vérification de la reconnaissance contextuelle

1. Dans Outils Siebel, cliquez sur *Déboguer* > *Démarrer*.
2. Naviguez vers un écran quelconque et cliquez sur le menu *Visualiser*.
   Votre nouvel élément de menu Crystal Reports doit s'afficher dans le menu.
3. Cliquez sur l'élément de menu *Crystal Reports*.
   La plateforme de BI ouvre la fenêtre Zone de lancement BI qui demande le nom d'utilisateur et le mot de passe pour se connecter. Cela n'est nécessaire que lors de la première connexion avant une expiration de la session. Le nom de domaine configuré en HTML et l'authentification Siebel doivent déjà être indiqués.

> **Remarque**
>
> Cette étape sert uniquement à vérifier votre installation jusqu'à ce point. Vous ne pouvez pas vous connecter à la plateforme de BI avec l'authentification Siebel tant que vous n'avez pas mappé les responsabilités Siebel à la plateforme de BI.

28.4.3.4 Ajout de dossiers à la plateforme de BI

L'intégration de la plateforme de BI pour Siebel requiert que certains dossiers soient ajoutés à la zone de lancement BI pour activer entièrement la fonctionnalité de reconnaissance contextuelle.

Pour fonctionner correctement, les dossiers contextuels doivent avoir la structure suivante : `Dossiers publics\Siebel\<Nom de domaine>`. Seuls les rapports stockés dans le sous-dossier `<Nom de domaine>` et configurés dans le système Siebel pour être associés avec un composant d'entreprise SAP BusinessObjects particulier s'afficheront à l'aide de la fonctionnalité de reconnaissance contextuelle. Le `<Nom de domaine>` utilisé ici doit être identique à celui défini pour Siebel dans la configuration de l'authentification et à la valeur configurée côté Siebel dans le fichier `BusinessObjectsEnterpriseServer.html`.

> **Remarque**
>
> Les Outils Siebel sont nécessaires pour terminer les étapes de cette section.

28.4.4 Configuration de la connexion unique pour SAP Crystal Reports et Siebel

Par défaut, la plateforme de BI est configurée pour permettre aux utilisateurs de SAP Crystal Reports d'accéder aux données Siebel à l'aide de la connexion unique.

28.4.4.1 Pour désactiver la connexion unique pour Siebel et SAP Crystal Reports

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.
3. Cliquez sur *Options de connexion unique*.
4. Sélectionnez *crdb_siebel*.
5. Cliquez sur *Supprimer*.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez SAP Crystal Reports.

28.4.4.2 Pour activer la connexion unique pour Siebel et SAP Crystal Reports

Si vous avez désactivé la connexion unique pour Siebel et SAP Crystal Reports et souhaitez la réactiver.

1. Dans la CMC (Central Management Console), cliquez sur *Applications*.
2. Cliquez deux fois sur *Configuration de Crystal Reports*.

3. Cliquez sur *Options de connexion unique*.
4. Sous *Utiliser le contexte de connexion unique pour se connecter à la base de données*, saisissez *crdb_siebel*.
5. Cliquez sur *Ajouter*.
6. Cliquez sur *Enregistrer et fermer*.
7. Redémarrez les serveurs SAP Crystal Reports.

28.4.5 Configuration de la communication Secure Sockets Layer

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) pour toutes les communications réseau établies entre clients et serveurs au sein de vos déploiements Siebel et de la plateforme de BI.

De même que pour la configuration SSL d'autres serveurs et clients de la plateforme de BI, stockez les fichiers de clés et de certificats suivants dans un répertoire sécurisé accessible aux ordinateurs de votre déploiement Siebel.

- Fichier de certificat approuvé (cacert.der).
- Fichier de certificat serveur généré (servercert.der).
- Fichier de clé serveur (server.key).
- Fichier de phrase de passe (passphrase.txt).

Fichier de propriétés de la configuration SSL

Le fichier de propriétés `sslconf.properties` contient toutes les informations pour les certificats et les clés utilisés par les composants Integration for Siebel. Par exemple :

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Le fichier `sslconf.properties` doit être placé dans le dossier où est installé le produit de la plateforme de BI, par défaut : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`.

28.4.5.1 Pour activer la connexion aux données Siebel avec SSL

> **Remarque**
>
> Toutes les valeurs décrites dans la procédure suivante sont sensibles à la casse.

1. Copiez vos certificats SSL sous `C:\SSLCert`.
2. Démarrez le Central Configuration Manager (CCM).
3. Arrêtez le Server Intelligence Agent (SIA).
4. Cliquez deux fois sur le SIA pour ouvrir la boîte de dialogue *Propriétés*.
5. Cliquez sur l'onglet *Protocole*.
6. Sélectionnez *Activer SSL*.
7. Comme *Dossier des certificats SSL*, choisissez le répertoire contenant les certificats SSL : `C:\SSLCert`.
8. Pour le *Fichier du certificat SSL du serveur*, sélectionnez `servercert.der`.
9. Pour les *Fichiers des certificats SSL approuvés*, sélectionnez `cacert.der`.
10. Pour le *Fichier de la clé privée SSL*, sélectionnez `server.key`.
11. Pour le *Fichier contenant la phrase de passe de la clé privée SSL*, sélectionnez `passphrase.txt`.
12. Cliquez sur *Appliquer*.
13. Démarrez le Server Intelligence Agent.

Vous devez redémarrer les serveurs de reporting de la plateforme de BI (tels que l'Adaptive Job Server) pour que ces changements prennent effet.

29 Gestion et configuration des journaux

29.1 Journalisation des traces de composant

Historiques

La plateforme de BI génère des messages au niveau du système et les écrit dans des fichiers journaux. Les administrateurs système peuvent utiliser ces fichiers journaux pour suivre les performances ou déboguer les erreurs.

Traces

La plateforme de BI génère également des traces (enregistrements des événements qui se produisent pendant l'exécution d'un composant surveillé) et les collecte dans des fichiers journaux portant l'extension `.glf`. Les événements suivis vont des messages de statut aux erreurs d'exceptions graves. Les équipes de SAP support et les développeurs peuvent utiliser les traces pour créer des rapports sur les performances des composants de la plateforme de BI (serveurs et applications Web) et l'activité des composants surveillés.

En définissant le niveau du journal de suivi, vous déterminez le type et la verbosité des informations envoyées au fichier journal. Le niveau du journal de suivi est un filtre qui supprime les traces inférieures à un seuil spécifié. En surveillant le journal de suivi d'un composant, vous pouvez déterminer si l'instance actuelle d'un composant ou sa configuration doit être modifiée pour fonctionner avec une charge de travail accrue.

> **Remarque**
>
> Vous pouvez afficher les fichiers journaux de la plateforme de BI dans n'importe quel éditeur de texte.

29.2 Niveaux du journal de suivi

Les niveaux du journal de suivi suivants sont disponibles pour les composants de la plateforme de BI :

Niveau	Description
Non spécifié	Le niveau du journal de suivi est spécifié par d'autres moyens, (généralement un fichier `.ini`).
Aucun	Aucun suivi n'est effectué.
Bas	Le filtre de journal de suivi autorise les messages d'erreur de journalisation tout en ignorant les messages

Niveau	Description
	d'avertissement et d'état. Les messages d'état importants sont journalisés pour des messages de démarrage ou d'arrêt d'un composant, ou pour les messages de requête de début et de fin. Ce niveau n'est pas recommandé pour les besoins du débogage.
Moyen	Le filtre du journal de suivi est défini pour inclure les messages d'erreur, d'avertissement et la plupart des messages d'état. Les messages d'état moins importants ou très détaillés sont refusés. Ce niveau n'est pas assez détaillé pour les besoins du débogage.
Elevé	Aucun message n'est filtré. Ce niveau est recommandé pour les besoins du débogage. **⚠ Attention** Ce niveau du journal de suivi affecte considérablement les ressources du système, en augmentant l'utilisation de l'unité centrale et la consommation de l'espace de stockage.

29.3 Configuration du suivi pour les serveurs

Un message de journal est un enregistrement permanent des événements et statuts d'un système logiciel. Les traces d'un déploiement de la plateforme de BI surveillé sont écrites dans un fichier journal `.glf` particulier et stockées dans le répertoire de journalisation.

- Sous Windows, l'emplacement par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\logging`
- Sous Unix, l'emplacement par défaut est `<REPINSTALL>/sap_bobj/logging`

Le nom du fichier journal `.glf` comprend un identificateur abrégé, le nom du serveur et un numéro de référence, par exemple, `aps_monsia.ServeurTraitementAdaptatif_trace.000012.glf`. Un nouveau fichier journal de suivi est créé pour le serveur surveillé lorsque la taille du fichier journal approche le seuil de dix mégaoctets. En outre, cinq fichiers journaux sont gérés à la fois. Quand de nouveaux fichiers journaux sont créés, les anciens sont supprimés.

Vous pouvez calibrer la gravité et l'importance des traces collectées dans le fichier journal en définissant le niveau du journal de suivi d'un serveur ou d'un groupe de serveurs particulier.

> **ⓘ Remarque**
>
> Pour modifier le niveau du journal de suivi de serveurs ou groupes de serveurs spécifiques, utilisez le service du journal de suivi dans la CMC (Central Management Console). Pour modifier les autres paramètres, changez manuellement le niveau du journal de suivi et les autres paramètres dans le fichier `BO_trace.ini`.

29.3.1 Pour définir le niveau de journalisation dans la CMC

Vous pouvez modifier le niveau du journal de suivi d'un serveur sans affecter les autres paramètres de suivi.

1. Dans la zone *Serveurs* de la CMC, accédez à un serveur.
   - Sélectionnez un serveur d'une catégorie spécifique.
   - Cliquez sur *Liste des serveurs* dans le volet de navigation pour accéder à la liste complète des serveurs, puis sélectionnez-en un.
2. Cliquez avec le bouton droit sur ce serveur et sélectionnez *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
3. Dans la zone *Service de journal de suivi*, sélectionnez le paramètre souhaité dans la liste *Niveau de journalisation*.
4. Cliquez sur *Enregistrer et fermer*.

Le nouveau niveau du journal de suivi s'applique immédiatement.

Pour spécifier un répertoire de sortie différent pour les fichiers journaux, incluez le paramètre `-loggingPath <répertoire_cible>` dans la zone *Paramètres de ligne de commande*. Redémarrez le serveur pour que ce paramètre s'applique.

Informations associées

Niveaux du journal de suivi [page 709]

29.3.2 Pour définir le niveau de journalisation de plusieurs serveurs dans la CMC

1. Dans la zone *Serveurs* de la CMC, accédez à plusieurs serveurs.
   - Sélectionnez les serveurs d'une catégorie particulière.
   - Cliquez sur *Liste des serveurs* dans le volet de navigation pour accéder à la liste complète des serveurs. Maintenez la touche `Ctrl` enfoncée et cliquez sur plusieurs serveurs pour les sélectionner.
2. Cliquez avec le bouton droit sur les serveurs sélectionnés, puis sélectionnez *Modifier les services communs*.
   La boîte de dialogue *Modifier les services communs* s'affiche.
3. Dans la zone *Service de journal de suivi*, sélectionnez le paramètre souhaité dans la liste *Niveau de journalisation*.
4. Cliquez sur *OK*.

Le nouveau niveau du journal de suivi s'applique immédiatement.

Pour spécifier un répertoire de sortie différent pour les fichiers journaux, incluez le paramètre `-loggingPath <répertoire_cible>` dans la zone *Paramètres de ligne de commande*. Redémarrez le serveur pour que ce paramètre s'applique.

Informations associées

Niveaux du journal de suivi [page 709]

29.3.3 Pour configurer le suivi de serveur à l'aide du fichier Bo_trace.ini

Le fichier `BO_trace.ini` enregistre uniquement les erreurs et les assertions par défaut.

1. Ouvrez le fichier `BO_trace.ini`.
   - Sous Windows, l'emplacement par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf`
   - Sous Unix, l'emplacement par défaut est `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/`
2. Retirez les marques de commentaire des lignes de la section « Trace Syntax and Setting ».
3. Modifiez les paramètres de suivi du serveur. Les paramètres suivants sont utilisés pour configurer le suivi des serveurs :

Nom du paramètre	Valeurs possibles	Description
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Détermine la gravité des messages du journal. La gravité par défaut est **`log_error`**. La gravité du journal respecte une hiérarchie, avec **`log_information`** au niveau supérieur et **`log_none`** au niveau inférieur. Lorsque vous définissez un niveau de gravité, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité sur **`log_warning`**, les messages comprenant **`log_warning`**, **`log_error`** et **`log_fatal`** seront écrits dans le fichier journal. **Remarque** **`log_information`** et **`log_warning`** peuvent être abrégés en **`log_info`** et **`log_warn`**.

Nom du paramètre	Valeurs possibles	Description
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Détermine la gravité des messages de suivi. La gravité par défaut du suivi est `trace_error`. La gravité du suivi respecte une hiérarchie, avec `trace_debug` au niveau supérieur et `trace_none` au niveau inférieur. Lorsque vous définissez un niveau de gravité du suivi, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité du suivi sur `trace_path`, les messages incluant `trace_path`, `trace_information` et `trace_error` seront écrits dans le fichier journal. **Remarque** `trace_information` peut être abrégé en `trace_info`.

4. Enregistrez, puis fermez le fichier `BO_trace.ini`.

Le fichier `BO_trace.ini` est lu fréquemment. Les modifications du fichier `BO_trace.ini` s'appliquent dans les cinq minutes suivant leur enregistrement. Si vous redémarrez le CMS, les modifications du fichier `BO_trace.ini` s'appliquent immédiatement.

Exemple

Fichier `BO_trace.ini`

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

29.3.3.1 Pour configurer le suivi d'un serveur spécifique

Le fichier `BO_trace.ini` spécifie les paramètres de suivi des serveurs de la plateforme de BI. Les paramètres affectent tous les serveurs gérés. Les administrateurs peuvent utiliser le fichier `BO_trace.ini` afin de définir des paramètres de suivi particuliers pour un serveur donné.

> **Attention**
>
> Les nouveaux paramètres de niveau de journalisation du suivi spécifiés dans la CMC pour un serveur spécifique remplaceront ceux du fichier `BO_trace.ini`.

1. Ouvrez le fichier `BO_trace.ini`.
   - Sous Windows, l'emplacement par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf`
   - Sous Unix, l'emplacement par défaut est `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/`
2. Utilisez une instruction `if` pour spécifier les paramètres de suivi d'un serveur spécifique. Par exemple :

```
if (process == "aps_MySIA.ProcessingServer") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

> → Conseil
>
> Le processus doit être spécifié pour que le paramètre de suivi s'applique à un serveur spécifique.

3. Enregistrez, puis fermez le fichier `BO_trace.ini`.

Les paramètres modifiés s'appliquent dans les cinq minutes.

29.4 Configuration du suivi pour les applications Web

Les traces d'un déploiement de la plateforme de BI surveillé sont écrites dans un fichier journal `.glf` spécifique et stockées dans un répertoire de l'ordinateur qui héberge le dossier des applications Web.

- Sur Windows, l'emplacement par défaut est `C:\Windows\System32\config\systemprofile\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` Par exemple, `C:\Windows\System32\config\systemprofile\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- Sous Unix, l'emplacement par défaut est `$userHome/SBOPWebapp_<APPLICATION>_<ADRESSEIP>_<PORT>/` Par exemple, `$userHome/AppWebSBOP_CMC_192.0.2.0_8080/`

Par défaut, le niveau du journal de suivi des applications Web dans la CMC est défini sur *Non spécifié*. Les paramètres du journal des événements sont disponibles pour les applications suivantes dans la CMC :

- Central Management Console
- Zone de lancement BI
- Open Document
- Service Web

> ⓘ Remarque
>
> Pour modifier le niveau du journal de suivi de serveurs ou groupes de serveurs spécifiques, utilisez le service du journal de suivi dans la CMC (Central Management Console). Pour modifier les autres paramètres, changez manuellement le niveau du journal de suivi et les autres paramètres dans le fichier `BO_trace.ini`. Ce fichier est déployé avec les fichiers `BOE.war` et `dswsbobje.war` sur le serveur d'applications Web.

Avant de configurer le fichier `BO_trace.ini`, vous devez utiliser l'outil WDeploy pour annuler le déploiement des applications Web existantes de votre serveur d'applications Web. Après configuration du fichier

`BO_trace.ini`, il doit être redéployé avec les applications Web sur le serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour préparer, déployer et annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

29.4.1 Définition du niveau de journalisation de suivi des applications Web dans la CMC

Pour suivre d'autres applications Web, vous devez configurer manuellement le fichier `BO_trace.ini` correspondant.

1. Dans la zone *Applications* de la CMC, faites un clic droit sur une application et sélectionnez *Paramètres du journal de suivi*.

   > **Remarque**
   >
   > Ces applications comportent des paramètres de journal de suivi : zone de lancement BI façon Fiori, CMC, Open Document, Gestion des promotions, Gestion des versions, Différence visuelle et Service Web.

   La boîte de dialogue *Paramètres du journal de suivi* s'affiche.
2. Sélectionnez un paramètre dans la liste *Niveau de journalisation*.
3. Cliquez sur *Enregistrer et fermer*.
4. Redémarrez le serveur d'applications Web.

Le nouveau niveau du journal de suivi prend effet après la prochaine connexion à l'application Web.

Informations associées

Niveaux du journal de suivi [page 709]

29.4.2 Configuration des paramètre de suivi de serveur à l'aide du fichier `BO_trace.ini`

Le fichier `BO_trace.ini` est déployé avec les fichiers `BOE` et `dswsbobje .war` sur le serveur d'applications Web. Vous pouvez utiliser le fichier `BO_trace.ini` pour spécifier des paramètres de suivi pour les applications Web de la plateforme de BI. Comme ce fichier n'est pas toujours accessible, vous devez annuler le déploiement des applications Web concernées sur le serveur d'applications Web.

1. Utilisez WDeploy pour annuler le déploiement de l'application Web sur votre serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.
   - Si vous utilisez le serveur d'applications Web Tomcat fourni avec l'installation de la plateforme de BI, il n'est pas nécessaire d'annuler le déploiement des applications Web. Vous pouvez modifier les fichiers directement.

- Le fichier de configuration de suivi pour le fichier `BOE.war` est disponible sous : `<REPINSTALL>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
- Le fichier de configuration de suivi pour le fichier `dswsbobje.war` est disponible sous : `<REPINSTALL>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

> **Remarque**
>
> Si vous utilisez le serveur d'applications Web Tomcat fourni, ignorez l'étape 2.

2. Accédez à une version prédéployée du fichier `BO_trace.ini` :
   - L'emplacement par défaut d'une version prédéployée du fichier de configuration du fichier `BOE.war` est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - L'emplacement par défaut d'une version prédéployée du fichier de configuration du fichier `dswsbobje.war` est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Ouvrez le fichier `BO_trace.ini`.
   - Sous Windows, l'emplacement par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf`
   - Sous Unix, l'emplacement par défaut est `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/`
4. Modifiez les paramètres de suivi du serveur. Les paramètres suivants sont utilisés pour configurer le suivi des serveurs :

Nom du paramètre	Valeurs possibles	Description
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Détermine la gravité des messages du journal. La gravité par défaut est **`log_error`**. La gravité du journal respecte une hiérarchie, avec **`log_information`** au niveau supérieur et **`log_none`** au niveau inférieur. Lorsque vous définissez un niveau de gravité, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité sur **`log_warning`**, les messages comprenant **`log_warning`**, **`log_error`** et **`log_fatal`** seront écrits dans le fichier journal. **Remarque** **`log_information`** et **`log_warning`** peuvent être

Nom du paramètre	Valeurs possibles	Description
		abrégés en `log_info` et `log_warn`.
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Détermine la gravité des messages de suivi. La gravité par défaut du suivi est `trace_error`. La gravité du suivi respecte une hiérarchie, avec `trace_debug` au niveau supérieur et `trace_none` au niveau inférieur. Lorsque vous définissez un niveau de gravité du suivi, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité du suivi sur `trace_path`, les messages incluant `trace_path`, `trace_info` et `trace_error` seront écrits dans le fichier journal. ⓘ Remarque `trace_information` peut être abrégé en `trace_info`.

5. Enregistrez, puis fermez le fichier `BO_trace.ini`.
6. Utilisez Wdeploy pour déployer le fichier `.war` sur l'ordinateur qui héberge le serveur d'applications Web.

Les paramètres de suivi modifiés s'appliquent lors de la prochaine connexion aux applications Web.

29.4.2.1 Pour configurer le suivi d'une application Web donnée

Le fichier `BO_trace.ini` est déployé avec les fichiers WAR `BOE` et `dswsbobje .war` sur votre serveur d'applications Web. Vous pouvez utiliser le fichier `BO_trace.ini` pour spécifier des paramètres de suivi pour les applications Web de la plateforme de BI. Comme ce fichier n'est pas toujours accessible, vous devez annuler le déploiement des applications Web concernées sur le serveur d'applications Web. Applications Web et fichiers `.war` associés :

Application Web	Fichier WAR	Emplacement prédéployé
Central Management Console	`BOE.war`	`<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles`

Application Web	Fichier WAR	Emplacement prédéployé
		\webapps\BOE\WEB-INF\TraceLog
Zone de lancement BI	BOE.war	<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Open Document	BOE.war	<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Service Web	dswsbobje.war	<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf

1. Utilisez WDeploy pour annuler le déploiement de l'application Web sur votre serveur d'applications Web. Pour en savoir plus sur l'utilisation de WDeploy pour annuler le déploiement d'applications Web, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.
   - Si vous utilisez le serveur d'applications Web Tomcat fourni avec l'installation de la plateforme de BI, il n'est pas nécessaire d'annuler le déploiement des applications Web. Vous pouvez modifier le fichier directement.
     - Le fichier de configuration de suivi pour le fichier `BOE.war` est disponible sous : `<REPINSTALL>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - Le fichier de configuration de suivi pour le fichier `dswsbobje.war` est disponible sous : `<REPINSTALL>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

   > **Remarque**
   >
   > Si vous utilisez le serveur d'applications Web Tomcat fourni, ignorez l'étape 2.

2. Accédez à une version prédéployée du fichier `BO_trace.ini` :
   - L'emplacement par défaut d'une version prédéployée du fichier de configuration du fichier `BOE.war` est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - L'emplacement par défaut d'une version prédéployée du fichier de configuration du fichier `dswsbobje.war` est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Ouvrez le fichier `BO_trace.ini`.
   - Sous Windows, l'emplacement par défaut est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf`
   - Sous Unix, l'emplacement par défaut est `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/`

4. Utilisez une instruction `if` pour spécifier les paramètres de suivi d'une application Web spécifique. Par exemple :

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

Le processus doit être spécifié pour que le paramètre de suivi s'applique à une application Web spécifique. Les applications Web suivantes sont disponibles après l'installation initiale :

Application Web	Nom de l'appareil
Zone de lancement BI	`WebApp_BIlaunchpad`
Central Management Server	`WebApp_CMC`
OpenDocument	`WebApp_OpenDocument`

Les paramètres suivants sont utilisés pour configurer le suivi du serveur d'applications Web :

Nom du paramètre	Valeurs possibles	Description
`sap_log_level`	`log_information` `log_warning` `log_error` `log_fatal` `log_none`	Détermine la gravité des messages du journal. La gravité par défaut est `log_error`. La gravité du journal respecte une hiérarchie, avec `log_information` au niveau supérieur et `log_none` au niveau inférieur. Lorsque vous définissez un niveau de gravité, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité sur `log_warning`, les messages comprenant `log_warning`, `log_error` et `log_fatal` seront écrits dans le fichier journal. **Remarque** `log_information` et `log_warning` peuvent être abrégés en `log_info` et `log_warn`.
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Détermine la gravité des messages de suivi. La gravité par défaut du suivi est `trace_error`.

Nom du paramètre	Valeurs possibles	Description
		La gravité du suivi respecte une hiérarchie, avec **trace_debug** au niveau supérieur et **trace_none** au niveau inférieur. Lorsque vous définissez un niveau de gravité du suivi, tous les messages de ce niveau et de niveau inférieur sont affichés. Par exemple, si vous définissez la gravité du suivi sur **trace_path**, les messages incluant **trace_path**, **trace_info** et **trace_error** seront écrits dans le fichier journal. **Remarque** **trace_information** peut être abrégé en **trace_info**.

5. Enregistrez, puis fermez le fichier `BO_trace.ini`.
6. Utilisez Wdeploy pour déployer le fichier `.war` sur l'ordinateur hébergeant le serveur d'applications Web.

29.5 Configuration du traçage pour les applications clientes de la plateforme de BI

Le traçage peut être activé sur les clients suivants :

- Outil de conception d'univers
- Outil de conception d'information
- Web Intelligence Rich Client

Vous pouvez configurer le traçage pour ces composants en modifiant les fichiers .ini pour chaque type de client : Ces fichiers .ini fonctionnent de la même façon que le fichier BO_trace.ini décrit plus loin dans ce chapitre. Voir Pour configurer le suivi de serveur à l'aide du fichier Bo_trace.ini [page 1091] pour les détails de modification du fichier .ini.

Les fichiers doivent se trouver dans les répertoires de travail configurés pour ces applications (`<REPINSTALL>\SAP BusinessObjects` par défaut). S'ils n'existent pas, vous devez les créer. Les fichiers ont les noms suivants

- Outil de conception d'univers : `designer_trace.ini`.
- Outil de conception d'information : `BO_Trace.ini`
- Web Intelligence Rich Client : `WebIRichClient_trace.ini`

Pour en savoir plus, voir la documentation de ces produits.

29.6 Configuration du suivi des messages d'erreur

Vous pouvez activer le suivi pour certaines applications, pour SAP BusinessObjects Web Intelligence par exemple, afin de générer des fichiers journaux qui contiennent des informations détaillées concernant les messages d'erreur renvoyés par l'application.

> **Remarque**
>
> Ces fichiers journaux sont destinés aux ingénieurs du service de support SAP. Leur format est JSON.

Pour activer les fichiers journaux contenant les informations détaillées sur les messages d'erreur, modifiez le fichier suivant dans l'installation SAP BusinessObjects BI : `extended_info.properties`.

29.7 Pour activer des fichiers journaux contenant les informations détaillées sur les messages d'erreur

Vous pouvez récupérer les informations détaillées sur un message d'erreur renvoyé par une application. Pour cela, vous devez activer les fichiers journaux contenant les informations détaillées sur les messages d'erreur.

> **Remarque**
>
> Dans SAP BusinessObjects BI Suite version 4.2 SP5, cette fonctionnalité est prise en charge uniquement pour SAP BusinessObjects Web Intelligence.

1. Ouvrez le fichier ci-dessous dans votre installation SAP BusinessObjects BI : `extended_info.properties`.

   Par défaut, ce fichier réside à l'emplacement suivant :
   - Sous Windows : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - Sous UNIX : `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Définissez les paramètres comme suit :

Paramètre	Valeurs possibles	Description
`output.format`	• Json • none	Contrôle le format des fichiers générés. **Remarque** Si vous définissez le format sur none, aucun fichier n'est généré.

Paramètre	Valeurs possibles	Description
`output.size`	`<size><unit>` où `<size>` est un entier positif et `<unit>` correspond à "g" pour gigaoctets ou à "m" pour mégaoctets. **Remarque** Par défaut, cette valeur est exprimée en kilo-octets.	La taille totale de tous les fichiers qu'une application peut générer. Les fichiers anciens sont supprimés lorsque cette taille est dépassée.

Les fichiers journaux sont générés dans le même dossier que les fichiers de trace. Par défaut, ce fichier réside à l'emplacement suivant :

- Sous Windows : `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`
- Sous UNIX : `<INSTALLDIR>/sap_bobj/logging/`

Les fichiers sont nommés `<application_name>_<error_id>_exinfo.<format>`.

Le nom d'application est le nom de l'application qui a généré l'erreur. L'ID d'erreur est généré de manière aléatoire. Le format de fichier est le format spécifié dans le fichier de configuration.

> **Remarque**
>
> La seule extension de fichier possible est `.json`.

Un fichier journal distinct est généré pour chaque message renvoyé par l'application spécifiée.

30 Intégration à SAP Solution Manager

30.1 Présentation de l'intégration

Des fonctionnalités de modalités de prise en charge ont été ajoutées à la plateforme de BI pour permettre l'intégration à SAP Solution Manager. Les composants de SAP Solution Manager™ peuvent être utilisés pour fournir une prise en charge de votre déploiement de la plateforme de BI :

- Répertoire du paysage de solution
- Solution Manager Diagnostics
- Introscope par CA Wily
- Passeport SAP

> **Remarque**
>
> Pour accéder au portail d'assistance SAP pour SAP BusinessObjects, accédez à : https://support.sap.com/home.html

30.2 Liste de vérification de l'intégration SAP Solution Manager

Le tableau suivant résume les composants nécessaires à l'activation de SAP Solution Manager pour prendre en charge la plateforme de BI.

Prise en charge de SAP Solution Manager	Nécessaire pour la plateforme de BI
enregistrement SLD	• SAPHOSTAGENT doit être installé pour permettre l'enregistrement des serveurs de la plateforme de BI. **Remarque** Le programme d'installation de la plateforme de BI enregistrera automatiquement les serveurs si SAPHOSTAGENT est déjà installé. • Doit créer un fichier connect.key pour le fournisseur de données créant des rapports sur les serveurs clés. • (Facultatif) Pour l'enregistrement SLD avec WebSphere 6.1 ou 7, l'outil d'enregistrement SLDREG doit être installé sur chaque serveur d'applications Web WebSphere. Pour en savoir plus, voir la note SAP 1482727. • (Facultatif) Pour l'enregistrement SLD avec SAP NetWeaver 7.2, installez SLDREG sur chaque hôte NetWeaver. Pour en savoir plus, voir la note SAP 1018839. • (Facultatif) Pour l'enregistrement SLD avec Apache Tomcat, SLDREG doit être installé sur chaque serveur Tomcat. Pour en savoir plus, voir la note SAP 1508421.
Intégration SMD	• Doit télécharger et installer l'agent SMD (DIAGNOSTICS.AGENT) sur tous les hôtes des serveurs de la plateforme de BI. • Le compte utilisateur SMAdmin doit être activé sur la plateforme de BI.
Instrumentation des performances	• L'agent Introscope doit être configuré pour se connecter à Enterprise Manager. Utilisez le programme d'installation de la plateforme de BI ou des espaces réservés de nœuds de la CMC pour configurer les connexions. • L'agent SMD doit être installé. • La plateforme de BI doit être configurée pour se connecter à l'agent SMD. Utilisez le programme d'installation de la plateforme de BI ou des espaces réservés de nœuds de la CMC pour configurer les connexions.
Passeport SAP	• Vous devez télécharger et installer l'outil client Passeport SAP.

30.3 Gestion de l'enregistrement du répertoire du paysage système

30.3.1 Enregistrement de la plateforme de BI dans le paysage système

Le répertoire du paysage système (SLD) est un référentiel central des informations de paysage système pertinentes pour la gestion du cycle de vie du logiciel. Le System Landscape Directory contient une description de l'infrastructure système : les composants système et logiciels actuellement installés. Les fournisseurs de données du répertoire du paysage système enregistrent les systèmes sur le serveur SLD et gardent les informations à jour. Les applications de gestion et professionnelles accèdent aux informations stockées dans le répertoire du paysage système pour accomplir des tâches dans un environnement de calcul collaboratif.

Le fournisseur de données du répertoire du paysage système (SLD-DS) est l'application responsable de l'enregistrement des serveurs de la plateforme de BI dans le serveur SLD. Un fournisseur de données spécifique est disponible pour chaque installation de la plateforme afin de créer des rapports sur les composants suivants :

- Serveurs de la plateforme de BI
- Applications et services Web hébergés sur le serveur d'applications Web WebSphere.

> **Remarque**
>
> SAP NetWeaver dispose d'un fournisseur de données du répertoire du paysage système intégré qui enregistre le serveur d'applications NetWeaver de même que les services et applications Web hébergés. Ce fournisseur de données du répertoire du paysage système est pertinent pour les déploiements la plateforme de BI intégrés à un environnement SAP NetWeaver.

Le fournisseur de données du répertoire du paysage système qui crée des rapports sur les serveurs de la plateforme de BI nécessite l'installation et la configuration du programme SLDREG. Le programme SLDREG est installé en même temps que l'outil SAPHOSTAGENT. Pour en savoir plus sur l'accès à SAPHOSTAGENT et son installation, voir la section Préparation du *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*. Une fois installé SLDREG, vous devez créer un fichier `connect.key` pour lui permettre de se connecter au serveur SLD.

Pour en savoir plus sur le mode de configuration du fournisseur de données spécifique pour WebSphere, voir le *Guide de déploiement d'applications Web*.

Au cours de l'installation de la plateforme de BI, les informations requises pour l'enregistrement de la plateforme de BI sont stockées dans un fichier de configuration. Le fichier contient des informations utilisées par le fournisseur de données du répertoire du paysage système pour se connecter à la base de données de la plateforme de BI.

30.3.1.1 Pour créer un fichier connect.key pour le fournisseur de données du répertoire du paysage système

Avant de créer un fichier `connect.key` pour le fournisseur de données du répertoire du paysage système, vous devez télécharger et installer le SAPHOSTAGENT. Voir la section Préparation du *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence* pour en savoir plus.

> **Remarque**
>
> Le fichier `connect.key` est nécessaire pour l'enregistrement SLD avec le fournisseur de données créant des rapports sur les serveurs de la plateforme de BI.

1. Ouvrez une console de ligne de commande.
2. Naviguez jusqu'au chemin d'installation SAPHOSTAGENT par défaut.
   - Sous Windows : `Program Files\SAP\hostctrl\exe`
   - Sous Unix : `/usr/sap/hostctrl/exe`
3. Exécutez la commande suivante :

   ```
   sldreg -configure connect.key
   ```

4. Saisissez les détails de configuration suivants
    - Nom d'utilisateur
    - Mot de passe
    - Hôte
    - Numéro de port
    - Spécifiez l'utilisation HTTP

L'outil `sldreg` crée un fichier connect.key qui va être automatiquement utilisé par le fournisseur de données pour pousser les informations vers le serveur SLD.

30.3.2 Déclenchement de l'enregistrement SLD

Le processus d'enregistrement SLD est invoqué par le fournisseur de données créant des rapports sur les serveurs principaux de la plateforme de BI dans les scénarios suivants :

- Un nœud de serveur sur votre déploiement de la plateforme de BI est redémarré.
- Un nouveau serveur ou un nœud est ajouté au déploiement.
- Un serveur ou un nœud est supprimé.

> **Remarque**
>
> Si un serveur ou un nœud est supprimé, le processus d'enregistrement du répertoire du paysage système ne modifie pas le contenu du serveur SLD. Pour mettre à jour le serveur SLD lorsqu'un serveur ou un nœud est supprimé, supprimez le système du SLD et renvoyez-le en redémarrant la plateforme de BI.

Le fournisseur de données pour l'enregistrement SLD WebSphere peut être invoqué manuellement ou défini pour s'exécuter à intervalles réguliers, toutes les 24 heures, par exemple. Pour en savoir plus sur la configuration de ce fournisseur de données, voir la note SAP 482727.

30.3.3 Nettoyage du serveur SLD avant une installation de correctif

Les données des versions précédentes de la plateforme de BI s'accumulent dans le serveur SLD après une installation de correctif et complique le diagnostic du produit via SAP Solution Manager. Pour éviter un tel problème, suivez les étapes mentionnées ci-dessous avant de commencer l'installation d'un correctif :

> **Remarque**
>
> La fonctionnalité est disponible pour les versions 4.2 SP3 et ultérieures.

1. Ouvrez `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Exécutez le fichier batch bobjsldds.bat avec les paramètres de nettoyage (`-clean`).

> **Remarque**
>
> Le système crée un fichier XML (avec les paramètres prédéfinis) qui est transmis au serveur SDL en vue du nettoyage. Le nettoyage prend effet après avoir redémarrer le SIA.

30.3.4 Connexion de la connectivité SLD

Fichier de configuration du fournisseur de données

Un fichier de configuration utilisé pour l'enregistrement SLD est créé pour les déploiements de la plateforme de BI. Le fichier `sldparserconfig.properties` est situé dans le répertoire suivant : `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

Connexion de la connectivité SLD

La connectivité entre le serveur SLD et le fournisseur de données sur le déploiement de la plateforme de BI est contrôlé par le biais de l'outil `sldreg` et du fichier `connect.key`.

> **Remarque**
>
> Le nom de fichier journal est spécifié sous forme de propriété dans le fichier `sldparserconfig.properties`.

Le fichier journal pour le fournisseur de données SLD créant des rapports sur les serveurs principaux de la plateforme de BI est situé par défaut à l'emplacement suivant : `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. Le fichier d'archives est écrasé lors de chaque exécution du fournisseur de données.

Les fichiers journaux `sldreg` sont situés par défaut à l'emplacement suivant : `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. Les noms des fichiers journaux sldreg ne peuvent pas être modifiés et utilisent le format suivant : `sldreg_<Horodatage>.log`.

Un nouveau fichier journal est créé à chaque appel de sldreg par le fournisseur de données.

30.3.5 Nom d'hôte virtuel

Lorsque *Server Intelligence Agent* est redémarré, un fichier de fournisseur de données est généré pour chaque nœud. Le fichier est ajouté à System Landscape Directory en vue de son utilisation ultérieure par SAP Solution Manager. Dans la plateforme de Business Intelligence 4.2 Support Package 4 et versions ultérieures, le nom d'hôte physique était ajouté au fichier de fournisseur de données. Dans la plateforme de Business Intelligence 4.2 Support Package 5, vous pouvez définir un nom d'hôte virtuel dans le fichier *sldparserconfig.properties* afin de garantir que le fichier de fournisseur de données utilise ce nom d'hôte virtuel.

> **Remarque**
>
> Par défaut, le fichier de fournisseur de données récupère le nom d'hôte physique si le fichier "sldparserconfig.properties" ne contient aucun nom d'hôte virtuel.

Suivez les étapes ci-dessous pour ajouter le nom d'hôte virtuel dans le fichier sldparserconfig.properties :

1. Ouvrez `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Modifiez le fichier sldparserconfig.properties.
3. Ajoutez le paramètre suivant : `virtualHostName = <Virtual Hostname>`.
4. Enregistrez le fichier.
5. Redémarrez *Server Intelligence Agent* afin de vous assurer que les modifications sont utilisées par le fichier de fournisseur de données.

> **Remarque**
>
> Les modifications peuvent également être utilisées via l'exécution de la commande suivante :
>
> Sous Windows : `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` sous `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
>
> Sous Unix : `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` sous `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds`.

30.4 Gestion des agents Solution Manager Diagnostics

30.4.1 Présentation de Solution Manager Diagnostics (SMD)

Le composant Solution Manager Diagnostics (SMD) de SAP Solution Manager fournit toutes les fonctionnalités pour analyser et surveiller de manière centrale un paysage système complet. La plateforme de BI peut être surveillée par le serveur SMD si un agent SMD est installé. L'agent SMD (`DIAGNOSTICS.AGENT`) réunit pour le SMD des informations qui peuvent ensuite être utilisées pour l'analyse de causes racine. Les informations recueillies et envoyées au serveur SMD comprennent les configurations de serveurs principaux et l'emplacement des fichiers journaux de serveurs.

30.4.2 Utilisation des agents SMD

La plateforme de BI n'installe pas l'agent SMD. L'agent `DIAGNOSTICS.AGENT` est peut être téléchargé depuis l'emplacement suivant : https://support.sap.com/swdc.

Des informations sur l'installation et la configuration de l'agent sont disponibles à l'adresse : http://service.sap.com/diagnostics

Instructions pour l'utilisation de l'agent SMD

Les instructions d'utilisation des agents SMD pour surveiller la plateforme de BI sont détaillées ci-après :

- Ordre d'installation du système et de l'agent surveillés n'importe pas. Vous pouvez choisir d'installer l'agent SMD avant ou après l'installation et le déploiement de la plateforme de BI.
- Lors de l'installation d'un agent SMD, prenez note du nom d'hôte et du port d'écoute. Ils sont essentiels pour configurer la plateforme de BI en tant que système surveillé. Si vous avez installé l'agent avant le système surveillé, vous pouvez fournir les informations de configuration durant la configuration d'installation de la plateforme de BI. Ces informations peuvent également être fournies ultérieurement par le biais d'espaces réservés pour les nœuds de la CMC de votre déploiement.
- Si les serveurs principaux sont déployés sur un système distribué, vous devez installer un agent SMD sur chaque ordinateur hébergeant un serveur principal.
- En ce qui concerne l'instrumentation de performances de serveurs non Java, l'agent SMD est nécessaire.
- Vous devez activer le compte utilisateur SMAdmin pour permettre au serveur SMD d'accéder au CMS.

30.4.3 Compte utilisateur SMAdmin

Chaque déploiement de la plateforme de BI dispose d'un compte utilisateur créé pour faciliter l'intégration SMD. Ce compte en lecture seule est utilisé par le serveur SMD pour se connecter au CMS et regrouper la configuration serveur et d'autres informations sur le déploiement.

Le compte SMAdmin est désactivé par défaut.

30.4.3.1 Pour activer le compte SMAdmin

1. Dans la zone de gestion des *Utilisateurs et groupes* de la CMC, sélectionnez le groupe *Liste des utilisateurs*. La liste des utilisateurs s'affiche.
2. Cherchez le compte utilisateur *SMAdmin*.
3. Cliquez sur *Gérer* > *Propriétés*.
   La boîte de dialogue *Propriétés* s'affiche.
4. Désactivez la case *Le compte est désactivé*.
5. Cliquez sur *Enregistrer et fermer*.

30.5 Gestion de l'instrumentation des performances

30.5.1 Instrumentation de performances pour la plateforme de BI

Vous pouvez utiliser CA Wily Introscope dans le cadre de SAP Solution Manager pour mesurer l'instrumentation de performances de la plateforme de BI. Lors de l'installation de la plateforme, les ressources suivantes sont fournies pour votre déploiement

- Agent Introscope : Les agents Introscope recueillent les indicateurs de performances des serveurs principaux Java de la plateforme de BI. Les agents recueillent également des informations auprès de l'environnement de calcul environnant. Les agents rapportent ensuite ces métriques à Enterprise Manager.
- Fichiers fournis pour faciliter le processus d'instrumentation. Un jeu de fichiers est fourni pour l'instrumentation des serveurs non Java et un autre jeu de fichiers pour l'instrumentation des serveurs Java. Du côté de SAP Solution Manager, le composant Enterprise Manager (EM) est requis. EM fait office de référentiel central pour toutes les données de performances Introscope et métriques recueillies dans un environnement d'application. EM traite les données de performances des processus et les met à disposition des utilisateurs pour la surveillance de production et le diagnostic.

30.5.2 Configuration de l'instrumentation de performances pour la plateforme de BI

Il existe deux manières de configurer l'instrumentation de performances pour les workflows s'exécutant sur les serveurs principaux de la plateforme de BI.

1. Au cours de la configuration d'installation pour la plateforme de BI. Vous devrez connaître le nom d'hôte et le port d'écoute pour l'agent SMD. Pour en savoir plus, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*. Si vous choisissez cette option, l'instrumentation sera exécutée par défaut une fois que vous aurez terminé le déploiement du système surveillé.
2. Après avoir installé la plateforme de BI, vous pouvez fournir les informations de configuration de l'agent SMD au moyen des espaces réservés dans les propriétés de nœud de la CMC (Central Management Console).

> **Remarque**
>
> Pour l'instrumentation de workflows sur des serveurs non Java, vous devez avoir installé l'agent SMD (`DIAGNOSTICS.AGENT`).

Informations associées

Utilisation des agents SMD [page 1107]

30.5.2.1 Pour configurer des nœuds pour l'instrumentation

Utilisez les instructions suivantes si vous n'avez pas fourni les informations de configuration de l'agent SMD et Enterprise Manager au cours de la configuration d'installation de la plateforme de BI.

1. Accédez à la zone *Serveurs* de la CMC.
2. Dans le volet de navigation, cliquez sur *Nœuds*.
   Toutes les nœuds disponibles s'affichent.
3. Cliquez avec le bouton droit sur le nœud sur lequel vous voulez effectuer une instrumentation et sélectionnez *Espaces réservés*.
   La boîte de dialogue Espaces réservés s'affiche.
4. Modifiez la valeur des espaces réservés suivants.

Espace réservé	Description
%IntroscopeAgentEnableInstrumentation%	Active ou désactive l'instrumentation sur les serveurs Java. A activer si vous avez fourni des détails de configuration pour Enterprise Manager au cours de la configuration d'installation. Affectez la valeur `true` pour activer l'instrumentation.
%IntroscopeAgentEnterpriseManagerHost%	Nom d'hôte de l'ordinateur sur lequel est installé Enterprise Manager.
%IntroscopeAgentEnterpriseManagerPort%	Port d'écoute utilisé par Enterprise Manager.
%IntroscopeAgentEnterpriseManagerTransport%	Protocole de communication utilisé par Enterprise Manager. Les protocoles pris en charge sont TCP, SSL, HTTP Tunnel et HTTPS.
%NCSInstrumentLevelThreshold%	Sert à définir le niveau d'instrumentation pour les serveurs non Java. Attribuez la valeur « 0 » pour désactiver l'instrumentation. Attribuez n'importe quelle valeur supérieure à « 0 » pour activer l'instrumentation.
%SMDAgentHost%	Nom d'hôte de l'ordinateur sur lequel est installé l'agent SMD (`DIAGNOSTICS.AGENT`).
%SMDAgentPort%	Port d'écoute utilisé par l'agent SMD.

5. Cliquez sur *Enregistrer et fermer*.
6. Redémarrez le nœud.

Une fois le nœud redémarré, les nouvelles valeurs fournies se propagent à tous les serveurs gérés.

30.5.3 Instrumentation de performances pour le niveau Web

Les données d'instrumentation pour les composants de niveau Web ne sont pas incluses à la plateforme de BI.

30.5.4 Fichiers journaux d'instrumentation

Une fois configuré votre déploiement de la plateforme de BI pour exécuter l'instrumentation, les messages sont consignés à des emplacements spécifiques. La consultation des fichiers journaux est un moyen de vérifier les statuts d'instrumentation.

En ce qui concerne l'instrumentation sur les serveurs principaux Java, un fichier journal est situé dans le répertoire suivant :`<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs` . Un fichier `.log` séparé est créé pour chaque processus Java. Le dossier contiendra également les fichiers `AutoProbe.log` qui spécifient quelles méthodes ont été chargées pour l'instrumentation.

Pour l'instrumentation sur les serveurs principaux non Java, les fichiers journaux sont situés dans le répertoire suivant : `<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/logging/`. Sous Unix, les fichiers sont situés dans le répertoire `<sap_bobj>\logging\`. Les fichiers journaux relatifs à l'instrumentation pour les serveurs non Java sont enregistrés en tant que fichiers `.trc`.

En ce qui concerne l'instrumentation sur les serveurs d'applications Web, un fichier journal est situé dans le répertoire suivant :`<REPINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Deux types de fichiers journaux apparaissent dans ce dossier : `Introscope.log` et `Autoprobe.log`.

30.6 Suivi avec le Passeport SAP

Outre le suivi des composants de la plateforme de BI comme les serveurs et applications Web, le mécanisme de suivi peut prendre en charge le suivi d'une action précise. Une analyse de suivi de bout en bout analyse les performances d'une seule transaction. La consolidation de toutes les informations de suivi d'une action précise permet au personnel de support technique de voir toutes les données de suivi sans être distrait par les informations de suivi liées à d'autres actions.

Pour en savoir plus, rendez-vous sur 1861180.

Passeport SAP

Le mécanisme prenant en charge le suivi de bout en bout de la plateforme de BI est un outil appelé Passeport SAP™. L'outil client Passeport SAP injecte un identificateur unique dans toutes les requêtes HTTP pour un workflow particulier et cet identificateur est transmis à tous les serveurs utilisés dans le workflow. Le personnel de support technique SAP peut réaliser un suivi de bout en bout pour le workflow en utilisant cet identificateur unique.

> **Remarque**
>
> Les niveaux du journal de suivi spécifiés dans la CMC et le fichier de configuration `BO_trace.ini` sont utilisés s'ils sont supérieurs aux niveaux spécifiés dans l'outil client SAP Passport : `SAPClientPlugin.exe`.

Vous pouvez trouver le Passeport dans les journaux pour les serveurs principaux, les journaux d'applications Web et de services Web.

L'outil client Passeport SAP n'est pas installé dans le cadre de la plateforme de BI. Pour accéder à l'outil et le télécharger, accédez à : https://support.sap.com/swdc.

31 Administration de la ligne de commande

31.1 Scripts UNIX

Cette section détaille chacun des outils d'administration et des scripts inclus avec la distribution Unix de la plateforme de BI. Cette section est fournie surtout à titre de référence. Des concepts et des procédures de configuration sont décrits plus en détail tout au long de ce guide.

> **Remarque**
>
> Seul l'utilisateur ayant installé la plateforme de BI dispose des droits d'exécution des scripts shell dans la plateforme de BI.

La distribution Unix de la plateforme de BI inclut un certain nombre de scripts qui, ensemble, vous offrent toutes les options de configuration disponibles dans la version Windows du CCM (Central Configuration Manager). Il existe un certain nombre d'autres scripts qui vous fournissent d'autres options spécifiques à UNIX ou vous servent de modèles pour vos propres scripts. Il existe également plusieurs scripts secondaires qui sont utilisés par la plateforme de BI. Chaque script est décrit ci-dessous et est accompagné d'options de ligne de commande, le cas échéant.

> **Remarque**
>
> Lors de la saisie de paramètres de la ligne de commande Unix, vous devez ignorer les caractères shell spéciaux. Par exemple, si le point d'exclamation « ! » est utilisé dans un mot de passe, vous devez ignorer le point d'exclamation ainsi : `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

31.1.1 Utilitaires de script

Cette section décrit les scripts administratifs qui vous aident à travailler avec la plateforme de BI sous UNIX. La suite de cette section décrit les concepts qui sous-tendent chacune des tâches que vous pouvez effectuer avec ces scripts. Cette section de référence vous fournit les principales options de ligne de commande et leurs arguments.

31.1.1.1 ccm.sh

Le script `ccm.sh` se trouve dans le répertoire `<REPINSTALL>/sap_bobj` de l'installation. Ce script vous fournit une version de ligne de commande du CCM (Central Configuration Manager). Cette section répertorie les options de ligne de commande et fournit quelques exemples.

> **Remarque**
>
> Les arguments entre crochets [ ] sont facultatifs.

> **Remarque**
>
> Si vous n'êtes pas sûr du nom d'un Server Intelligence Agent, vérifiez dans les propriétés Command du fichier `ccm.config` et utilisez la valeur affichée après l'option `-name`.

> **Remarque**
>
> Le script `ccm.sh` ne peut être lancé que par l'utilisateur qui a effectué l'installation de la plateforme de BI.

- Les arguments identifiés par **`<autres informations d'authentification>`** sont présentés dans le deuxième tableau.

Option CCM	Arguments valides	Description
`-help`	n/a	Afficher l'aide de la ligne de commande.
`-start`	`tout` ou **`<nomsia>`**	Démarrer chaque Server Intelligence Agent en tant que processus. L'option `tout` démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
`-stop`	`tout` ou **`<nomsia>`**	Arrête chaque Server Intelligence Agent en mettant fin à son ID de processus. L'option `tout` démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
`-restart`	`tout` ou **`<nomsia>`**	Arrêter chaque Server Intelligence Agent en mettant fin à son identification de processus ; chaque SIA est ensuite redémarré. L'option `tout` démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
`-managedstart`	**`<nom complet du serveur><[autres informations d'authentification]>`**	Démarrer un serveur.

Option CCM	Arguments valides	Description
-managedstop	**<nom complet du serveur><[autres informations d'authentification]>**	Arrêter un serveur.
-managedrestart	**<nom complet du serveur><[autres informations d'authentification]>**	Arrêter un serveur, puis redémarrer le serveur.
-managedforceterminate	**<nom complet du serveur><[autres informations d'authentification]>**	Arrête le serveur immédiatement sans terminer les requêtes en cours de traitement.
-enable	**<nom complet du serveur><[autres informations d'authentification]>**	Activer un serveur démarré pour qu'il s'enregistre auprès du système et lance l'écoute sur le port approprié. Utiliser la forme complète du nom de serveur.
-disable	**<nom complet du serveur><[autres informations d'authentification]>**	Désactiver un serveur pour qu'il cesse de répondre aux requêtes de la plate-forme de BI, mais reste démarré en tant que processus. Utiliser la forme complète du nom de serveur.
-display	**< [autres informations d'authentification]>**	Rapporte le statut actuel de tous les serveurs du cluster, y compris les noms de serveur, les noms d'hôte, les ID de processus, les descriptions, s'ils sont en cours d'exécution et s'ils sont activés ou désactivés.

Le tableau suivant décrit les options formant l'argument identifié par **<[autres informations d'authentification]>**.

> **Remarque**
>
> Pour une sécurité accrue, vous devez toujours fournir les références de connexion d'un compte avec l'authentification Enterprise. Les autres types d'authentification ne sont pas pris en charge.

Option d'authentification	Arguments valides	Description
-cms	**<nomcms:numéroport>**	Spécifiez le CMS auquel vous souhaitez vous connecter. Par défaut, s'il n'est pas défini, le CCM se reporte sur la machine locale et le port par défaut (6400).

Option d'authentification	Arguments valides	Description
`-username`	`<nomutilisateur>`	Spécifiez un compte qui octroie des droits administratifs à la plateforme de BI. Si aucun compte n'est spécifié, le compte "Administrator" est utilisé par défaut.
`-password`	`<mot de passe>`	Spécifiez le mot de passe correspondant. Si aucun mot de passe n'est spécifié, un mot de passe vide est utilisé. **Remarque** Pour spécifier l'argument `-password`, vous devez également spécifier l'argument `-username`.

Le CCM lit les chaînes de démarrage et les autres valeurs de configuration à partir du fichier `ccm.config`.

Informations associées

ccm.config [page 1117]

31.1.1.1.1 Exemples

Ces deux commandes démarrent et activent tous les serveurs de la plateforme de BI. Le CMS (Central Management Server) démarre sur la machine locale et le port par défaut (6400) :

```
ccm.sh -start all
ccm.sh -enable all
```

Ces deux commandes démarrent et activent tous les serveurs de la plateforme de BI. Le CCM va activer tous les serveurs du cluster où le CMS s'exécute sur l'ordinateur MACHINE01 et le port 6701 :

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Ces deux commandes démarrent et activent tous les serveurs de la plateforme de BI, avec un compte administratif spécifique nommé `SysAdmin` et le mot de passe fourni :

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Cette commande unique se connecte sous un compte administratif spécifique pour désactiver un Adaptative Job Server en cours d'exécution sur un deuxième ordinateur :

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.1.1.1.2 ccm.config

Ce fichier de configuration définit les chaînes de démarrage et les autres valeurs utilisées par le CCM lorsque vous exécutez ses commandes. Ce fichier est géré par le CCM lui-même et par les autres utilitaires de script de la plateforme de BI. En général, vous ne modifiez ce fichier que lorsque vous devez modifier une ligne de commande d'un Server Intelligence Agent. Il est fortement conseillé de sauvegarder ce fichier avant de le modifier manuellement.

Informations associées

Présentation des lignes de commande [page 1124]

31.1.1.2 cmsdbsetup.sh

Le script `cmsdbsetup.sh` se trouve dans le répertoire `<sap_bobj>` de votre installation. Le script fournit un programme basé sur des fichiers texte qui permet d'effectuer les tâches suivantes :

- Configurer une base de données système du CMS
- Réinitialiser une base de données système du CMS
- Copier les données d'une autre source de données
- Changer la clé du cluster
- Changer le nom du cluster

> **Remarque**
>
> Avant d'exécuter ce script, effectuez une sauvegarde de la base de données système du CMS et du contenu de vos Input et Output File Repositories actuels. Pour en savoir plus, voir « Sauvegarde et restauration de votre système ». Veillez également à consulter Mise en cluster de Central Management Servers dans le chapitre « Administration du serveur » du *Guide d'administration de la pateforme SAP BI* pour en savoir plus sur les clusters de CMS et la configuration de la base de données du CMS.

Le script vous invitera à saisir le nom de votre Server Intelligence Agent (SIA). Pour vérifier le nom de votre SIA, consultez les propriétés de commande du SIA dans le fichier `ccm.config`. Le nom en cours du SIA apparaît après l'option `-name`. Sinon, vous pouvez utiliser l'option 8 avec le fichier `serverconfig.sh`.

Informations associées

Mise en cluster de Central Management Servers [page 441]
Présentation de la sauvegarde et de la restauration [page 565]

31.1.1.3 serverconfig.sh

Le script `serverconfig.sh` se trouve dans le répertoire `<sap_bobj>` de votre installation. Ce script fournit un programme basé sur des fichiers texte qui permet d'effectuer les opérations suivantes.

- Ajouter un nœud
- Supprimer un nœud
- Modifier un nœud
- Déplacer un nœud
- Sauvegarder la configuration du serveur
- Restaurer la configuration du serveur
- Modifier la configuration du niveau Web
- Lister tous les noeuds

31.1.1.3.1 Pour ajouter, supprimer, modifier et répertorier des nœuds sous UNIX

1. Accédez au répertoire `<REPINSTALL>/sap_bobj` de l'installation.
2. Entrez la commande suivante :

   ```
   ./serverconfig.sh
   ```

   Le script vous propose une liste d'options :

   1. Ajouter un nœud
   2. Supprimer un nœud
   3. Modifier un nœud
   4. Déplacer un nœud
   5. Sauvegarder la configuration du serveur
   6. Restaurer la configuration du serveur
   7. Modifier la configuration du niveau Web
   8. Lister tous les noeuds
3. Saisissez le chiffre correspondant à l'action que vous souhaitez effectuer.
4. Si vous ajoutez, supprimez ou modifiez un serveur, donnez au script toutes les informations supplémentaires qu'il demande.

31.1.2 Modèles de scripts

31.1.2.1 startservers

Le script `startservers` se trouve dans le répertoire `<REPINSTALL>/sap_bobj` de l'installation. Ce script peut être utilisé comme modèle pour vos propres scripts : il est fourni à titre d'exemple pour montrer comment vous pouvez configurer vos propres scripts de démarrage des serveurs de la plateforme de BI en exécutant une série de commandes dans le CCM. Pour en savoir plus sur l'écriture de commandes dans le CCM pour vos serveurs, voir la section ccm.sh [page 1113].

31.1.2.2 stopservers

Le script `stopservers` se trouve dans le répertoire `<REPINSTALL>/sap_bobj` de l'installation. Ce script peut être utilisé comme modèle pour vos propres scripts : il est fourni à titre d'exemple pour montrer comment vous pouvez configurer vos propres scripts d'arrêt des serveurs de la plateforme de BI en exécutant une série de commandes dans le CCM. Pour en savoir plus sur l'écriture de commandes dans le CCM pour vos serveurs, voir la section ccm.sh [page 1113].

31.1.3 Scripts utilisés par la plateforme de BI

Ces scripts secondaires sont souvent exécutés en arrière-plan lorsque vous exécutez les utilitaires du script principal de la plateforme de BI et vous n'avez pas besoin de les exécuter vous-même.

bobjrestart.sh

Ce script est exécuté en interne par le CCM pour gérer les nœuds du Server Intelligence Agent. N'exécutez pas ce script vous-même.

env.sh

Le script `env.sh` se trouve dans le répertoire `<sap_bobj/setup>` de votre installation. Ce script définit les variables d'environnement de la plateforme de BI requises par certains des autres scripts. Les scripts de la plateforme de BI exécutent env.sh si nécessaire. Pour en savoir plus, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*.

env-locale.sh

Le script `env-locale.sh` est utilisé pour convertir les chaînes linguistiques de script en fonction des différents types d'encodage (par exemple, UTF8, EUC ou Shift-JIS). Ce script est exécuté par `env.sh` lorsque c'est nécessaire.

initlaunch.sh

Le script `initlaunch.sh` exécute `env.sh` pour définir les variables d'environnement de la plateforme de BI, puis exécute les éventuelles commandes que vous avez ajoutées sous forme d'argument de ligne de commande pour ce script. Ce script est essentiellement destiné à servir d'outil de débogage au personnel de SAP BusinessObjects.

postinstall.sh

Le script `postinstall.sh` se trouve dans le répertoire `<REPSCRIPT>` de votre installation. Vous ne devez pas exécuter ce script vous-même.

setup.sh

Le script `setup.sh` est installé dans le répertoire racine de votre installation. Ce script fournit un programme textuel qui permet de configurer l'installation de la plateforme de BI. Il est exécuté automatiquement lorsque vous installez la plateforme de BI. Il vous demande les informations requises pour configurer la plateforme de BI pour la première fois.

Pour en savoir plus sur les réponses à fournir au script de configuration lors de l'installation de la plateforme de BI, voir le *Guide d'installation de la plateforme SAP BusinessObjects Business Intelligence*.

setupinit.sh

Le script `setupinit.sh` se trouve dans le répertoire `</sap_bobj/init>` de l'installation. Ce script copie les scripts de contrôle d'exécution dans vos répertoires `rc#`, pour un démarrage automatisé. Pour que les serveurs de la plateforme de BI démarrent et s'arrêtent en même temps que l'ordinateur où ils sont installés, exécutez ce script à la fin du script `setup.sh`.

> **Remarque**
>
> Vous devez posséder des droits d'accès root pour exécuter ce script.

31.2 Scripts Windows

Cette section détaille chacun des outils d'administration et des scripts inclus avec la distribution Windows de la plateforme de BI. Cette section est fournie surtout à titre de référence. Des concepts et des procédures de configuration sont décrits plus en détail tout au long de ce guide.

La distribution Windows de la plateforme de BI inclut la version Windows du CCM (Central Configuration Manager). Outre l'interaction avec l'interface utilisateur graphique, vous pouvez choisir d'exécuter le fichier exécutable du CCM depuis la ligne de commande avec des options pour gérer vos serveurs.

31.2.1 ccm.exe

Le fichier exécutable `ccm.exe` est installé sous le répertoire `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` de votre installation. Vous pouvez exécuter le fichier exécutable directement depuis la ligne de commande pour effectuer certaines opérations. Cette section répertorie les options de ligne de commande et fournit quelques exemples.

> **Remarque**
>
> Un SIA (Server Intelligence Agent) et un CMS (Central Management Server) doivent être en cours d'exécution avant d'utiliser les options de ligne de commande du fichier `ccm.exe` pour interagir avec un serveur individuel.

> **Remarque**
>
> Les arguments entre crochets [ ] sont facultatifs.

> **Remarque**
>
> Les arguments identifiés par **`<autres informations d'authentification>`** sont présentés dans le deuxième tableau.

Option CCM	Arguments valides	Description
`-help`	n/a	Afficher l'aide de la ligne de commande.
`-managedstart`	`all` ou **`<nom complet du serveur> <[autres informations d'authentification]>`**	Démarrer un serveur.
`-managedstop`	`all` ou **`<nom complet du serveur> <[autres informations d'authentification]>`**	Arrêter un serveur.

Option CCM	Arguments valides	Description
`-managedrestart`	`all` ou **`<nom complet du serveur> <[autres informations d' authentification]>`**	Arrêter un serveur, puis redémarrer le serveur.
`-managedforceterminate`	`all` ou **`<nom complet du serveur> <[autres informations d' authentification]>`**	Arrête le serveur immédiatement sans terminer les requêtes en cours de traitement.
`-enable`	`all` ou **`<nom complet du serveur> <[autres informations d' authentification]>`**	Activer un serveur démarré pour qu'il s'enregistre auprès du système et lance l'écoute sur le port approprié.
`-disable`	`all` ou **`<nom complet du serveur> <[autres informations d' authentification]>`**	Désactiver un serveur pour qu'il cesse de répondre aux requêtes de la plateforme de BI, mais reste démarré en tant que processus.
`-display`	**`< [autres informations d'authentification]>`**	Rapporte le statut actuel de tous les serveurs du cluster, y compris les noms de serveur, les noms d'hôte, les ID de processus, les descriptions, s'ils sont en cours d'exécution et s'ils sont activés ou désactivés.

Le tableau suivant décrit les options formant l'argument identifié par **`<[autres informations d'authentification]>`**.

> **Remarque**
>
> Vous devez toujours fournir les références de connexion d'un compte avec l'authentification Enterprise.

Option d'authentification	Arguments valides	Description
`-cms`	**`<nomcms:numéroport>`**	Spécifiez le CMS auquel vous souhaitez vous connecter. Par défaut, s'il n'est pas défini, le CCM se reporte sur la machine locale et le port par défaut (6400).
`-username`	**`<nom d'utilisateur>`**	Spécifiez un compte qui octroie des droits administratifs à la plateforme de BI. Si aucun compte n'est spécifié, le compte "Administrator" est utilisé par défaut.

Option d'authentification	Arguments valides	Description
`-password`	`<mot de passe>`	Spécifiez le mot de passe correspondant. Si aucun mot de passe n'est spécifié, un mot de passe vide est utilisé. **Remarque** Pour spécifier l'argument `-password`, vous devez également spécifier l'argument `-username`.
`-authentication`	`<type d'authentification>`	Spécifiez le type d'authentification. Seul `secEnterprise` est pris en charge.

Le CCM lit les chaînes de démarrage et les autres valeurs de configuration à partir du fichier `ccm.config`.

31.2.1.1 Exemples

Les exemples suivants supposent qu'un SIA (Server Intelligence Agent) et un CMS (Central Management Server) ont déjà démarré et sont en cours d'exécution. Avant d'utiliser les options de ligne de commande de `ccm.exe` pour interagir avec un serveur individuel, vous pouvez utiliser la commande Windows suivante pour démarrer le service SIA :

```
net start "Server Intelligence Agent (NODENAME)"
```

Le SIA peut également être arrêté à l'aide de la commande `net stop "Server Intelligence Agent (NOMNŒUD)"`

Cette commande démarre tous les serveurs de la plateforme de BI :

```
ccm.exe -managedstart all
```

Cette commande démarre un Adaptive Job Server. Le CMS a démarré sur le port 6701, plutôt que sur le port par défaut :

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Cette commande active un Adaptive Job Server avec un compte administratif nommé `SysAdmin` :

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

Cette commande connecte à un compte administratif spécifique pour désactiver un Adaptative Job Server en cours d'exécution sur un deuxième ordinateur :

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.3 Lignes de commande des serveurs

31.3.1 Présentation des lignes de commande

Cette section répertorie les options de ligne de commande qui contrôlent le comportement de chaque serveur de la plateforme de BI.

Lorsque vous démarrez ou configurez un serveur à partir de la CMC (Central Management Console), le serveur démarre (ou redémarre) à l'aide d'une ligne de commande par défaut qui inclut un ensemble d'options et de valeurs standard. Dans la plupart des cas, il est inutile de modifier les lignes de commande par défaut directement. Vous pouvez par ailleurs réviser les paramètres les plus courants à partir des différents écrans de configuration des serveurs disponibles dans la CMC. Cette section répertorie, à titre de référence, l'intégralité des options de ligne de commande prises en charge par chaque serveur. Vous pouvez modifier directement la ligne de commande de chaque serveur si vous souhaitez personnaliser davantage le fonctionnement de la plateforme de BI.

Les valeurs indiquées entre crochets [ ] dans cette section sont facultatives.

> **Remarque**
>
> Les tableaux suivants répertorient les options de commande de ligne prises en charge. Les serveurs de la plateforme de BI utilisent un certain nombre d'options internes qui ne figurent pas dans ces tableaux. Ces options internes ne peuvent pas être modifiées.

31.3.1.1 Pour afficher ou modifier la ligne de commande d'un serveur

1. Utilisez la CMC pour arrêter le serveur.
2. Cliquez avec le bouton droit sur le serveur et sélectionnez *Propriétés*.
3. Dans l'écran *Propriétés*, modifiez la ligne de commande pour le serveur et cliquez sur *Enregistrer et fermer*.
4. Démarrez le serveur.

31.3.2 Options standard communes à tous les serveurs

Sauf indication contraire, les options de ligne de commande ci-dessous s'appliquent à tous les serveurs de la plateforme de BI. La suite de cette section présente les options propres à chaque type de serveur.

Option	Arguments valides	Comportement
-requestPort	**<port >**	Spécifie le port que le serveur écoute. Le serveur enregistre ce port auprès du CMS. Si rien n'est spécifié, le serveur choisit n'importe quel port disponible supérieur à 1024. **Remarque** Ce port est utilisé dans des buts différents par plusieurs serveurs. Avant d'effectuer une modification, consultez la section consacrée à la modification des numéros de port par défaut des serveurs dans le *Guide d'administration de la plateforme de BI*.
-loggingPath	**<chemin d'accès absolu>**	Spécifie le chemin où les fichiers journaux sont créés.

31.3.2.1 Traitement des signaux UNIX

Sous UNIX, les démons de la plateforme de BI traitent les signaux suivants :

- SIGTERM entraîne un arrêt progressif du serveur (code de sortie = 0).
- SIGSEGV, SIGBUS, SIGSYS, SIGFPE et SIGILL entraînent un arrêt rapide (code de sortie = 1).

31.3.3 Central Management Server

Cette section décrit les options de ligne de commande spécifiques au CMS. Le chemin par défaut du serveur sous Windows est :<REPINSTALL>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe.

Le chemin par défaut du serveur sous UNIX est :<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>/boe_cmsd.

Option	Arguments valides	Comportement
-threads	**<nombre>**	Spécifie le nombre de threads de travail que le CMS initialise et utilise. Ce nombre doit être compris entre 12 et 150 ; par défaut, il a pour valeur 50.

Option	Arguments valides	Comportement
`-reinitializedb`		Entraîne la suppression par le CMS de la base de données système pour en recréer une contenant uniquement les objets système par défaut. Toutes les données existantes de la base de données sont perdues lors de sa recréation.
`-quit`		Oblige le CMS à se fermer après le traitement de l'option `-reinitializedb` .
`-receiverPool`	**`<nombre>`**	Spécifie le nombre de threads créés par le CMS pour recevoir les requêtes client. Un client peut être un autre serveur SAP BusinessObjects, l'Assistant de publication de rapport, Crystal Reports ou une application client que vous avez créée. La valeur par défaut est 5. Normalement, vous n'avez pas besoin d'augmenter cette valeur sauf si vous créez une application personnalisée avec de nombreux clients.
`-maxobjectsincache`	**`<nombre>`**	Spécifie le nombre maximal d'objets enregistrés par le CMS dans son cache mémoire. Augmenter le nombre d'objets réduit le nombre d'appels requis à la base de données et améliore sensiblement les performances du CMS. Toutefois, un nombre trop élevé d'objets en mémoire peut limiter de manière excessive la mémoire disponible du CMS pour traiter les requêtes. La valeur par défaut est 100000.
`-ndbqthreads`	**`<nombre>`**	Spécifie le nombre de threads ouvriers du CMS envoyant des requêtes à la base de données. Chaque thread ayant une connexion à la base de données, vous devez veiller à ne pas dépasser la capacité de la base de données. La plupart du temps, la valeur maximale doit être définie à 20.

Option	Arguments valides	Comportement
-oobthreads	<nombre>	Si votre cluster comporte plus de huit membres du cluster de CMS, assurez-vous que la ligne de commande de chaque CMS contient cette option. Spécifiez le nombre de services CMS dans votre cluster. Cette option fait en sorte que le cluster puisse prendre en charge des charges importantes.

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.4 Crystal Reports Processing Server et Crystal Reports Cache Server

Le Crystal Reports Processing Server et le Crystal Reports Cache Server sont contrôlés à peu près de la même manière depuis la ligne de commande. Les options de la ligne de commande déterminent si le serveur doit démarrer en tant que serveur de traitement, Cache Server ou les deux. Les options qui ne s'appliquent qu'à un type de serveur précis sont indiquées ci-dessous.

Les chemins par défaut des serveurs sous Windows sont :

- <RÉPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0 \win64_x64\cacheserver.exe.
- <RÉPINSTALL>\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.

Les chemins par défaut des serveurs sous UNIX sont :

- <RÉPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>/boe_cachesd.
- <RÉPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>/boe_procd.

Option	Arguments valides	Comportement
-cache		Active la fonctionnalité Cache Server.
-deleteCache		Supprime le répertoire de la mémoire cache à chaque démarrage et arrêt du serveur.
-report_ProcessExtPath	<cheminabsolu>	Spécifie le répertoire par défaut des extensions de traitement.

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.5 Job Servers

Cette section décrit les options de ligne de commande spécifiques à l'Adaptative Job Servers.

Le chemin par défaut du serveur sous Windows est : `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`

Le chemin par défaut du serveur sous UNIX est :`<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>/boe_jobsd`.

Option	Arguments valides	Comportement
`-dir`	**`<cheminabsolu>`**	Spécifie le répertoire des données du Job Server.
`-maxJobs`	**`<nombre>`**	Définit le nombre maximal de travaux que le serveur peut gérer simultanément. La valeur par défaut est cinq.
`-requestJSChildPorts`	**`<limiteinférieure-limitesupérieure>`**	Spécifie la plage de ports que les processus enfants doivent utiliser dans un environnement de pare-feu. `6800-6805` limite, par exemple, les processus enfants à six ports. **Remarque** Pour que cette option soit prise en compte, vous devez également spécifier le paramètre `-requestPort`.
`-report_ProcessExtPath`	**`<cheminabsolu>`**	Spécifie le répertoire par défaut des extensions de traitement. Pour en savoir plus, voir le *Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence*.

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.6 Serveur de traitement adaptatif

Le serveur de traitement adaptatif utilise les paramètres définis pour la machine virtuelle Java de SAP (SAP JVM). Consultez la documentation SAP JVM pour plus d'informations.

31.3.7 Report Application Server

Cette section décrit les options de ligne de commande spécifiques au Report Application Server.

Le chemin par défaut du serveur sous Windows est : `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

Le chemin par défaut du serveur sous UNIX est `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>/ras/boe_crystalrasd`.

Option	Arguments valides	Comportement
`-ipport`	**`<port>`**	Spécifie le numéro de port pour recevoir les requêtes TCP/IP lors de l'exécution en mode autonome (en dehors de la plateforme de BI).
`-report_ProcessExtPath`	**`<cheminabsolu>`**	Spécifie le répertoire par défaut des extensions de traitement. Pour en savoir plus, voir le *Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence*.

Option	Arguments valides	Comportement
`-ProcessAffinityMask`	`<masque>`	Utilise un masque pour spécifier exactement les processeurs centraux que le RAS doit utiliser lorsqu'il s'exécute sur un ordinateur multiprocesseur. Le masque est de la forme `0xffffffff`, où chaque lettre `f` représente un processeur et la liste de processeurs se lit de droite à gauche (autrement dit, la dernière lettre `f` représente le premier processeur). Remplacez chaque lettre `f` par 0 (utilisation d'un processeur central non autorisée) ou `1` (utilisation d'un processeur central autorisée). Par exemple, si vous exécutez le RAS sur un ordinateur doté de 4 processeurs et souhaitez qu'il utilise les troisième et quatrième processeurs, recourez au masque `0x1100`. Pour utiliser les deux processeurs, recourez au masque `0x0110`. **Remarque** Le RAS utilise les premiers processeurs autorisés dans la chaîne, dans la limite maximale spécifiée par votre licence. Si votre licence est valable pour deux processeurs, la chaîne `0x1110` a le même effet que la chaîne `0x0110`. **Remarque** La valeur par défaut du masque est `-1`, ce qui a la même signification que `0x1111`.

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.8 Web Intelligence Processing Server

Cette section répertorie les options de ligne de commande propres au Web Intelligence Processing Server.

Le chemin par défaut du serveur sous Windows est `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Le chemin par défaut du serveur sous UNIX est `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>/WIReportServer`.

Option	Arguments valides	Comportement
-ConnectionTimeout Minutes	**<minutes>**	Indique le nombre de minutes avant que la connexion au serveur n'arrive à expiration.
-MaxConnections	**<nombre>**	Indique le nombre maximum de connexions simultanées autorisées par le serveur.
-DocExpressEnable		Active la mise en cache d'un document Web Intelligence lorsque ce document est visualisé.
-DocExpressRealTime CachingEnable		Active la mise en cache en temps réel des documents Web Intelligence.
-DocExpressCache DurationMinutes	**<minutes>**	Indique (en minutes) la durée de stockage du contenu dans la mémoire cache.
-DocExpressMaxCache SizeKB	**<kilo-octets>**	Indique la taille du document mis en cache.
-EnableListOfValues Cache		Active la mise en cache des listes de valeurs par session utilisateur
-ListOfValuesBatchSize	**<nombre>**	Indique le nombre maximum de valeurs qui peut être renvoyé par lot de listes de valeurs.
-UniverseMaxCacheSize	**<nombre>**	Indique le nombre d'univers à mettre en cache.
-WIDMaxCacheSize	**<nombre>**	Indique le nombre maximum de documents Web Intelligence qui peuvent être stockés dans la mémoire cache.

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.9 Input et Output File Repository Servers

Cette section décrit les options de ligne de commande spécifiques aux Input et aux Output File Repository Servers.

Le chemin par défaut des serveurs sous Windows est : `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

Le chemin par défaut du programme qui fournit les deux serveurs sous UNIX est : `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>/boe_filesd`. Par défaut, le Server Intelligence Agent lancera une instance de `boe_filesd` pour l'Input File Repository Server et une instance pour l'Output File Repository Server.

Option	Arguments valides	Comportement
`-rootDir`	**`<cheminabsolu>`**	Définit le répertoire racine des différents sous-dossiers et fichiers gérés par le serveur. Les chemins d'accès aux fichiers utilisés pour décrire les fichiers du File Repository Server sont interprétés en fonction de ce répertoire racine. **Remarque** Tous les Input File Repository Servers doivent partager le même répertoire racine et tous les Output File Repository Servers doivent également partager le même répertoire racine (dans le cas contraire, vous risquez d'avoir des instances incohérentes). En outre, le répertoire racine des Input File Repository Servers doit être différent de celui des Output File Repository Servers. Il est recommandé de répliquer les répertoires racine en utilisant une matrice de disques RAID ou une autre solution matérielle.

Option	Arguments valides	Comportement
`-tempDir`	**`<cheminabsolu>`**	Définit l'emplacement du répertoire temporaire que le FRS utilise pour transférer les fichiers. Servez-vous de cette option de ligne de commande si vous voulez contrôler le répertoire temporaire du FRS ou si le nom du répertoire temporaire par défaut généré par le FRS dépasse la limite du chemin du système de fichiers (qui empêche le démarrage du FRS). **Remarque** Ne spécifiez pas de répertoire existant pour cette option. Le répertoire spécifié sera vidé au démarrage des FRS, puis supprimé à leur arrêt. Si vous utilisez un répertoire existant, il sera vidé puis supprimé.
`-maxidle`	**`<minutes>`**	Spécifie le nombre de minutes après lequel une session inactive est éliminée.
`-legacymode`		Permet aux anciennes versions du SDK ou aux clients antérieurs à la version 4.0 d'accéder complètement à la plateforme de BI.
`-vsaFileLoc`	**`<cheminabsolu>`**	Définissez le chemin absolu sur le fichier de bibliothèque de l'adaptateur de l'analyse anti-virus. **Remarque** Tous les Input File Repository Servers doivent partager le même répertoire racine et tous les Output File Repository Servers doivent également partager le même répertoire racine (dans le cas contraire, vous risquez d'avoir des instances incohérentes).

Informations associées

Options standard communes à tous les serveurs [page 1124]

31.3.10 Event Server

Cette section décrit les options de ligne de commande spécifiques à l'Event Server.

Le chemin par défaut du serveur sous Windows est : `<REPINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`

Le chemin par défaut du serveur sous Unix est : `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>/boe_eventsd`.

Option	Arguments valides	Comportement
`-cleanup`	**`<minutes>`**	Spécifie, en minutes, la fréquence à laquelle le serveur supprime tout proxy écouteur. La valeur représente le temps nécessaire pour effectuer deux nettoyages. Si vous spécifiez la valeur 10, par exemple, les serveurs proxy seront nettoyés toutes les cinq minutes.

Informations associées

Options standard communes à tous les serveurs [page 1124]

32 Repository Diagnostic Tool

32.1 Présentation du Repository Diagnostic Tool

Le Repository Diagnostic Tool (RDT) est un outil de ligne de commande qui analyse, effectue un diagnostic et répare les incohérences pouvant se produire entre votre CMS (Central Management Server) et le stockage des fichiers FRS (File Repository Server), ou les incohérences pouvant se produire dans les métadonnées des InfoObjects stockés dans la base de données du CMS.

Lors des opérations normales, il est rare de trouver des incohérences dans la base de données système du CMS. Cependant, des incohérences peuvent se produire pendant des événements inattendus tels qu'une récupération après sinistre, une restauration de sauvegarde ou des coupures réseau. Durant ces événements, la base de données système du CMS peut être interrompue au cours de l'exécution d'une tâche. Cela peut provoquer des incohérences avec les objets de la base de données système du CMS.

Le RDT analyse la base de données système et identifie les incohérences dans les objets tels que les rapports, utilisateurs, groupes d'utilisateurs, dossiers, serveurs, univers, connexions d'univers et autres objets.

Le RDT analyse trois types d'incohérence.

- Incohérences objet-fichier.
  Il s'agit des incohérences qui se produisent entre InfoObjects dans la base de données du CMS et les fichiers correspondants dans les référentiels de fichiers. Par exemple, un fichier stocké dans les FRS peut ne pas posséder d'objet correspondant dans la base de données système du CMS.
- Incohérences dans les métadonnées des InfoObjects.
  Il s'agit des incohérences qui peuvent exister dans la définition d'objet d'un InfoObject (métadonnées) dans la base de données du CMS. Par exemple, un InfoObject peut faire référence à un InfoObject inexistant dans la base de données du CMS.
- Incohérences de relation
  Des incohérences se produisent lorsqu'une relation existe entre deux InfoObjets, mais que l'un d'entre eux a été supprimé. Seules les relations nœud d'entreprise-serveur, service-serveur, conteneur de services-serveur sont traitées.

Le RDT effectue deux opérations, selon le paramètre que vous fournissez lors de l'exécution de l'outil :

- Il analyse la base de données système du CMS et le stockage des fichiers FRS, signale les incohérences et crée un fichier journal de sortie au format XML avec des suggestions d'actions pour réparer les incohérences.
- Il analyse et répare les incohérences identifiées dans la base de données du CMS et dans le FRS, puis consigne les actions entreprises dans un fichier journal de sortie au format XML.

32.2 Utilisation du Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel)

L'outil de diagnostic de référentiel (RDT, Repository Diagnostic Tool) est disponible sur tous les ordinateurs dotés d'un CCM (Central Configuration Manager). Cet outil de ligne de commande analyse, diagnostique et répare les incohérences pouvant se produire entre la base de données système du CMS (Central Management Server) et le stockage de fichiers FRS (File Repository Server), ou les incohérences pouvant se produire dans les métadonnées d'un InfoObject.

Il est recommandé de sauvegarder la base de données du CMS et le stockage de fichiers FRS, puis d'exécuter le RDT sur la version sauvegardée lorsque les services de la plateforme de BI sont arrêtés. Si cela n'est pas possible, le RDT peut être exécuté sur une base de données active.

Pour exécuter le RDT sur une base de données active, tenez compte des éléments suivants :

- Le RDT utilisera une seule connexion de base de données lors de son exécution.
- Le RDT ne vérifiera les incohérences de la base de données que jusqu'au moment où il a commencé à s'exécuter. Aucune incohérence se produisant alors que le RDT est en cours d'exécution ne sera journalisée ni corrigée.
- Il est recommandé que l'ordinateur exécutant le RDT ait une mémoire supérieure aux recommandations système normales disponibles pour le traitement des transactions du RDT :
  - Une base de données de 50 000 InfoObjects ou moins doit disposer de 350 Mo supplémentaires pour le traitement
  - Une base de données de 50 000 à 400 000 InfoObjects doit disposer d'1,7 Go supplémentaires pour le traitement
  - Une base de données de 400 000 à 1 000 000 d'InfoObjects doit disposer de 4 Go supplémentaires pour le traitement
- Le RDT ne doit pas être exécuté depuis le serveur du CMS. L'exécution sur un ordinateur distinct peut aider à réduire l'impact sur les performances du système.
- L'outil peut avoir des effets modérés sur les performances de la base de données quand il est exécuté.

Il n'est pas nécessaire que le service CMS soit en cours d'exécution pour utiliser le RDT, celui-ci s'exécute directement sur la base de données du CMS.

32.2.1 Pour utiliser l'outil de diagnostic de référentiel

1. Si vous exécutez l'outil sur un ordinateur fonctionnant sous Windows, ouvrez une fenêtre de ligne de commande, puis exécutez la commande suivante :

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe <arguments>`, où `<arguments>` désigne la liste des paramètres que vous souhaitez spécifier.
2. Si vous exécutez l'outil sur un ordinateur UNIX, ouvrez un shell compatible avec /usr/bin/sh, puis exécutez la commande suivante.

   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>` où `<plateforme>` désigne soit « linux64_x64 », « solaris_sparcv9 », « hpux_ia64 » soit « aix_rs6000_64 » et où `<arguments>` désigne la liste des paramètres que vous souhaitez spécifier.

> **Remarque**
>
> Lors de la saisie des paramètres de la ligne de commande Unix, vous devrez peut-être ignorer les caractères shell spéciaux. Par exemple, si le point d'exclamation « ! » est utilisé dans un mot de passe, vous devrez peut-être ignorer le point d'exclamation ainsi : `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

L'outil de diagnostic de référentiel analyse le référentiel pour rechercher des incohérences. Selon les paramètres spécifiés, il effectue un diagnostic puis journalise les incohérences ou il répare les incohérences puis consigne l'action qu'il a effectuée.

`Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` répertorie les incohérences que l'outil trouve. Lorsque l'outil répare les incohérences trouvées, il crée également le fichier `Repo_Repair_aaaa_mm_dd_hh_mm_ss.xml`. Ce fichier détaille les objets réparés et les fichiers orphelins supprimés. S'il existe des incohérences ne pouvant être réparées, elles seront également répertoriées.

Le chemin d'accès aux fichiers journaux peut spécifié à l'aide du paramètre `outputdir`. Si ce paramètre n'est pas spécifié, le répertoire par défaut des fichiers journaux est `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` sous Windows et `./sap_bobj/enterprise_xi40/reposcan` sous Unix.

> **Remarque**
>
> L'application fournit également un fichier XSL par défaut utilisé avec un fichier XML pour créer une page HTML. Le fichier XSL est stocké dans `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` sous Windows et `./sap_bobj/enterprise_xi40/reposcan` sous Unix.

Pour obtenir la liste des messages d'avertissement et des actions recommandées effectuées par le RDT lorsqu'il trouve des incohérences, voir *Incohérences dans les métadonnées du CMS* et *Incohérences entre le CMS et le FRS*.

Informations associées

Incohérences dans les métadonnées du CMS [page 1146]
Incohérences entre le CMS et le FRS [page 1146]

32.2.2 Paramètres du Repository Diagnostic Tool

Le RDT (Repository Diagnostic Tool, outil de diagnostic de référentiel) accepte les paramètres figurant dans le tableau suivant :

> **Remarque**
>
> Les arguments de ligne de commande remplacent toutes les entrées du fichier de paramètres lors de l'exécution.

> **Remarque**
>
> Pour en savoir plus sur les options des paramètres de la base de données SAP HANA, voir la note SAP 1916845.

Paramètres généraux

Paramètre	Facultatif ou Obligatoire	Description
`dbdriver`	Obligatoire	Type de pilote utilisé pour la connexion à la base de données du CMS. Les valeurs acceptées sont les suivantes : • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`
`connect`	Obligatoire	Détails de connexion utilisés pour la connexion à la base de données du CMS. Par exemple : `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"`

Paramètre	Facultatif ou Obligatoire	Description
`dbkey`	Obligatoire	Saisissez la clé de cluster de votre déploiement de la plateforme de BI. Si vous ne connaissez pas la clé de cluster, réinitialisez-la en suivant ces étapes : **Remarque** Si l'ordinateur fait partie d'un cluster, ces étapes doivent être effectuées pour tous les membres du cluster. Sauvegardez la base de données du CMS et le stockage des fichiers avant de continuer. 1. Lancez le Central Configuration Manager (CCM). 2. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez *Arrêter*. Ne passez à l'étape 3 que lorsque le statut du SIA est « Arrêté ». 3. Cliquez avec le bouton droit sur le SIA et choisissez *Propriétés*. 4. Dans l'onglet Configuration, cliquez sur *Modifier* en regard de l'option *Configuration de clé de cluster*. 5. Un message d'avertissement s'affiche. Cliquez sur Oui pour continuer. 6. Dans la boîte de dialogue *Modifier la clé de cluster*, saisissez la même clé à huit caractères dans les champs *Nouvelle clé de cluster* et *Confirmer la nouvelle clé de cluster*. **Remarque** Le RDT ne s'exécute pas si le paramètre `dbkey` est omis ou si la clé de cluster est erronée. **Remarque** La clé de cluster affichée dans le CCM est cryptée et ne peut pas être utilisée dans le paramètre `dbkey`. Pour en savoir plus sur les clés de cluster, voir « Sécurisation de la plateforme de BI » dans le *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.
`inputfrsdir`	Obligatoire	Chemin d'accès au fichier du Input File Repository Server. **Remarque** Le compte utilisateur sous lequel vous êtes connecté est utilisé pour exécuter l'outil de ligne de commande. Un contrôle total est requis sur l'emplacement des fichiers.

Paramètre	Facultatif ou Obligatoire	Description
`outputfrsdir`	Obligatoire	Chemin d'accès au fichier du Output File Repository Server. **Remarque** Le compte utilisateur sous lequel vous êtes connecté est utilisé pour exécuter l'outil de ligne de commande. Un contrôle total est requis sur l'emplacement des fichiers.
`outputdir`	Facultatif	Chemin d'accès au fichier où le RDT enregistre les fichiers journaux. Par défaut, il s'agit de `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\reposcan` sous Windows et `./sap_bobj/enterprisexi_40/reposcan` sous Unix.
`count`	Facultatif	Nombre approximatif d'erreurs à analyser. Permet d'obtenir des performances optimales. Le nombre plus élevé est 2e31 - 1. La valeur 0 est interprétée comme le référentiel complet. La valeur par défaut est 1000.
`repair`	Facultatif	Demande au RDT de réparer toutes les incohérences qu'il trouve. Le comportement par défaut est de signaler les incohérences mais de n'effectuer aucune réparation. Si la ligne de commande comporte le paramètre `-repair`, le Repository Diagnostic Tool (RDT) crée un rapport sur toutes les incohérences et les répare. **Attention** Ce processus supprimera tous les objets ou fichiers orphelins de la base de données du référentiel.
`scanfrs`	Facultatif	Indique si le RDT analyse les incohérences du CMS et du FRS.
`scancms`	Facultatif	Indique si le RDT analyse le CMS pour rechercher les incohérences entre InfoObjects.
`submitterid`	Facultatif	Spécifie l'ID utilisateur qui remplace les ID manquants ou non valides pour les objets planifiés. Si aucune valeur n'est fournie, le RDT ne remplace pas les ID non valides. Si l'ID utilisateur fourni n'existe pas dans le CMS, le RDT invite l'utilisateur à saisir un ID valide. Ce paramètre n'est utilisé que lorsque le RDT fonctionne en mode réparation.

Paramètre	Facultatif ou Obligatoire	Description
`startid`	Facultatif	Spécifie l'objet dans la base de données du CMS pour lequel démarrer l'analyse. Par exemple, si vous avez déjà analysé les 500 premiers objets dans votre référentiel, vous pouvez définir **`-startid=501`** pour démarrer l'analyse au 501e objet. La valeur par défaut est **`1`**.
`optionsfile`	Facultatif	Indique le chemin d'accès au fichier de paramètres. Le fichier de paramètres est un fichier texte qui répertorie chaque option de ligne de commande avec ses valeurs. Ce fichier ne doit comporter qu'un seul paramètre par ligne. **Remarque** Cette option permet de définir tous les paramètres dans un fichier texte comme décrit ci-dessus. Elle permet également de cibler le fichier de paramètres sans saisir les paramètres sur la ligne de commande.
`syscopy`	Facultatif	Ce paramètre est utilisé lors de la copie de la base de données du référentiel. Vous devez exécuter l'outil sur une copie récemment créée, ce qui mettra à jour la copie pour l'empêcher de former un cluster avec les serveurs du système source. Si la copie n'est pas destinée à communiquer avec le système source, cela n'est pas nécessaire. Il ne doit être utilisé qu'avec les paramètres obligatoires et non combiné avec d'autres paramètres facultatifs de la liste. **Remarque** Veillez à ne pas exécuter le RDT avec le paramètre `syscopy` sur votre système source.
`trace`	Facultatif	Ce paramètre génère des traces (enregistrements des événements qui se produisent pendant l'exécution d'un composant surveillé) et les collecte dans des fichiers journaux portant l'extension .glf à l'emplacement suivant : `<RÉP_INST_SAP_BOBJ>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging`

Paramètre	Facultatif ou Obligatoire	Description
`scankind`	Facultatif	Saisissez le type d'InfoObject que vous souhaitez analyser pour rechercher des incohérences. **Exemple** SI_KIND - rapports Web Intelligence, rapports Crystal La liste des infoObjects pris en charge qui peuvent être analysés pour rechercher des incohérences comprend : • dossier • rapport Crystal • raccourci • utilisateur • groupe d'utilisateurs • calendrier • connexion • category • lot d'objets • publication • PDF • RTF • txt • note • Word • Excel • base de données • profil • programme • agnostique • univers • lien hypertexte • FullClient • PowerPoint • scopebatch • metadata.dataconnection • Webi • QaaWS • lcmjob • overload • Xcelsius

Paramètre	Facultatif ou Obligatoire	Description
		• biwidgets • mon.probe • LiveOffice • mdanalysis • visualdiff • ao.workbook • dsl.metadatafile • afdashboardpage • ao.presentation • ccis.dataconnection • platformsearchqueue • metadata.businessview • platformsearchindex • platformsearchcontentstore • platformsearchcontentsurrogate **Remarque** Le fichier de sortie XML pouvant être analysé affiche la liste des incohérences par rapport aux infoObjects. En d'autres termes, les objets fichiers affectés ne se trouvent pas dans la liste.
`scandays`	Facultatif	Saisissez le nombre de jours pendant lesquels vous souhaitez que Reposcan recherche des incohérences. **Exemple** Tout chiffre ou nombre supérieur à 0. **Remarque** Cette option se base sur l'heure système en cours.

La relation n'est pas analysée lors des analyses partielles. Des analyses partielles ont lieu si l'une des trois options suivantes est utilisée :

- startid
- scankind
- scandays

Incohérences dans les relations

Message d'avertissement	Incohérence	Suggestion	Action
`Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)`	La bordure d'une relation n'existe plus.	Autorisez l'application à supprimer la relation.	Relation supprimée.

Les paramètres suivants sont utilisés si le Repository Diagnostic Tool est exécuté sur un CMS mis en cluster actif.

Utilisation de l'outil de diagnostic du référentiel avec un CMS mis en cluster

Paramètre	Facultatif ou Obligatoire	Description
`requestport`	Facultatif	Numéro de port utilisé par le RDT pour communiquer avec le CMS. Accepte des nombres entiers positifs. Par défaut, l'outil utilise la valeur du système d'exploitation de l'ordinateur sur lequel s'exécute le RDT.
`numericip`	Facultatif	Indique si le RDT utilise l'adresse IP numérique au lieu du nom d'hôte pour la communication entre le CMS et l'ordinateur sur lequel s'exécute le RDT. Les valeurs acceptées sont **`True`** et **`False`**. La valeur par défaut est **`False`** (faux).
`ipv6`	Facultatif	Nom ipv6 de l'ordinateur sur lequel s'exécute le RDT. Accepte une chaîne de caractères. La valeur par défaut est le nom d'hôte de l'ordinateur sur lequel s'exécute le RDT.
`port`	Facultatif	Nom ipv4 de l'ordinateur sur lequel s'exécute le RDT. Accepte une chaîne de caractères. La valeur par défaut est le nom d'hôte de l'ordinateur sur lequel s'exécute le RDT.
`threads`	Facultatif	Nombre de threads à utiliser. Accepte des nombres entiers positifs. La valeur par défaut est **`12`**.

Les paramètres suivants sont utilisés lorsque le RDT utilise l'authentification SSL pour communiquer avec la base de données de CMS analysée.

Utilisation du RDT avec SSL

Paramètre	Facultatif ou Obligatoire	Description
`protocol`	Facultatif	Indique si l'outil doit être exécuté en mode SSL. La seule valeur acceptée est **`ssl`**.
`ssl_certdir`	Facultatif	Répertoire qui contient les certificats SSL.
`ssl_trustedcertificate`	Facultatif	Nom de fichier du certificat.
`ssl_mycertificate`	Facultatif	Nom de fichier du certificat signé.
`ssl_mykey`	Facultatif	Nom du fichier contenant la clé privée SSL.
`ssl_mykey_passphrase`	Facultatif	Nom du fichier contenant la phrase de passe SSL.

Exemple

L'exemple Windows suivant analyse le CMS et le FRS à la recherche des deux types d'incohérence, puis répare les incohérences trouvées.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect
« UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306> »
-inputfrsdir « C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input »
-outputfrsdir    « C:\Program Files (x86)\SAP BusinessObjects\SAP
BusinessObjects Enterprise XI 4.0\FileStore\Output »
-dbkey <cluster key>
-repair
```

Exemple

Exemple Unix :

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

32.3 Incohérences entre le CMS et le FRS

Le tableau suivant décrit les incohérences possibles entre une base de données du CMS (Central Management Server) et les FRS (File Repository Servers), reconnues par le Repository Diagnostic Tool (RDT).

- Message d'avertissement
  Message d'avertissement qui figure dans les fichiers journaux de réparation et d'analyse.
- Incohérence
  Description de l'incohérence trouvée par le RDT pour l'objet.
- Suggestion
  Action suggérée par le RDT lorsqu'il trouve une incohérence. Figure dans le fichier journal de l'analyse.
- Action
  Action effectuée par le RDT pour réparer une incohérence. Figure dans le fichier journal de la réparation.

Message d'avertissement	Incohérence	Suggestion	Action
L'objet `<Type d'objet>` de `<Nom d'objet>` (ID d'objet = `<ID>`) fait référence à des fichiers qui n'existent pas dans le FRS (`<Nom de fichier>`).	L'objet existe dans la base de données du CMS mais il n'existe aucun fichier correspondant dans le FRS.	Autorisez l'application à supprimer cet objet. Tous les objets descendants de cet objet seront également supprimés.	Cet objet a été supprimé du référentiel.
Le fichier `<Nom de fichier>` existe dans l'Input ou l'Output FRS, mais le référentiel ne contient aucun InfoObject correspondant.	Le fichier existe dans le FRS, mais il n'existe aucun fichier correspondant dans la base de données du CMS.	Autorisez l'application à supprimer le fichier non lié.	Aucune action effectuée.
L'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) possède le fichier `<Nom de fichier>`. La taille du fichier enregistré (`<Taille>` octets) ne correspond pas à la taille réelle du fichier (`<Taille>` octets).	La taille du fichier ne correspond pas à celle du fichier InfoObject.	Autorisez l'application à mettre à jour l'objet avec la bonne taille.	L'objet a été mis à jour pour que la taille de fichier soit correcte.
Ce répertoire ne contient aucun fichier.	Le dossier FRS est vide.	Autorisez l'application à supprimer le répertoire.	Dossier vide supprimé.

32.4 Incohérences dans les métadonnées du CMS

Le tableau suivant décrit les incohérences reconnues par le Repository Diagnostic Tool (RDT) susceptibles de se produire dans les métadonnées des objets figurant dans une base de données système du CMS (Central Management Server).

- Message d'avertissement
  Message d'avertissement qui figure dans les fichiers journaux de réparation et d'analyse.

- Incohérence
  Description de l'incohérence trouvée par le RDT pour l'objet.
- Suggestion
  Action suggérée par le RDT lorsqu'il trouve une incohérence. Figure dans le fichier journal de l'analyse.
- Action
  Action effectuée par le RDT pour réparer une incohérence. Figure dans le fichier journal de la réparation.

Message d'avertissement	Incohérence	Suggestion	Action
L'objet parent de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID objet = `<ID>`) est manquant (ID objet parent = `<ID>`).	L'ID d'objet parent de cet objet est manquant ou non valide.	Autorisez l'application à déplacer l'objet dans le dossier "Réparation BOE".	L'objet et ses enfants sont déplacés dans le répertoire Réparation BOE.
L'objet propriétaire de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet propriétaire = `<ID>`).	L'ID d'objet propriétaire de cet objet est manquant ou non valide.	Autorisez l'application à affecter l'objet à l'Administrateur	L'objet est affecté à l'Administrateur.
L'objet de demandeur de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet de demandeur = `<ID>`).	L'ID d'objet de demandeur de cet objet est manquant ou non valide.	La recommandation affichée par le RDT varie selon que vous avez fourni ou non une valeur pour le paramètre `-submitterid`. • Si vous avez fourni ce paramètre, la recommandation est la suivante : « Autoriser l'application à mettre à jour l'objet avec l'ID de demandeur fourni ». • Si vous n'avez pas fourni ce paramètre, la recommandation est « Replanifier l'objet ou utiliser la ligne de commande -submitterid pour remplacer l'ID de demandeur non valide. »	Si vous fournissez une valeur pour le paramètre `-submitterid` , le RDT applique cette valeur à l'ID de demandeur de l'objet. Si vous ne fournissez aucune valeur pour ce paramètre, le RDT n'effectue aucune action. Lorsque vous replanifiez l'objet, le CMS applique un nouvel ID.
La propriété de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) de la dernière instance réussie fait référence à un objet manquant (ID d'objet de la dernière instance réussie = `<ID>`).	La dernière instance réussie de l'objet est manquante ou non valide.	Autorisez l'application à recalculer la propriété.	Propriété recalculée.

Message d'avertissement	Incohérence	Suggestion	Action
L'objet de calendrier de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet de calendrier = `<ID>`).	L'objet fait référence à un calendrier inexistant.	Replanifiez l'objet avec un calendrier existant. Aucune action ne peut être effectuée par cette application.	Aucune action effectuée.
Le groupe de serveurs de planification requis de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet de groupe de serveurs = `<ID>`).	Le serveur préféré n'existe pas.	Replanifiez l'objet et sélectionnez un groupe de serveurs existant. Aucune action ne peut être effectuée par cette application.	Aucune action effectuée.
La liste d'événements en attente de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient un ou plusieurs objets manquants (ID d'objet d'événement = `<ID>`).	Le ou les événements que cet objet attend n'existent pas.	Replanifiez l'objet pour qu'il attende des objets d'événement existants. Aucune action ne peut être effectuée par cette application.	Aucune action effectuée.
La liste d'événements à déclencher de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient un ou plusieurs objets manquants (ID d'objet d'événement = `<ID>`).	Cet objet déclenche un événement qui n'existe pas.	Autorisez l'application à supprimer les événements manquants de la liste des événement à déclencher de l'objet.	Les événements manquants sont supprimés de la liste des événements à déclencher de l'objet.
La liste de contrôle d'accès de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) fait référence à un principal manquant (ID d'objet de principal = `<ID>`).	Entrée de contrôle d'accès orpheline.	Autorisez l'application à supprimer l'objet principal manquant de la liste des contrôles d'accès de l'objet.	Objet principal manquant supprimé de la liste des contrôles d'accès de l'objet.
La liste de contrôle d'accès de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) fait référence à un niveau d'accès manquant (ID d'objet de niveau d'accès = `<ID>`).	Entrée de contrôle d'accès orpheline.	Autorisez l'application à supprimer le niveau d'accès manquant de la liste des contrôles d'accès de l'objet.	Niveau d'accès manquant supprimé de la liste des contrôles d'accès de l'objet.
L'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient plusieurs dossiers Favoris.	Un compte d'utilisateur spécifique comporte plusieurs dossiers.	Autorisez l'application à regrouper plusieurs dossiers en un seul dossier de favoris.	Tous les dossiers de favoris ont été regroupés en un seul dossier de favoris.

Message d'avertissement	Incohérence	Suggestion	Action
L'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient des entrées de fichiers d'entrée non valides (`<Fichiers>`).	L'objet contient des entrées non valides dans sa liste de fichiers d'entrée.	Autorisez l'application à supprimer les entrées non valides de l'objet de sa liste de fichiers d'entrée.	Entrées non valides supprimées de la liste de fichiers d'entrée de l'objet.
L'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient des entrées de fichiers de sortie non valides (`<Fichiers>`).	L'objet contient des entrées non valides dans sa liste de fichiers de sortie.	Autorisez l'application à supprimer les entrées non valides de l'objet de sa liste de fichiers de sortie.	Entrées non valides supprimées de la liste de fichiers de sortie de l'objet.
Le groupe de serveurs de mise en cache requis de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet de groupe de serveurs = `<ID>`).	Le groupe de serveurs de mise en cache requis de l'objet est manquant.	Replanifiez l'objet et sélectionnez un groupe de serveurs existant.	Aucune action effectuée.
Le groupe de serveurs de traitement requis de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) est manquant (ID d'objet de groupe de serveurs = `<ID>`).	Le groupe de serveurs de traitement requis de l'objet est manquant.	Replanifiez l'objet et sélectionnez un groupe de serveurs existant.	Aucune action effectuée.
La liste de profils de l'objet `<Nom d'objet>` de `<Type d'objet>` (ID d'objet = `<ID>`) contient un ou plusieurs objets manquants (ID d'objet de profil = `<ID>`).	L'objet comporte des objets manquants dans sa liste de profils.	Veuillez mettre à jour votre publication avec des profils existants. Aucune action ne peut être effectuée par l'application.	Aucune action effectuée.

32.5 Gestion du SDK Restful dans l'application Web BOE

Pour activer la partie de l'application Web BIPRWS de l'application Web BOE dans 4.3 SP03, définissez l'indicateur sur *vrai* à l'emplacement ci-dessous :

```
<BOE_INST_DIR>\SAP BusinessObjects\tomcat\webapps\BOE\WEB-
INF\internal\Global.properties
```

Définissez `use.boe.internal.biprws=true`.

Lorsque l'indicateur est défini sur vrai, les applications internes ne dépendent pas de l'URL de l'application RESTful ou de l'indicateur de chemin relatif défini dans la CMC.

Cette fonctionnalité est avantageuse car elle permet d'éviter ce qui suit :

- Problèmes CORS (Cross-Origin Resource Sharing)
- Problèmes de connectivité au système interne et externe

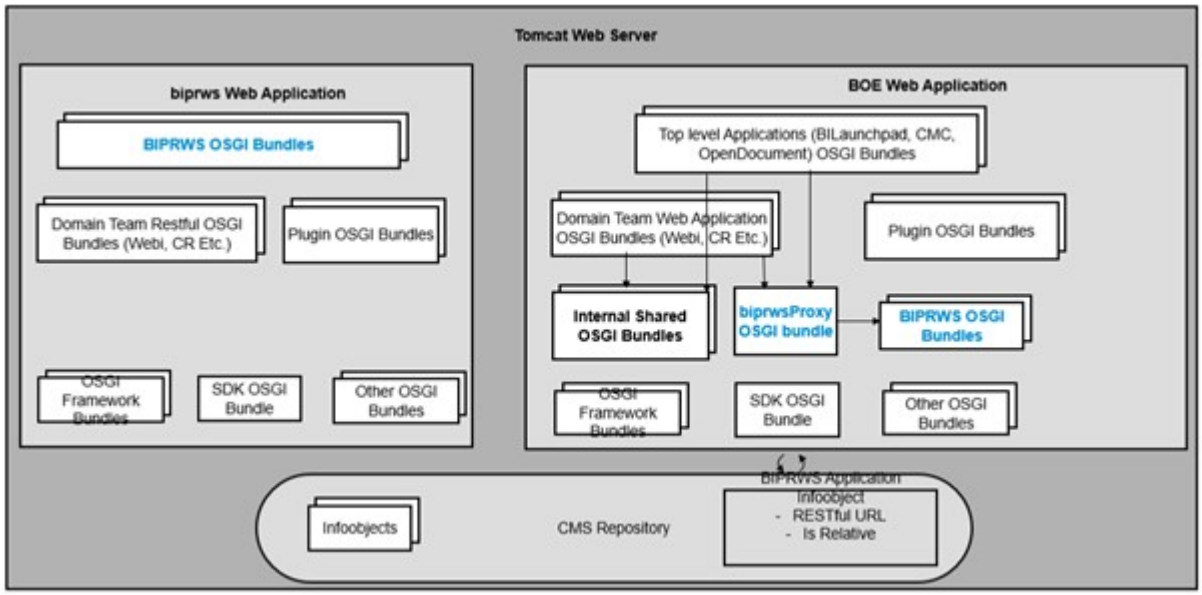
- Envoi d'une commande Ping à l'application Web BOE pour maintenir la session active
- Problèmes liés au proxy car il n'existe pas de configuration distincte pour BIPRWS et BOE.
- Problèmes liés au cluster d'applications Web.

Le déploiement existant avec l'application Web BOE fonctionne de manière transparente après la mise à niveau.

Journalisation :

Une fois BIPRWS fusionné dans l'application Web BOE, les journaux sont générés dans le cadre de l'emplacement de la zone de lancement BI ou du journal des applications de la CMC.

Architecture :



33 HSTS (Strict Transport Security) HTTP

33.1 Configuration de HSTS (Strict Transport Security) HTTP

HSTS (Strict Transport Security) HTTP est un mécanisme politique qui aide les sites Web à lutter contre les attaques internes telles que les attaques de mise à niveau inférieur de protocole et les détournements de cookies.

Il permet aux serveurs Web de déclarer que les navigateurs Web (ou d'autres agents utilisateurs conformes) doivent interagir automatiquement avec lui en utilisant uniquement des connexions HTTPS. On obtient alors un protocole Transport Layer Security (TLS/SSL), contrairement à une utilisation HTTP non sécurisée.

HSTS est un protocole standard IETF et est spécifié dans la RFC 6797.

La politique HSTS est communiquée par le serveur à l'agent utilisateur via un champ d'en-tête de réponse HTTP nommé "Strict-Transport-Security".

1. Cette politique spécifie une période pendant laquelle l'agent utilisateur doit uniquement accéder au serveur de manière sécurisée.
2. La plupart du temps, les sites qui utilisent le protocole HSTS n'acceptent pas la navigation en clair HTTP, soit en refusant les connexions via HTTP, soit en redirigeant systématiquement les utilisateurs vers HTTPS (bien que cela ne soit pas requis par la spécification).
   Cela permet de s'assurer qu'un agent utilisateur qui n'est pas capable d'établir un protocole TLS n'est peut-être pas en mesure de se connecter au site.
3. La protection ne s'applique qu'après qu'un utilisateur a visité le site au moins une fois en s'appuyant sur le principe de la confiance lors de la première utilisation.

Fonctionnement

Lorsqu'un utilisateur saisit ou sélectionne une URL sur le site qui spécifie HTTP, l'URL effectue automatiquement une montée de version vers HTTPS sans effectuer de requête HTTP. Cela permet d'éviter une attaque interne.

Dans la version 4.3 SP03, SAP BOE prend en charge la disposition HSTS.

Avant de configurer HSTS, votre serveur d'applications doit être configuré avec SSL.

Pour activer la prise en charge HSTS, exécutez les étapes ci-dessous :

1. Arrêtez Tomcat.
2. Accédez à `E:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default`.
3. Ouvrez le fichier Global.properties et définissez les paramètres ci-dessous.
   1. `hsts.enabled` True/False. La valeur par défaut est définie sur False.
   2. `hsts.Include.SubDomains` True /False - Affecte tous les sous-domaines du nom de domaine.
   3. `hsts.MaxAge.Seconds` = 31536000.
   4. Par défaut = 365 jours.

4. Enregistrez les modifications.

34 Annexe relative aux droits

34.1 A propos de l'annexe relative aux droits

Cette annexe relative aux droits répertorie et décrit la plupart des droits qui peuvent être définis sur différents objets du système de la plateforme de BI. Pour les situations dans lesquelles vous avez besoin de plusieurs droits pour effectuer une tâche sur un objet, elle fournit également des informations sur les droits supplémentaires requis ainsi que sur les objets auxquels doivent s'appliquer ces droits. Pour en savoir plus sur la définition des droits, voir le chapitre *Définition des droits* du *Guide d'administration de la plateforme SAP BI*.

34.2 Droits généraux

Les droits mentionnés dans cette section s'appliquent à différents types d'objets. De nombreux droits généraux possèdent également des droits de propriétaire équivalents. Les droits de propriétaire sont les droits qui s'appliquent uniquement au propriétaire de l'objet pour lequel les droits sont vérifiés.

Les droits suivants s'appliquent uniquement aux objets pouvant être planifiés :

- Droit *Planifier l'exécution du document*.
- Droit *Planifier de la part d'autres utilisateurs*.
- Droit *Planifier vers des destinations*.
- Droit *Afficher les instances du document*.
- Droit *Supprimer les instances*.
- Droit *Suspendre et reprendre les instances du document*.
- Droit *Replanifier les instances*.

Droit	Description
Visualiser les objets	Permet de visualiser les objets et leurs propriétés. Si vous ne possédez pas ce droit sur un objet, ce dernier est masqué dans le système de la plateforme de BI. Il s'agit d'un droit de base requis pour toutes les tâches.
Ajouter les objets au dossier	Permet d'ajouter des objets à un dossier. Ce droit s'applique également aux objets qui se comportent comme des dossiers tels que les boîtes de réception, les dossiers `Favoris` ou les lots d'objets.
Modifier les objets	Permet de modifier le contenu d'un objet mais également les propriétés des objets et des dossiers.

Droit	Description
Modifier les droits des utilisateurs sur les objets	Permet de modifier les paramètres de sécurité d'un objet.
Modifier en toute sécurité les droits des utilisateurs sur les objets	Permet d'accorder des droits ou des niveaux d'accès que vous possédez déjà sur un objet à d'autres utilisateurs. Pour ce faire, vous avez besoin de ce droit sur l'utilisateur ainsi que sur l'objet concerné. Pour en savoir plus sur ce droit, voir le chapitre « Définition des droits » du *Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence*.
Définir les groupes de serveurs pour traiter les travaux	Permet de spécifier le groupe de serveurs à utiliser pour le traitement des objets. Ce droit s'applique uniquement aux objets pour lesquels vous pouvez spécifier des serveurs de traitement. Pour spécifier un groupe de serveurs, vous avez également besoin du droit *Modifier les objets* sur l'objet.
Supprimer les objets	Permet de supprimer les objets ainsi que leurs instances.
Copier les objets dans un autre dossier	Permet de créer des copies des objets dans d'autres dossiers du CMS. Pour ce faire, vous avez également besoin du droit *Ajouter les objets au dossier* sur le dossier de destination. **Remarque** Lorsqu'un objet est copié, la sécurité explicite sur l'objet n'est pas copiée ; le nouvel objet hérite des paramètres de sécurité à partir du dossier de destination, mais vous devez redéfinir une sécurité explicite.
Répliquer le contenu	Permet de répliquer les objets sur un autre système d'une fédération.
Planifier l'exécution du document	Permet de planifier les objets.
Planifier de la part d'autres utilisateurs	Permet de planifier des objets pour d'autres utilisateurs ou groupes. L'utilisateur ou le groupe pour lequel vous planifiez l'objet devient le propriétaire de l'instance de l'objet. Pour planifier un objet pour d'autres utilisateurs ou groupes, vous avez également besoin des droits suivants : • Ce droit sur l'utilisateur ou le groupe. • Droit *Planifier l'exécution du document* sur l'objet.
Planifier vers des destinations	Le droit *Planifier vers des destinations* est le droit parent de *Planifier vers FTP, SMTP, Boîte de réception BI, SFTP* et

Droit	Description
	Système de fichiers. Sélectionnez le droit *Planifier vers des destinations* en combinaison avec le droit enfant spécifique pour planifier un objet vers une destination spécifique. Par exemple, vous devez sélectionner les droits *Planifier vers des destinations* et *Planifier vers FTP* pour planifier un objet vers une destination FTP. Si vous mettez à jour l'infrastructure BI à partir de BI 4.2 SP04 ou version antérieure vers BI 4.2 SP05 ou une version ultérieure, voir les notes SAP 2675734, 2642221, 2626550 pour plus d'informations sur la correction des erreurs. Pour planifier un objet vers des destinations, vous avez également besoin des droits suivants : • Droit *Planifier l'exécution du document* sur l'objet à planifier. • Droit *Ajouter les objets au dossier* sur la boîte de réception du destinataire (si vous souhaitez planifier vers une boîte de réception). • Droit *Copier les objets dans un autre dossier* sur l'objet à planifier (si vous souhaitez envoyer une copie vers une boîte de réception à la place d'un raccourci). **Remarque** Si le droit *Planifier vers des destinations* est affecté par *Niveau d'accès* tel qu'un rôle *Contrôle total* ou *Planifier* dans BI 4.2 SP04 ou version antérieure, alors après la mise à jour vers BI 4.2 SP05 Patch 03 ou version supérieure, les droits enfant sur la destination tels que *Planifier vers FTP, SMTP, SFTP, Boîte de réception BI* et *Système de fichiers* seront également accordés. Pour les *Niveaux d'accès* tels que les rôles *Visualiser à la demande* et les rôles *Personnalisés* existants dans BI 4.2 SP04 ou version antérieure, après la mise à jour vers BI 4.2 SP05 Patch 03 ou version supérieure, les droits enfant sur la destination ne sont pas accordés par défaut. Vous devez accorder les droits manuellement. Par conséquent, le job de planification de périodicité créé dans BI 4.2 SP04 ou version antérieure planifiera correctement les objets dans BI 4.2 SP05 Patch 03 ou version supérieure.
Planifier vers FTP	Permet de planifier l'envoi d'un objet vers une destination FTP.
Planifier vers SFTP	Permet de planifier l'envoi d'un objet vers une destination SFTP.
Planifier vers SMTP	Permet de planifier l'envoi d'un objet vers une destination SMTP.
Planifier vers le système de fichiers	Permet de planifier l'envoi d'un objet vers une destination Système de fichiers.

Droit	Description
Planifier vers la boîte de réception BI	Permet de planifier l'envoi d'un objet vers une destination Boîte de réception BI.
Afficher les instances du document	Permet de visualiser les instances de l'objet. Il s'agit d'un droit de base requis pour toutes les tâches effectuées sur les instances d'un objet.
Supprimer les instances	Permet de supprimer uniquement les instances des objets. Si vous disposez du droit *Supprimer les objets*, vous n'avez pas besoin de ce droit pour supprimer les instances.
Suspendre et reprendre les instances du document	Permet de suspendre et de reprendre les instances de l'objet en cours d'exécution.
Replanifier les instances	Permet de replanifier les instances de l'objet.
Ajouter des commentaires - Commentaires BI	Permet à un utilisateur d'ajouter des commentaires à un document à l'aide de l'application Commentaires BI.
Supprimer des commentaires - Commentaires BI	Permet à un utilisateur de supprimer des commentaires à un document à l'aide de l'application Commentaires BI
Supprimer des commentaires créés par l'utilisateur - Commentaires BI	Permet à un utilisateur de supprimer d'un document des commentaires qu'il a créés à l'aide de l'application Commentaires BI.
Modifier des commentaires - Commentaires BI	Permet à un utilisateur de modifier des commentaires dans un document à l'aide de l'application Commentaires BI.
Modifier des commentaires créés par l'utilisateur - Commentaires BI	Permet à un utilisateur de modifier les commentaires qu'il a créés dans un document à l'aide de l'application Commentaires BI.
Afficher des commentaires - Commentaires BI	Permet à un utilisateur d'afficher des commentaires dans un document à l'aide de l'application Commentaires BI
Afficher des commentaires créés par l'utilisateur - Commentaires BI	Permet à un utilisateur d'afficher les commentaires qu'il a créés dans un document à l'aide de l'application Commentaires BI.
Masquer les commentaires - Commentaires BI	Permet à un utilisateur de masquer les commentaires dans un document à l'aide de l'application Commentaires BI

Droit	Description
Masquer les commentaires créés par l'utilisateur - Commentaires BI	Permet à un utilisateur de masquer les commentaires qu'il a créés dans un document à l'aide de l'application Commentaires BI.
Ajouter des commentaires en bloc - Commentaires BI	Permet à un utilisateur de migrer un document et les commentaires associés.

34.2.1 Droits sur la destination

Chaque destination est associée à un droit spécifique sur la destination. L'administrateur BOE doit s'assurer que les utilisateurs disposent des droits souhaités sur la destination.

Auparavant, lorsqu'un utilisateur disposait du droit *Planifier vers des destinations*, il pouvait planifier vers toutes les destinations disponibles. À partir de la version SP05, des droits individuels sur la destination ont été attribués aux utilisateurs où *Planifier vers des destinations* correspond uniquement à l'*Emplacement par défaut d'Enterprise*.

De nouveaux droits ont été introduits sous Droits généraux pour chaque destination :

- Planifier vers le système de fichiers
- Planifier vers FTP
- Planifier vers la boîte de réception
- Planifier vers SFTP
- Planifier vers SMTP
- Planifier vers Google Drive

Pour en savoir plus sur les *Droits généraux*, voir Droits généraux [page 1153].

Pour offrir ces options de destination lors de la planification, l'administrateur doit accorder des droits individuels respectifs sur la destination. Voir la Note SAP 2621878. Si l'utilisateur ne dispose que du droit *Planifier vers des destinations*, il ne pourra pas planifier vers la destination FTP, Boîte de réception, SFTP, SMTP et le système de fichiers.

Si le droit *Planifier vers des destinations* est affecté dans une version antérieure par Niveau d'accès, comme les rôles Contrôle total ou Planifier, après la mise à jour vers 4.2 SP05, des droits supplémentaires (nouvellement introduits) seront également accordés. Ainsi, la planification vers n'importe quelle destination s'effectue avec succès.

Si le droit est affecté par le niveau d'accès *Visualiser à la demande*, via n'importe quel rôle personnalisé ou qu'il est directement affecté (droit individuel, et non via n'importe quel rôle), seule la planification vers l'*Emplacement par défaut d'Enterprise* s'effectue avec succès et la planification vers les autres destinations échoue.

Pour en savoir plus, voir Options de destination et Propriétés de destination de courrier électronique

34.3 Droits sur les types d'objet spécifiques

34.3.1 Droits d'accès aux dossiers

Afin de faciliter l'administration des droits, il est recommandé de définir les droits sur les dossiers afin que leur contenu puisse hériter des paramètres de sécurité. Les droits d'accès aux dossiers incluent :

- Droits généraux qui s'appliquent à l'objet dossier.
- Droits spécifiques aux types s'appliquant au contenu du dossier (tels que le droit *Imprimer les données du rapport* dans les rapports Crystal).

34.3.2 Catégories

Les droits mentionnés dans cette section sont des droits généraux mais possédant une signification spécifique dans le contexte des catégories publiques et personnelles.

> **Remarque**
>
> Les objets faisant partie de catégories n'héritent d'aucun droit défini pour ces catégories.

Droit	Description
Ajouter les objets au dossier	Permet de créer des catégories à l'intérieur des catégories existantes. Ce droit n'est pas nécessaire pour ajouter des objets à une catégorie.
Modifier les objets	Permet d'effectuer les opérations suivantes : • Modifier les propriétés de la catégorie. • Déplacer la catégorie dans une autre catégorie, la première catégorie devenant ainsi sous-catégorie. • Ajouter des objets à la catégorie. • Supprimer des objets de la catégorie. Pour déplacer une catégorie dans une autre catégorie en tant que sous-catégorie, vous avez également besoin des droits suivants : • Droit *Supprimer les objets* sur la catégorie d'origine. • Droit *Ajouter les objets au dossier* sur la catégorie de destination.
Supprimer les objets	Permet de supprimer la catégorie.

34.3.3 Rapports Crystal

Les droits mentionnés dans cette section s'appliquent uniquement aux rapports Crystal.

> **Remarque**
>
> Ces droits s'appliquent uniquement lorsque les rapports Crystal se trouvent dans l'environnement de la plateforme de BI. Lorsque vous téléchargez des rapports Crystal sur votre disque local, ces droits ne sont pas effectifs. Afin de prévenir ce problème, vous pouvez refuser le droit *Télécharger les fichiers associés à l'objet* sur le rapport Crystal.

Droit	Description
Imprimer les données du rapport	Permet d'imprimer le rapport.
Actualiser les données du rapport	Permet d'actualiser les données du rapport.
Exporter les données du rapport	Permet d'exporter les données du rapport dans n'importe quel format lorsque vous visualisez le rapport en ligne dans le visualiseur de rapports Crystal. Pour exporter des données de rapport au format RPT, vous avez besoin du droit *Télécharger les fichiers associés à l'objet*.
Télécharger les fichiers associés à l'objet	Ce droit permet d'effectuer les opérations suivantes : • Exporter le rapport au format RPT. • Ouvrir le rapport dans Crystal Reports Designer. • Planifier le rapport au format RPT vers des destinations externes.

34.3.4 Documents Web Intelligence

Les droits présentés dans cette section s'appliquent uniquement aux documents Web Intelligence.

Droit	Description
Utiliser la liste de valeurs	Permet d'utiliser les listes de valeurs.
Exporter les données du rapport	Permet à l'utilisateur d'exporter les données des rapports au format Texte, CSV, Excel, PDF ou HTML. Cette commande permet également d'utiliser la commande Imprimer qui génère un fichier PDF imprimable.
Script de requête : activer la visualisation (SQL, MDX...)	Permet de visualiser les scripts de requêtes (SQL et MDX).

Droit	Description
Script de requête : activer la modification (SQL, MDX...)	Permet de modifier les scripts de requêtes (SQL et MDX). Vous pouvez également modifier les sources de données FHSQL (SQL à la carte)
Actualiser les données du rapport	Permet d'actualiser les données du document.
Modifier la requête	Permet de modifier les requêtes dans le document.
Actualiser la liste des valeurs	Permet d'actualiser la liste des valeurs des invites lorsque vous créez une invite ou lorsque vous visualisez un document. Pour ce faire, vous devez également disposer du droit *Utiliser la liste des valeurs* sur le document.
Envoyer à	Permet d'envoyer des documents à la Planification, à une boîte de réception de la plateforme de BI ou de les envoyer sous forme de liens hypertexte dans un courrier électronique. Ce droit permet également aux utilisateurs de Web Intelligence Rich Client d'envoyer des documents sous forme de pièces jointes aux courriers électroniques.

34.3.5 Utilisateurs et groupes

Vous pouvez définir des droits sur les utilisateurs et les groupes de la même manière que pour d'autres objets dans l'environnement de la plateforme de BI. Les droits présentés dans cette section sont des droits spécifiques à un type qui s'appliquent uniquement aux objets utilisateur et groupe ou des droits généraux qui ont une signification particulière dans le contexte des utilisateurs et des groupes.

> **Remarque**
>
> Les utilisateurs et les sous-groupes peuvent hériter de droits d'une appartenance à un groupe.

> **Remarque**
>
> Le créateur d'un compte utilisateur est considéré comme le propriétaire du compte. Toutefois, une fois le compte utilisateur créé, cet utilisateur, pour lequel le compte est créé, est également considéré comme propriétaire du compte.

Droit	Description
Modifier les objets	Permet d'effectuer les opérations suivantes : • Modifier les propriétés de l'utilisateur ou du groupe. • Gérer l'appartenance au groupe. Pour ajouter un utilisateur ou un groupe à un autre groupe, vous devez disposer de ce droit sur l'utilisateur ou le groupe, ainsi que sur le groupe de destination.

Droit	Description
Changer le mot de passe utilisateur	Permet d'effectuer les opérations suivantes : • Modifier le mot de passe de votre compte utilisateur. Pour ce faire, vous devez également disposer du droit *Modifier les objets* sur le compte utilisateur. • Modifier le mot de passe du compte d'un autre utilisateur. Pour ce faire, vous devez également disposer des droits *Modifier les objets* et *Modifier les droits des utilisateurs sur les objets* sur le compte utilisateur. **Remarque** Ce droit n'affecte pas les paramètres de mot de passe utilisateur suivants : *Le mot de passe n'expire jamais* *L'utilisateur doit modifier le mot de passe à la prochaine session* *L'utilisateur ne peut pas changer de mot de passe* **Remarque** Ce droit ne s'applique pas aux références des données source des univers SAP BusinessObjects.
S'abonner aux publications	Permet d'ajouter l'utilisateur aux publications en tant que destinataire.
Planifier de la part d'autres utilisateurs	Permet de planifier des objets de la part de l'utilisateur afin que cet utilisateur devienne propriétaire de l'instance de l'objet. Pour ce faire, vous devez également disposer du droit *Planifier de la part d'autres utilisateurs* sur l'objet.
Ajouter des attributs utilisateur ou les modifier	Permet de modifier la valeur de l'adresse électronique d'un utilisateur ou de personnaliser les attributs utilisateur. Ce droit est applicable aux utilisateurs.
Ajouter des attributs utilisateur ou les modifier (droit du propriétaire)	Permet au propriétaire d'un objet utilisateur de modifier la valeur de l'adresse électronique d'un utilisateur ou de personnaliser les attributs utilisateur. Ce droit est applicable aux utilisateurs.
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu Préférences ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour

Droit	Description
	les rapports dans l'application Web Intelligence ou la barre de lancement BI.

34.3.6 Niveaux d'accès

Les droits mentionnés dans cette section s'appliquent uniquement aux niveaux d'accès.

Droit	Description
Utiliser le niveau d'accès pour l'affectation de la sécurité	Permet d'affecter le niveau d'accès lorsque vous ajoutez des utilisateurs ou des groupes principaux à des listes de contrôle d'accès pour les objets. Pour ce faire, vous devez également disposer du droit *Modifier les droits des utilisateurs sur les objets* ou *Modifier en toute sécurité les droits des utilisateurs sur les objets* sur l'utilisateur ou le groupe principal et sur l'objet. Pour les cas où le droit *Modifier en toute sécurité les droits des utilisateurs sur les objets* est affecté, vous devez également disposer du même niveau d'accès sur l'objet.

34.3.7 Droits d'univers (.unv)

Les droits mentionnés dans cette section s'appliquent aux univers créés à l'aide de l'outil de conception d'univers ou d'univers .unv. Les droits présentés sont des droits spécifiques au type qui s'appliquent uniquement aux univers ou des droits généraux qui ont une signification particulière dans le contexte des univers.

> **Remarque**
>
> Les droits d'univers s'appliquent uniquement lorsque vous importez des univers du CMS dans l'application Outil de conception d'univers. Ces droits ne s'appliquent pas lorsque l'univers est enregistré sur le disque local.

Droit	Description
Ajouter les objets au dossier	Permet d'ajouter des ensembles de restrictions ou des objets à l'univers. Pour ce faire, vous devez également disposer du droit *Modifier les restrictions d'accès*.
Visualiser les objets	Permet d'accéder à l'univers et de le visualiser.
Modifier les objets	Ce droit permet d'effectuer les opérations suivantes :

Droit	Description
	• Modifier l'univers dans la CMC ou dans l'outil de conception d'univers. • Verrouiller ou déverrouiller l'univers. Pour déverrouiller un univers, vous devez également disposer du droit *Déverrouiller l'univers*.
Supprimer les objets	Permet de supprimer l'univers.
Traduire les objets	Permet de sauvegarder les noms d'objets d'univers traduits à l'aide de l'outil de gestion de la traduction. **Remarque** Vous pouvez aussi sauvegarder des traductions si vous disposer explicitement du droit *Modifier les objets* et que le droit *Traduire les objets* ne vous a pas été explicitement refusé.
Nouvelle liste de valeurs	Ce droit permet d'effectuer les opérations suivantes : • Associer de nouvelles listes de valeurs à des objets. • Modifier des listes de valeurs existantes. **Remarque** Ce droit n'empêche pas de créer des listes de valeurs en cascade.
Imprimer l'univers	Permet d'imprimer l'univers.
Afficher les valeurs de table ou d'objet	Permet d'afficher les valeurs associées aux tables ou aux objets de l'univers.
Modifier les restrictions d'accès	Permet de modifier les restrictions d'accès (surcharges) de l'univers.
Déverrouiller l'univers	Permet d'effectuer les opérations suivantes : • Déverrouiller l'univers s'il a été verrouillé par un autre utilisateur. • Exporter l'univers à partir du CMS. Pour déverrouiller un univers, vous devez également disposer du droit *Modifier les objets*.
Accès aux données	Permet d'extraire les données de l'univers et d'actualiser les documents en fonction de l'univers. Pour ce faire, vous devez également disposer de ce droit sur l'application Outil de conception d'univers le document et la connexion d'univers.

Droit	Description
Créer et modifier des requêtes se basant sur un univers	Permet de créer des documents et de modifier des requêtes basées sur l'univers.

34.3.8 Droits d'univers (.unx)

Les droits mentionnés dans cette section s'appliquent aux univers créés à l'aide de l'outil de conception d'information ou d'univers .unx. Les droits présentés sont des droits spécifiques au type qui s'appliquent uniquement aux univers ou des droits généraux qui ont une signification particulière dans le contexte des univers.

> **Remarque**
>
> Les droits d'univers s'appliquent uniquement aux univers publiés dans un référentiel. Ces droits ne s'appliquent pas lorsque l'univers est enregistré dans un dossier local.

Droit	Description
Visualiser les objets	Permet d'accéder à l'univers et de le visualiser.
Modifier les objets	Permet de republier l'univers.
Supprimer les objets	Permet de supprimer l'univers.
Extraire l'univers	Permet d'extraire un univers publié et de modifier les ressources sous-jacentes (couche de gestion et fondation de données) dans l'outil de conception d'information. **Remarque** Vous devez également disposer du droit *Extraire l'univers* de l'application Outil de conception d'information.
Modifier les profils de sécurité	Permet d'insérer, de modifier et de supprimer des profils de sécurité pour l'univers dans l'éditeur de sécurité de l'outil de conception d'information. **Remarque** Ce droit n'est pas requis pour afficher les profils de sécurité ou modifier les options d'agrégation de profils de sécurité.
Affecter des profils de sécurité	Permet d'affecter des profils de sécurité à des utilisateurs et des groupes ou d'annuler ces affectations dans l'éditeur de sécurité de l'outil de conception d'information.

Droit	Description
Accès aux données	Permet d'extraire les données de l'univers et d'actualiser les documents en fonction de l'univers. Dans l'outil de conception d'information, ce droit permet d'afficher un aperçu de l'ensemble de résultats dans l'Editeur de requête.
Créer et modifier des requêtes se basant sur cet univers	Permet de créer et de modifier des requêtes basées sur un univers. Dans l'outil de conception d'information, ce droit vous permet d'ouvrir l'Editeur de requête et d'exécuter une requête sur un univers.
Enregistrer pour tous les utilisateurs	Permet d'enregistrer l'univers pour tous les utilisateurs. **Remarque** Vous devez également disposer du droit Enregistrer pour tous les utilisateurs de l'application *Outil de conception d'information*.

34.3.9 Niveaux d'accès aux objets d'univers

Lorsque les concepteurs créent un univers à l'aide de l'outil de conception d'univers ou une couche de gestion à l'aide de l'outil de conception d'information, ils affectent un niveau d'accès aux objets à chaque objet de l'univers. Les niveaux d'accès aux objets sont les suivants :

Public (par défaut)
Contrôlé
Restreint
Confidentiel
Privé

Une fois l'univers publié dans le référentiel, vous pouvez accorder des accès à des objets d'univers en fonction des niveaux d'accès affectés dans l'application. Par exemple, vous pouvez accorder l'accès Public au groupe Tout le monde. Cela permet aux utilisateurs de ce groupe d'afficher les objets dans l'univers désignés en tant que publics.

Chaque niveau d'accès aux objets accorde un niveau d'accès supérieur au niveau précédent. Public est le niveau le plus bas. Les utilisateurs/groupes principaux disposant de l'accès Public peuvent uniquement afficher les objets désignés en tant que publics. Les utilisateurs/groupes principaux disposant de l'accès Contrôlé peuvent afficher les objets désignés en tant que publics et contrôlés. Le paramètre Privé correspond au niveau le plus élevé. Il autorise les utilisateurs/groupes principaux à accéder à tous les niveaux d'accès aux objets ; en d'autres termes, à tous les objets de l'univers.

> **Remarque**
>
> Les paramètres de sécurité des niveaux d'accès aux objets remplacent les paramètres de sécurité dont l'univers hérite.

> **Remarque**
>
> Pour les univers .unx, les paramètres de sécurité des niveaux d'accès aux objets sont pris en compte avec la sécurité de l'objet définie par le profil de sécurité. Pour en savoir plus sur les profils de sécurité, voir le *Guide de l'utilisateur de l'outil de conception d'information*.

Informations associées

Affectation de niveaux d'accès aux objets d'univers [page 1166]

34.3.9.1 Affectation de niveaux d'accès aux objets d'univers

Pour définir un niveau de sécurité d'accès aux objets d'univers, vous devez disposer du droit *Modifier les droits des utilisateurs sur les objets* sur l'univers.

1. Dans la zone *Univers* du CMS, sélectionnez un univers.
2. Cliquez sur *Action* > *Sécurité de l'univers*.
3. Dans la boîte de dialogue *Sécurité de l'univers*, sélectionnez, pour l'utilisateur ou le groupe, le niveau d'accès aux objets dans la liste *Niveau de sécurité objet*.

34.3.10 Droits de connexion

Les droits mentionnés dans cette section sont des droits spécifiques au type qui s'appliquent aux connexions d'univers ou des droits généraux qui possèdent une signification spécifique dans le contexte des connexions d'univers. Ces droits s'appliquent aux connexions publiées dans le référentiel.

Droits de connexion relationnelle

Droit	Description
Visualiser les objets	Permet de visualiser la connexion.
Modifier les objets	Permet de modifier les paramètres de connexion.

Droit	Description
Télécharger la connexion localement	Permet d'utiliser des univers créés sur la connexion dans Web Intelligence Rich Client en mode hors ligne. Permet d'utiliser le pilote de middleware local dans l'outil de conception d'information. Pour ce faire, sélectionnez l'option du middleware local dans les préférences de l'outil de conception d'information, sans quoi les requêtes envoyées à la base de données utiliseront le middleware du serveur. Ce droit est également nécessaire pour modifier une connexion sécurisée dans l'outil de conception d'information.
Supprimer les objets	Permet de supprimer la connexion.
Copier les objets dans un autre dossier	Permet de copier la connexion d'un dossier dans un autre.
Accès aux données	Permet d'extraire du contenu de la base de données spécifiée dans la connexion. Dans l'outil de conception d'information, ce droit permet de parcourir les données de table de la connexion et les éditeurs de la fondation de données. Il permet aussi d'afficher un aperçu de l'ensemble des résultats dans l'Éditeur de requête.
Utiliser la connexion pour les procédures stockées	Permet d'utiliser les procédures stockées dans la base de données spécifiée pour la connexion à l'univers. **Remarque** Ce droit s'applique aux univers .unv uniquement.
Utilisez la connexion pour les scripts SQL à la carte	Vous permet d'exécuter des scripts SQL sur la connexion.

Droits de connexion OLAP

Droit	Description
Visualiser les objets	Permet de visualiser la connexion.
Modifier les objets	Permet de modifier les paramètres de connexion dans l'éditeur de connexion de l'outil de conception d'information.
Supprimer les objets	Permet de supprimer la connexion.

Droit	Description
Copier les objets dans un autre dossier	Permet de copier la connexion d'un dossier dans un autre.
Télécharger la connexion localement	Permet d'utiliser des univers créés sur la connexion dans Web Intelligence Rich Client en mode hors ligne.

34.3.11 Applications

34.3.11.1 CMC

Droit	Description
Se connecter à la CMC pour accéder à cet objet dans la CMC	Permet à un utilisateur de se connecter à la CMC.
Autoriser l'accès au Gestionnaire d'instances	Permet à un utilisateur d'accéder au Gestionnaire d'instances.
Autoriser l'accès à la requête de relation	Permet à un utilisateur d'exécuter des requêtes de relation dans la CMC.
Autoriser l'accès à la requête de sécurité	Permet à un utilisateur d'exécuter des requêtes de sécurité dans la CMC.

34.3.11.2 Zone de lancement BI façon Fiori

Droit	Description
Se connecter à la nouvelle zone de lancement BI façon Fiori	Permet à un utilisateur de se connecter à la zone de lancement BI façon Fiori.
Organiser	Permet à un utilisateur de déplacer et de copier des objets, de les ajouter au dossier `Favoris` et de créer des raccourcis vers les objets.
Envoyer vers la boîte de réception Business Objects	Permet à un utilisateur d'envoyer des objets dans les boîtes de réception BI destinataires.
Envoyer vers la destination du courrier électronique	Permet à un utilisateur d'envoyer des objets aux destinataires par courrier électronique.
Envoyer vers l'emplacement de fichier	Permet à un utilisateur d'envoyer des objets vers un emplacement de fichier.

Droit	Description
Envoyer vers l'emplacement FTP	Permet à un utilisateur d'envoyer des objets vers un emplacement FTP.
Envoyer vers l'emplacement SFTP	Permet à un utilisateur d'envoyer des objets vers un emplacement SFTP. Les propriétés de la destination SFTP sont similaires à celle de la page de destination FTP, avec une option supplémentaire d'empreinte devant être fournie par l'utilisateur. Chaque serveur SFTP comporte dans ses propriétés une option d'empreinte. La comparaison/validation est effectué par le CMS dans le backend.

34.3.11.2.1 Droits pour les applications de collaboration

Ces droits d'accès s'appliquent à SAP Jam lorsque l'application est configurée dans la plateforme de BI.

Droit	Description
Commenter les documents possédés par l'utilisateur	Permet à un utilisateur d'ajouter des commentaires pour des documents et des instances qu'il possède.
Afficher les commentaires sur les documents possédés par l'utilisateur	Permet à un utilisateur d'afficher des commentaires pour des documents et des instances qu'il possède.
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports de l'application.

34.3.11.3 Espaces de travail BI

Droit	Description
Créer et modifier des espaces de travail BI	Permet à un utilisateur de créer des espaces de travail BI et de modifier des espaces de travail BI existants.
Créer et modifier des modules	Permet à un utilisateur de créer des modules et de modifier des modules existants.

Droit	Description
Modifier les espaces de travail BI	Permet à un utilisateur de modifier les espaces de travail BI existants (mais ne lui permet pas de créer des espaces de travail).
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

34.3.11.4 Web Intelligence

Les droits d'accès présentés dans cette section s'appliquent à l'application Web Intelligence (y compris à Rich Client) et peuvent affecter les visualiseurs et les éditeurs de requêtes de l'application.

Droit	Description
Données : activer le suivi des données	Permet à un utilisateur d'effectuer le suivi des données modifiées.
Données : activer la mise en forme des données modifiées	Permet à un utilisateur de sélectionner la mise en forme des données modifiées.
Général : activer l'accès client à Desktop	Permet à l'utilisateur d'utiliser Web Intelligence Desktop (Rich Client).
Desktop : exporter des documents	Dans Web Intelligence Rich Client, permet à un utilisateur d'exporter des documents vers le référentiel de la plateforme de BI.
Desktop : enregistrer les documents pour tous les utilisateurs	Dans Web Intelligence Rich Client, permet à un utilisateur d'enregistrer des documents localement sans aucune sécurité.
Documents : désactiver l'actualisation automatique à l'ouverture	Empêche l'actualisation automatique des documents lorsqu'ils sont ouverts.
Documents : activer l'enregistrement automatique	Permet d'enregistrer automatiquement les documents si l'enregistrement automatique est activé par l'administrateur dans la CMC.
Documents : activer la création	Permet à un utilisateur de créer des documents.
Général : modifier les préférences Web Intelligence	Permet à un utilisateur de modifier les préférences Web Intelligence dans la zone de lancement BI.

Droit	Description
Général : activer l'accès client Web	Permet à l'utilisateur d'utiliser le client Web Web Intelligence.
Requête : modifier le script généré à partir de l'univers	Dans l'Éditeur de requête, permet à un utilisateur de modifier les scripts de requête SQL ou MDX générés à partir de l'univers.
Requête : modifier le SQL à la carte	Permet à un utilisateur de modifier les scripts de requêtes SQL à la carte.
Requête : afficher le script généré à partir de l'univers	Dans l'Éditeur de requête, permet à un utilisateur de visualiser les scripts de requête SQL ou MDX générés à partir de l'univers.
Requête : afficher le SQL à la carte	Permet à un utilisateur de visualiser les scripts de requêtes SQL à la carte.
Reporting : créer des sauts de page et les modifier	Permet à un utilisateur de créer et de modifier des sauts.
Reporting : créer des règles de mise en forme conditionnelles et les modifier	Permet à un utilisateur de créer et de modifier des règles de mise en forme conditionnelles.
Reporting : créer des calculs prédéfinis et les modifier	Permet à un utilisateur de créer et de modifier des calculs prédéfinis.
Reporting : créer et modifier des contrôles d'entrée et des groupes	Permet à un utilisateur de créer et de modifier des contrôles d'entrée.
Reporting : créer et modifier des filtres de rapport et utiliser des contrôles d'entrée	Permet à l'utilisateur de créer et de modifier des filtres de rapport et également d'utiliser les contrôles d'entrée.
Reporting : créer des tris et des classements et les modifier	Permet à l'utilisateur de créer et de modifier des tris et des classements.
Reporting : créer des formules, des variables, des groupes et des références	Permet à l'utilisateur de créer des formules, des variables, des groupes et des références.
Reporting : activer la modification de document	Permet à un utilisateur de modifier la mise en forme du rapport. Sans ce droit d'accès, le mode Conception n'est pas disponible.
Reporting : fusionner les objets	Permet à un utilisateur de synchroniser les données à l'aide de dimensions fusionnées dans les rapports et dans le gestionnaire de données.
Reporting : insérer et supprimer des rapports, des tableaux, des diagrammes et des cellules	• Permet à un utilisateur d'insérer et de supprimer des rapports, des tableaux, des diagrammes et des cellules. • Autorise le workflow des doublons (copier/coller).

34.3.11.5 Outil de conception d'univers

Droit	Description
Vérifier l'intégrité de l'univers	Permet à un utilisateur de vérifier l'intégrité de l'univers.

Droit	Description
Actualiser la fenêtre de structure	Permet à un utilisateur d'actualiser la fenêtre Structure.
Utiliser la liste des tables	Permet à un utilisateur d'afficher les données de la base de données à l'aide de la liste des tables.
Appliquer les contraintes de l'univers	Permet à un utilisateur d'appliquer des contraintes d'univers prédéfinies aux utilisateurs d'un univers importé.
Lier l'univers	Permet à un utilisateur de lier deux univers et de partager des composants.
Créer, modifier ou supprimer des connexions	Permet à un utilisateur de créer, de modifier et de supprimer des connexions d'univers stockées dans le référentiel de la plateforme de BI ou stockées en tant que connexions personnelles ou partagées.
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

34.3.11.6 Outil de conception d'information

Droit	Description
Administrer des profils de sécurité	Permet à un utilisateur d'ouvrir l'éditeur de sécurité Pour utiliser des profils de sécurité, vous devez également disposer de droits sur l'univers.
Partager des projets	Permet à un utilisateur de partager un projet local et de synchroniser un projet partagé avec le projet local.
Créer, modifier ou supprimer des connexions	• Permet à un utilisateur de créer et de supprimer les connexions sécurisées de la vue Ressources publiées. • Permet à un utilisateur de modifier des connexions dans l'éditeur de connexion. • Permet à un utilisateur de publier des connexions dans un référentiel.

Droit	Description
Publier l'univers	Permet à un utilisateur de publier des univers dans un référentiel.
Extraire l'univers	Permet à un utilisateur d'extraire des univers publiés dans un projet local qui sera modifié.
Enregistrer pour tous les utilisateurs	Permet à un utilisateur d'enregistrer tous les utilisateurs lors de l'extraction des univers.
Calculer des statistiques	Permet à un utilisateur de sélectionner des tables et des colonnes dans lesquelles calculer et publier des statistiques.
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

34.3.11.7 Alertes

Droit	Description
Déclencher les alertes	Permet à un utilisateur de déclencher des événements d'alerte. Pour déclencher une alerte pour un document, les droits supplémentaires suivants sont requis : • Droits "Afficher" et "Planifier" pour le document • Droits "Afficher" et "Déclenchement" pour l'événement correspondant
S'inscrire aux objets	Permet à un utilisateur de s'inscrire à un événement d'alerte. Pour s'inscrire à un événement, les droits supplémentaires suivants sont requis : • Droits "Afficher" pour l'événement correspondant • Droit "S'inscrire" pour le compte de l'utilisateur Pour s'inscrire à une alerte pour un document, les droits supplémentaires suivants sont requis : • Droit "Afficher" pour le document • Droit "Afficher l'instance" pour le document • Droits "Afficher" pour l'événement correspondant

Droit	Description
	• Droit "S'inscrire" pour le compte de l'utilisateur
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

34.3.11.8 SAP BusinessObjects Mobile

Droit	Description
Connexion à l'application SAP BusinessObjects Mobile	Permet à un utilisateur de se connecter à la plateforme de BI à partir de l'application Mobile et d'afficher des documents.
S'inscrire aux alertes de documents	Permet à un utilisateur de s'inscrire à des alertes de document et d'instance périodique. Si ce droit a été accordé à un utilisateur par le passé (même si tel n'est plus le cas), cet utilisateur peut toujours recevoir les alertes auxquelles il s'est inscrit. Les utilisateurs doivent se désinscrire expressément d'une alerte s'ils ne souhaitent pas la recevoir. Pour s'inscrire aux alertes de document et aux instances périodiques pour les planifications, un utilisateur doit disposer de l'accès "Contrôle total" au dossier `Evénements système` sous *Evénements* dans la CMC.
Enregistrer les documents dans le stockage local d'un appareil	Permet à un utilisateur d'enregistrer des documents sur un périphérique mobile. Si le droit "d'enregistrer les documents localement sur le périphérique" a été accordé à un utilisateur par le passé (même si tel n'est plus le cas) et que cet utilisateur a enregistré des documents sur le périphérique mobile, les documents existent toujours sur le périphérique mais ils ne sont pas synchronisés au cours du processus de synchronisation.

Droit	Description
Envoyer les documents d'un appareil sous forme de courrier électronique	Permet à un utilisateur d'envoyer des rapports dans un message électronique.
Modifier les préférences des objets que possède l'utilisateur	Affiche le menu *Préférences* dans un objet d'application. Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu *Préférences* ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

Pour en savoir plus, voir le *Guide d'installation et de déploiement de SAP BusinessObjects Mobile*.

34.3.11.9 Cockpit d'administration de BI

Droits	Description
Autoriser l'accès au cockpit d'administration de BI	Permet d'accéder au cockpit d'administration de BI dans la CMC.
Autoriser l'accès à la surveillance	Permet d'accéder à la surveillance dans le cockpit d'administration de BI.
Autoriser l'accès à la différence visuelle	Permet d'accéder à la différence visuelle dans le cockpit d'administration de BI.
Différence visuelle : créer la comparaison	Permet de créer de nouvelles comparaisons entre les InfoObjects dans la différence visuelle.
Différence visuelle : supprimer la comparaison	Permet de supprimer les comparaisons précédentes dans la différence visuelle.
Différence visuelle : réexécuter la comparaison	Permet de réexécuter les comparaisons déjà créées dans la différence visuelle.
Différence visuelle : afficher la comparaison	Permet d'afficher une comparaison dans la différence visuelle.

35 Annexe relative aux propriétés des serveurs

35.1 A propos de l'annexe relative aux propriétés des serveurs

Cette annexe relative aux propriétés des serveurs répertorie et décrit les propriétés pouvant être définies pour chaque serveur de la plateforme de BI.

35.1.1 Propriétés courantes du serveur

Les propriétés de serveur décrites dans cette section s'appliquent à tous les types de serveur.

Propriétés du port de requêtes

Propriété	Description	Valeur par défaut
Nom du serveur	Nom du serveur.	La valeur par défaut est le nom du nœud sur lequel se trouve le serveur, ainsi que le nom du serveur.
ID, CUID	L'ID court et l'ID unique de cluster du serveur. Lecture seule.	Ces valeurs sont générées automatiquement.
Nœud	Nom du nœud où le serveur est situé.	Cette valeur est spécifiée au cours de l'installation.
Description	Description du serveur	La valeur par défaut est le nom du serveur.
Paramètres de ligne de commande	Paramètres de ligne de commande pour le serveur.	La valeur par défaut dépend du type de serveur.
Port de requêtes	Spécifie le port depuis lequel le serveur reçoit les requêtes. Dans un environnement comportant des pare-feu, configurez le serveur pour qu'il écoute uniquement les requêtes provenant des ports ouverts sur les pare-feu. Si vous indiquez un port pour le serveur, assurez-vous qu'il n'est pas déjà utilisé par un autre processus. **Remarque** Si l'option *Affecter automatiquement* est sélectionnée, le serveur se lie à un port alloué de façon dynamique. Cela signifie qu'un numéro de port aléatoire est attribué au serveur à chaque fois qu'il redémarre.	Par défaut, *Affecter automatiquement* a pour valeur **TRUE** et le champ *Port de requêtes* est vide.

Propriété	Description	Valeur par défaut
Affecter automatiquement	Spécifie si le serveur se lie à un port attribué de façon dynamique à chaque fois qu'il redémarre. Pour lier le serveur à un port spécifique, attribuez à *Affecter automatiquement* la valeur **FALSE** et spécifiez un *Port de requêtes* valide.	La valeur par défaut est **TRUE**.

Propriétés de démarrage automatique

Propriété	Description	Valeur par défaut
Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent	Indique si le serveur démarre automatiquement lors du démarre ou redémarrage du SIA (Server Intelligence Agent). Si ce paramètre a pour valeur **FALSE** lorsque le SIA démarre ou redémarre, le serveur reste arrêté.	La valeur par défaut est **TRUE**.

Propriétés des identifiants de l'hôte

Propriété	Description	Valeur par défaut
Affecter automatiquement	Spécifie si le serveur se lie à une interface réseau affectée automatiquement. Si cette propriété est définie sur **FALSE**, le serveur se lie à une interface réseau spécifique. Si elle est définie sur **TRUE**, le serveur accepte les requêtes sur la première adresse IP disponible. Sur les ordinateurs multiconnectés, vous pouvez indiquer une interface réseau spécifique à laquelle lier le serveur en attribuant à ce paramètre la valeur **FALSE** et en fournissant un nom d'hôte ou une adresse IP valide.	La valeur par défaut est **TRUE**.
Nom d'hôte	Nom d'hôte de l'interface réseau à laquelle se lie le serveur. Si un nom d'hôte est indiqué, le serveur accepte les requêtes sur toutes les adresses IP associées au nom d'hôte.	Par défaut, *Affecter automatiquement* est défini sur **TRUE** et le champ *Nom d'hôte* est vide.
Adresse IP	Adresse IP de l'interface réseau à laquelle se lie le serveur. Les protocoles IPv4 et IPv6 sont tous deux pris en charge. Si une adresse IP est indiquée, le serveur accepte les requêtes sur l'adresse IP uniquement.	Par défaut, *Affecter automatiquement* est défini sur **TRUE** et le champ *Adresse IP* est vide.

Propriétés des modèles de configuration

Propriété	Description	Valeur par défaut
Utiliser le modèle de configuration	Spécifie si un modèle de configuration doit être utilisé.	La valeur par défaut est **FALSE**.
Restaurer les valeurs par défaut du système	Spécifie si les paramètres par défaut d'origine doivent être restaurés pour le serveur.	La valeur par défaut est **FALSE**.
Définir le modèle de configuration	Indique si vous souhaitez utiliser les paramètres du service actuel en tant que modèle de configuration pour tous les services de même type. Si ce paramètre a pour valeur **TRUE**, tous les services de même type spécifiés dans *Utiliser le modèle de configuration* sont immédiatement reconfigurés de façon à utiliser les paramètres du service actuel.	La valeur par défaut est **FALSE**.

Propriétés du service de journal de suivi

Propriété	Description	Valeur par défaut
Niveau de journalisation	Spécifie le degré d'avertissement minimal que vous souhaitez consigner et détermine le volume d'informations enregistré dans le fichier journal du serveur. Les niveaux de seuil de journalisation possibles sont les suivants : • *Non spécifié* • *Aucun* • *Faible* • *Moyen* • *Elevé*	La valeur par défaut est **`Non spécifié`**.

35.1.2 Propriétés des services principaux

La catégorie Services principaux comprend les serveurs suivants :

- Adaptative Job Server
- Serveur de traitement adaptatif
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Serveur conteneur d'applications Web

Propriétés d'Adaptative Job Server

Propriétés générales

Propriété	Description	Valeur par défaut
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant. Pour améliorer la performance, assurez-vous que ce répertoire se trouve sur un disque local. **Remarque** Vous devez redémarrer le serveur pour valider les modifications.	%DefaultDataDir%

L'Adaptive Job Server peut héberger plusieurs services différents. Chaque service contient les propriétés suivantes :

Propriétés des services

Propriété	Description	Valeur par défaut
Nombre maximal de travaux simultanés	Nombre de processus indépendants simultanés (processus enfant) autorisé par le serveur. Vous pouvez personnaliser ce nombre en fonction de vos besoins en matière de reporting. Le paramètre par défaut convient pour la plupart des scénarios de reporting. Le paramètre idéal pour votre environnement de reporting dépend de votre configuration matérielle, de votre logiciel de base de données et de vos besoins en matière de reporting.	5
Nombre maximal de demandes enfant	Indique le nombre de travaux traités par l'enfant avant le redémarrage.	100

Propriétés du serveur de traitement adaptatif

Propriétés générales

Propriété	Description	Valeur par défaut
Délai d'expiration du démarrage des services (secondes)	Délai, en secondes, accordé par le serveur pour le démarrage des services. Lorsqu'un service ne démarre pas dans le délai spécifié, deux raisons sont possibles : • Le démarrage peut avoir échoué, par exemple, parce qu'une ressource requise (telle qu'une base de données) était introuvable ou parce que le service a rencontré un conflit de ports. • Il se peut également que le service n'ait pas pu démarrer dans le délai spécifié en raison, par exemple, de la lenteur du système. Pour connaître la raison, consultez le fichier journal du serveur. Si le service ne démarre pas dans le délai spécifié, essayez d'augmenter cette valeur.	1200

Propriétés du service proxy d'audit client

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de jetons de sécurité

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service Insight to Action

Métrique	Description	
Nombre maximal de connexions actives par session utilisateur	Nombre maximal de connexions avec le serveur SAP pour un utilisateur sur une période donnée. Lorsqu'un utilisateur ouvre un rapport ou un tableau de bord compatible RRI, une connexion avec le serveur SAP est établie pour déterminer les cibles RRI disponibles.	20
Nombre maximal de connexions inactives par session utilisateur	Nombre de connexions inactives à conserver ouvertes et à réutiliser pour les requêtes RRI suivantes. L'augmentation de ce paramètre entraîne l'affectation de ressources système supplémentaires.	20
Temps d'attente maximal de connexion (en secondes)	Durée pendant laquelle la structure Insight to Action doit attendre une réponse du serveur SAP avant d'expirer (en secondes).	30

Propriétés du service de publication

Propriété	Description	Valeur par défaut
Taille du pool de threads	Spécifie le nombre de threads de traitement ScopeBatch pouvant être exécutés en même temps. Si la valeur de cette propriété est définie sur « 0 », la taille du pool de threads est déterminée à l'aide d'une formule basée sur le nombre de cœurs d'UC de l'ordinateur.	0

Propriétés du service de traduction

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de surveillance

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de recherche de plateformes

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de post-traitement de la publication

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du Central Management Server

> **Remarque**
>
> Lorsque vous modifiez l'une de ces propriétés de serveur, redémarrez le serveur pour valider les modifications.

Propriétés du service de gestion centralisée

Propriété	Description	Valeur par défaut
Port du serveur de noms	Spécifie le port sur lequel le CMS écoute les requêtes de service de noms d'origine.	6400
Connexions à la base de données système requises	Nombre de connexions à la base de données système que le CMS tente d'établir. Si le serveur ne parvient pas à établir toutes les connexions requises à la base de données, il continue de fonctionner mais de façon réduite, puisque moins de requêtes simultanées peuvent être servies en même temps. Le CMS tente d'établir des connexions supplémentaires jusqu'à ce que le nombre de connexions requises soit atteint. La métrique *Connexions à la base de données système établies* du CMS indique le nombre actuel de connexions établies.	14
Reconnexion automatique à la base de données système	Indique si le CMS essaie automatiquement de rétablir une connexion à la base de données en cas de défaillance du service. Si ce paramètre a pour valeur **FALSE**, vous pouvez vérifier l'intégrité de la base de données CMS avant de rétablir la connexion ; vous devez redémarrer le CMS afin de rétablir la connexion à la base de données.	**TRUE**

Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique à une source de données avant qu'elle n'expire. S'applique aux utilisateurs Windows AD exécutant des rapports qui sont configurés pour une connexion unique Windows AD à la source de données.	86400

Propriétés de l'Event Server

Propriétés du service d'événements

Propriété	Description	Valeur par défaut
Intervalle entre les interrogations d'événement (secondes)	Indique la fréquence (en secondes) à laquelle le serveur interroge un fichier qui déclenche un événement.	10 La plage des valeurs autorisées s'étend de 1 à 1 200 secondes.
Intervalle de nettoyage (minutes)	Fréquence (en minutes) d'exécution de l'utilitaire de nettoyage.	20

Propriétés de l'Input File Repository Server

Propriétés du service de stockage des fichiers d'entrée

Propriété	Description	Valeur par défaut
Répertoire de stockage des fichiers	Spécifie le répertoire dans lequel sont stockés les objets du référentiel des fichiers. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultInputFRSDir/%
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant. Pour assurer de meilleures performances, il est recommandé que le *Répertoire temporaire* soit situé sur le même système de fichiers que le *Répertoire de stockage des fichiers*.	%DefaultInputFRS-Dir/temp%
Durée d'inactivité maximale (minutes)	Délai accordé par le serveur avant de procéder à la fermeture des connexions inactives. L'attribution d'une valeur trop basse peut entraîner la clôture prématurée de la requête d'un utilisateur. L'attribution d'une valeur trop élevée peut entraîner une consommation excessive des ressources du système, telles que le temps de traitement et l'espace disque.	10
Nombre maximal de tentatives d'accès au fichier	Nombre de tentatives d'accès à un fichier effectué par le serveur.	1
Emplacement du fichier de l'adaptateur de l'analyse anti-virus	Indique le chemin d'accès absolu vers l'emplacement du fichier de l'adaptateur de l'analyse anti-virus.	

Propriétés de l'Output File Repository Server

Propriétés du service de stockage des fichiers de sortie

Propriété	Description	Valeur par défaut
Répertoire de stockage des fichiers	Spécifie le répertoire dans lequel sont stockés les objets du référentiel des fichiers. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultOutputFRSDir/%

Propriété	Description	Valeur par défaut
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultOutputFRS-Dir/temp%
Durée d'inactivité maximale (minutes)	Délai accordé par le serveur avant de procéder à la fermeture des connexions inactives. L'attribution d'une valeur trop basse peut entraîner la clôture prématurée de la requête d'un utilisateur. L'attribution d'une valeur trop élevée peut entraîner une consommation excessive des ressources du système, telles que le temps de traitement et l'espace disque.	10
Nombre maximal de tentatives d'accès au fichier	Nombre de tentatives d'accès à un fichier effectué par le serveur.	1

Propriétés du serveur conteneur d'applications Web

Propriétés générales

Propriété	Description	Valeur par défaut
Délai d'expiration du démarrage des services (secondes)	Durée pendant laquelle le serveur WACS attend le démarrage des services hébergés avant que le démarrage n'expire. En cas de dépassement du délai d'expiration, le serveur WACS ne fournit pas les services qui n'ont pas encore démarré. Sur un ordinateur plus lent, vous pouvez envisager de spécifier un délai plus long. Si vous spécifiez un délai trop court et que le serveur WACS ne démarre pas avant l'expiration du délai, restaurez les paramètres par défaut du serveur WACS via le CCM (Central Configuration Manager).	1200

Propriétés du service TraceLog

Propriété	Description	Valeur par défaut
Niveau de journalisation	Permet la connexion et définit le niveau de gravité et de détail sur Aucun (uniquement les événements essentiels journalisés), Faible (démarrage, fermeture, messages de requête de début et de fin), Moyen (messages d'erreur, d'avertissement et la plupart des messages d'état) ou Elevé (Rien d'exclus). Utilisation réservée au débogage. Augmentation possible de la consommation de l'unité centrale, affectant sa performance). Les choix de menu disponibles sont : • *Non spécifié* • *Aucun* • *Faible* • *Moyen* • *Elevé*	Non spécifié

Propriétés du service BI du processus de gestion

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service du générateur de requêtes

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Service Web RESTful - propriétés de configuration des propriétés système

Propriété	Description	Valeur par défaut
Afficher la pile d'erreurs	Lorsqu'il est activé, le journal des erreurs inclus les messages d'erreur du service Web RESTful pour débogage. Il doit uniquement être utilisé dans ce but ou en cas de préoccupation relative à la sécurité lorsque des informations concernant la plateforme BI sont dévoilées.	Non sélectionné
Nombre d'objets par défaut sur une page	Le nombre d'entrées qui seront répertoriées par page. Les développeurs peuvent remplacer ce paramètre par &pageSize=<m> dans le SDK des services Web RESTful.	50
Délai d'expiration du jeton de session de l'entreprise (minutes)	Le délai d'expiration de validité d'un jeton de connexion. Un fois ce délai passé, un nouveau jeton de connexion doit être généré.	60

Propriété	Description	Valeur par défaut
Taille du groupe de sessions	Cela représente le nombre de sessions en mémoire cache qui doivent être stockées à un moment donné et qui sont utilisées pour améliorer la performance du serveur. Le groupe de sessions place en mémoire cache les sessions du service Web RESTful afin qu'elles puissent être réutilisées lorsqu'un utilisateur envoie une autre requête qui utilise le même jeton de connexion dans l'en-tête HTTP de la requête.	1000
Délai d'expiration du groupe de sessions (minutes)	Le temps, en minutes, avant que les sessions en mémoire cache n'expirent.	2
Activer l'authentification HTTP élémentaire	Si ce paramètre n'est pas activé, les requêtes du service Web RESTful doivent utiliser un jeton de connexion. Lorsque ce paramètre est activé, les utilisateurs doit fournir leur nom et mot de passe la première fois qu'ils font une requête du service Web RESTful. Lorsqu'il est activé, le menu déroulant *Plan d'authentification par défaut pour HTTP élémentaire* s'affiche.	Non sélectionné
Plan d'authentification par défaut pour HTTP élémentaire	Lorsque la case *Activer l'authentification HTTP élémentaire* est cochée, il est possible de sélectionner un des quatre types d'authentification. Notez que les noms et mots de passe sont transmis en clair à moins d'utiliser les options HTTP. Les valeurs acceptées sont les suivantes : • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	Vide. Néanmoins, si *Activer l'authentification HTTP élémentaire* est sélectionné, définissez-la par défaut sur *secEnterprise*.

Services Web RESTful - propriétés de la configuration de Cross-Origin Resource Sharing

Propriété	Description	Valeur par défaut
Autoriser les origines	Ce paramètre permet aux utilisateurs qui disposent de navigateurs adaptés à CORS d'accéder aux pages avec scripts Java qui doivent accéder à plusieurs noms de domaine. Ajoutez chaque nom de domaine en les séparant par une virgule. Par exemple : http://origin1.server.com:8080, http://origin2.server.com:8080. Par défaut, les navigateurs sont autorisés à accéder à tous les domaines (*).	(*) un astérisque
Âge maximum (minutes)	Correspond au temps maximum durant lequel les navigateurs peuvent cacher les requêtes HTTP.	1440

Service Web RESTful - propriétés de la configuration de l'authentification sécurisée

Propriété	Description	Valeur par défaut
Méthode d'extraction	Il s'agit d'un menu qui définit la méthode de requête qui doit être utilisée pour extraire les jetons de connexion à l'authentification sécurisée lors de l'utilisation de l'API du service Web RESTful `/logon/trusted`. • *HTTP_HEADER* est utilisé pour les requêtes GET avec l'en-tête de requête accept=application/xml (ou application/json). • *QUERY_STRING* est utilisé pour ajouter un nom de connexion à la fin d'une requête URL à l'aide de l'API du service Web RESTful, par exemple /logon/trusted/?user=johndoe. • *COOKIE* est utilisé lorsque le nom de connexion est extrait d'un cookie d'un navigateur Web. Le domaine, le nom, la valeur et le chemin doivent être stockés dans le cookie.	**HTTP_HEADER**
Paramètre du nom d'utilisateur	Il s'agit de l'étiquette utilisée pour identifier l'utilisateur sécurisé pour extraire un jeton de connexion.	**X-SAP-TRUSTED-USER**

Propriétés du service d'applications Web BOE

Type de propriété	Description	Valeur par défaut
Type d'authentification	Type d'authentification utilisé pour authentifier les utilisateurs se connectant à la zone de lancement BI. Les valeurs acceptées sont les suivantes : • *AD Kerberos* • *AD Kerberos SSO* • *Enterprise* • *LDAP*	*Enterprise*
Domaine AD par défaut	Le domaine Active Directory par défaut est utilisé afin que les utilisateurs n'aient pas à fournir un domaine lors de la connexion. Par exemple, si le domaine par défaut est « mondomaine » et qu'un utilisateur se connecte avec le nom « utilisateur », l'autorité de connexion Active Directory essaie d'authentifier « utilisateur@mondomaine.com ».	Vierge
Nom principal de service	Un nom principal de service (SPN, Service Principal Name) permet aux clients d'identifier de manière unique une instance d'un service. Le service d'authentification Kerberos utilise un nom SPN pour authentifier un service.	Vierge
Fichier Keytab	Chemin d'accès complet au fichier keytab. Un fichier keytab permet de configurer le filtre Kerberos sans afficher le mot de passe du compte utilisateur sur le serveur d'applications Web.	Vierge

Propriétés de SDK Services Web et QaaWS

Propriété	Description	Valeur par défaut
Activer la connexion unique Kerberos Active Directory	Indique si la connexion unique Kerberos AD doit être activée pour SDK Services Web et QaaWS.	**FALSE**

Propriété	Description	Valeur par défaut
Domaine AD par défaut	Le domaine Active Directory par défaut est utilisé pour éviter aux utilisateurs d'avoir à spécifier un domaine lors de leur connexion.	Vierge
Nom principal de service	Un nom principal de service (SPN, Service Principal Name) permet aux clients d'identifier de manière unique une instance d'un service. Le service d'authentification Kerberos utilise un nom SPN pour authentifier un service.	Vierge
Fichier Keytab	Chemin d'accès complet au fichier keytab. Un fichier keytab permet de configurer le filtre Kerberos sans afficher le mot de passe du compte utilisateur sur le serveur d'applications Web.	Vierge

Propriétés de la configuration HTTP

Propriété	Description	Valeur par défaut
Lier à toutes les adresses IP	Indique s'il faut lier à toutes les interfaces réseau. Si votre serveur comporte plusieurs cartes d'interface réseau et si vous souhaitez le lier à une carte en particulier, désactivez cette case à cocher.	**TRUE**
Lier au nom d'hôte ou à l'adresse IP	Spécifie l'interface réseau (adresse IP ou nom d'hôte) sur laquelle est fourni le service HTTP. Pour pouvoir spécifier une valeur, la case à cocher *Lier à toutes les adresses IP* doit être désactivée.	`localhost`
Port HTTP	Port sur lequel est fourni le service HTTP.	6405 La plage des valeurs autorisées s'étend de 1 à 65535.
Taille maximale de l'en-tête HTTP	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Propriétés de configuration du port HTTP via proxy

Propriété	Description	Valeur par défaut
Activer HTTP via proxy	Indique si le connecteur HTTP via proxy doit être activé sur le serveur WACS. Cette option est habituellement cochée sur les déploiements utilisant un proxy inverse.	**FALSE**
Lier à toutes les adresses IP	Indique si le port HTTP via proxy doit être lié à toutes les interfaces réseau.	**TRUE**
Lier au nom d'hôte ou à l'adresse IP	Spécifie l'interface réseau (adresse IP ou nom d'hôte) sur laquelle est fourni le service HTTP via proxy. Pour pouvoir spécifier une valeur, la case à cocher *Lier à toutes les adresses IP* doit être désactivée.	`localhost`
Port HTTP	Port sur lequel est fourni le service HTTP d'un déploiement avec proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTP via proxy* doit être activée.	6406 La plage des valeurs autorisées s'étend de 1 à 65535.
Nom d'hôte du proxy	Adresses IPv4 et IPv6, nom d'hôte ou nom de domaine complet du serveur proxy. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTP via proxy* doit être activée.	Vierge

Propriété	Description	Valeur par défaut
Port du proxy	Port du serveur proxy ou du serveur proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTP via proxy* doit être activée.	0 La plage des valeurs autorisées s'étend de 1 à 65535.
Taille maximale de l'en-tête HTTP	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Propriétés de configuration HTTPS

Propriété	Description	Valeur par défaut
Activer HTTPS	Indique si la communication HTTPS/SSL doit être activée.	**FALSE**
Lier au nom d'hôte ou à l'adresse IP	Spécifie l'interface réseau (adresse IP ou nom d'hôte) sur laquelle est fourni le service HTTPS. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	`localhost`
Port HTTPS	Port sur lequel est fourni le service HTTPS. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	443 La plage des valeurs autorisées s'étend de 1 à 65535.
Nom d'hôte du proxy	Adresses IPv4 et IPv6, nom d'hôte ou nom de domaine complet du serveur proxy. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	Vierge
Port du proxy	Port du serveur proxy ou du serveur proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	0 La plage des valeurs autorisées s'étend de 1 à 65535.
Protocole	Protocole de cryptage à utiliser. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	TLS Les valeurs autorisées sont TLS ou SSL.
Type de stockage de certificats	Type du fichier contenant vos certificats et clés privées. Il s'agit le plus souvent de *PCKS12*. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	PKCS12 Les valeurs autorisées sont PKCS12 ou JKS.
Emplacement du fichier de stockage des certificats	Chemin d'accès complet au fichier de stockage des certificats. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	Vierge
Mot de passe d'accès aux clés privées	Les fichiers de stockage des certificats PKCS12 et les fichiers de stockage des clés JKS contiennent des clés privées protégées par mot de passe afin d'empêcher tout accès non autorisé ou acte de malveillance. Saisissez le mot de passe utilisé lors de la création du fichier de stockage des certificats, afin que les serveurs WACS puissent accéder aux clés privées à partir du fichier de stockage des certificats. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	Vierge

Propriété	Description	Valeur par défaut
Alias du certificat	Alias du certificat dans le fichier de stockage des certificats. Si cet alias n'est pas spécifié et si un fichier de stockage de certificats contenant plusieurs certificats est utilisé, le premier certificat de la liste est utilisé. La plupart du temps, vous n'avez pas besoin d'indiquer une valeur. Pour pouvoir spécifier une valeur, la case à cocher *Activer HTTPS* doit être activée.	Vierge
Activer l'authentification du client	Si l'authentification du client est activée, seuls les clients disposant de clés dans le fichier de la liste de certificats de confiance peuvent bénéficier des services de serveur WACS. Les autres clients sont rejetés. Pour pouvoir activer l'authentification du client, vous devez activer la case à cocher *Activer HTTPS*.	**FALSE**
Emplacement du fichier de la liste de certificats de confiance	Chemin d'accès complet au fichier de la liste de certificats de confiance. Pour pouvoir spécifier une valeur, les cases à cocher *Activer HTTPS* et *Activer l'authentification du client* doivent être activées.	Vierge
Mot de passe d'accès aux clés privées de la liste de certificats de confiance	Mot de passe qui protège l'accès aux clés privées figurant dans la liste de certificats de confiance. Pour pouvoir spécifier une valeur, les cases à cocher *Activer HTTPS* et *Activer l'authentification du client* doivent être activées.	Vierge
Taille maximale de l'en-tête HTTP	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Propriétés d'exécution simultanée (par connecteur)

Propriété	Description	Valeur par défaut
Nombre maximal de requêtes simultanées	Le nombre de requêtes HTTP ou HTTPS simultanées que chaque connecteur (HTTP, HTTP via proxy, ou HTTPS) peut traiter simultanément.	**150** La plage des valeurs autorisées s'étend de 1 à 1000.

Propriétés de configuration d'Active Directory

Propriété	Description	Valeur par défaut
Emplacement du fichier Krb5.ini	Chemin d'accès complet au fichier `krb5.ini` qui stocke les propriétés de configuration Kerberos.	Vierge
Emplacement du fichier bscLogin.conf	Chemin d'accès complet au fichier `bscLogin.conf`.	Vierge

35.1.3 Propriétés des services de connectivité

La catégorie de service Connectivité comprend les services suivants :

- Service de connectivité natif (hébergé sur un serveur autonome)
- Service de connectivité natif (32 bits hébergé sur un serveur autonome)
- Adaptive Connectivity Service (hébergé sur l'APS)

Tous les services partagent les mêmes paramètres de configuration.

Données Excel, propriétés des service d'accès

Propriété	Description	Valeur par défaut
Intervalle (en secondes) entre chaque nettoyage d'accès aux données Excel	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	La valeur par défaut est 1 200 secondes.
Intervalle (en secondes) entre chaque permutation d'accès aux données Excel	Temps d'attente, en secondes, avant que le service obtienne un client inactif et permute sa session sur le disque dur. Il est recommandé d'indiquer une valeur inférieure à celle de la propriété *Intervalle (en secondes) entre chaque nettoyage d'accès aux données Excel*.	La valeur par défaut est 600 secondes.

Propriétés de l'opération de service

Propriété	Description	Valeur par défaut
→ N'oubliez pas Il n'est pas nécessaire de redémarrer le serveur après avoir modifié les propriétés d'opération de service suivantes.		
Pool de connexion	Active ou désactive le pool de connexion. Les valeurs possibles sont : • Activé - Avec délai d'expiration • Activé - Sans délai d'expiration • Désactivé ⓘ Remarque Le pool de connexions est une fonctionnalité de mise en cache qui veille à ce que les connexions restent réutilisables pour de meilleures performances du serveur.	Activé - Avec délai d'expiration
Délai d'expiration du pool de connexion	Spécifie la durée d'inactivité maximale pour les connexions dans le pool (en minutes). ⓘ Remarque Cette propriété est l'équivalente du paramètre `Max Pool Time` du fichier `cs.cfg`. La désactivation du pool revient à définir la `Durée maximale du pool` sur `0`. L'activation du pool sans délai d'expiration revient à définir la `Durée maximale du pool` sur `-1`. Pour en savoir plus, reportez-vous au *Guide d'accès aux données*.	**60**
Délai d'inactivité des objets provisoires	Spécifie la durée en minutes pendant laquelle un objet temporaire peut être conservé dans le serveur. Après ce délai, l'objet est supprimé et ses ressources sont restaurées.	**60**
Intervalle de l'horloge des objets provisoires	Spécifie l'intervalle entre les contrôles d'activité (en minutes). A intervalles réguliers, le serveur recherche des objets susceptibles d'être supprimés.	**5**

Propriété	Description	Valeur par défaut
Activer le bloc HTTP	Active ou désactive le bloc HTTP. **ⓘ Remarque** Le bloc HTTP est pertinent uniquement pour le déploiement 3-Tier. Il affecte la performance d'ouverture/actualisation des documents car des réponses plus importantes signifient moins d'allers-retours lors de l'extraction de documents volumineux. La désactivation du bloc HTTP équivaut à la *taille du bloc HTTP* définie sur **0**.	Activé
Taille du bloc HTTP	Spécifie la taille des réponses HTTP émises par le serveur (en kilo-octets).	**64**

Propriétés de suivi de bas niveau

Propriété	Description	Valeur par défaut
→ N'oubliez pas Il n'est pas nécessaire de redémarrer le serveur après avoir modifié les propriétés de suivi de bas niveau suivantes.		
Activer le suivi du travail	Active le suivi des travaux du serveur de connexion. **ⓘ Remarque** La propriété *Niveau de journalisation* doit être définie sur *Haut*.	Désactivé
Activer le suivi du middleware	Active le suivi de tout le middleware. Pour suivre un middleware spécifique, vous devez configurer le fichier `cs.cfg` et redémarrer le serveur. **ⓘ Remarque** La propriété *Niveau de journalisation* doit être définie sur *Elevé*.	Désactivé

Propriétés de sources de données actives

Propriété	Description	Valeur par défaut
⚠ Attention Vous devez redémarrer le serveur après avoir modifié les propriétés de sources de données actives suivantes.		

Propriété	Description	Valeur par défaut
Activer la source de données	Vous permet de sélectionner les sources de données pour lesquelles vous souhaitez des connexions. Cette propriété fonctionne comme un filtre pour les pilotes. Vous spécifiez les sources de données actives afin de charger les pilotes que vous souhaitez utiliser. **⚠ Attention** Par défaut, le serveur charge tous les pilotes disponibles. Utilisez ce paramètre pour spécialiser les serveurs. Il vous sera particulièrement utile lorsque vous déploierez plusieurs serveurs CORBA sur votre réseau. **→ N'oubliez pas** Seuls les pilotes pour les sources de données sélectionnées sont chargés. Tous les autres sont ignorés. Si vous ne sélectionnez aucune source de données, le serveur charge tous les pilotes disponibles. **ⓘ Remarque** Dans la métrique de serveur, vérifiez que les sources de données sélectionnées ont été activées. Les couches et les bases de données réseau sont affichées sous *Métrique de service de connexion*.	Non coché
Couche réseau	Spécifie la couche réseau utilisée par la connexion. **ⓘ Remarque** Seul le nom non localisé est considéré. Vous trouverez la liste des couches réseau disponibles dans le fichier `driver.cfg`, situé dans le répertoire `<connectionserver-install-dir>\connectionServer\`.	• `ODBC` pour les serveurs CORBA natifs • `JDBC` pour le serveur CORBA adaptatif
Base de données	Spécifie la base de données utilisée par la connexion. **ⓘ Remarque** Seul le nom non localisé est considéré. Les noms de bases de données peuvent être des expressions régulières à condition d'être des chaînes ASCII pures. Les formats utilisent la syntaxe GNU regexp. Utilisez le modèle `.*` pour remplacer un caractère quelconque. Par exemple, l'expression `MS SQL Server.*$` signifie que toutes les bases de données MS SQL Server sont utilisées. Pour en savoir plus sur les expressions régulières, consultez le site Web PERL à l'adresse http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions .	Le champ reste vide jusqu'à ce que vous y saisissiez un nom de base de données.

Propriétés du service personnalisé d'accès aux données

Propriété	Description	Valeur par défaut
Intervalle (en secondes) entre chaque nettoyage d'accès aux données personnalisées	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	La valeur par défaut est 1 200 secondes.
Intervalle (en secondes) entre chaque permutation d'accès aux données personnalisées	Temps d'attente, en secondes, avant que le service obtienne un client inactif et permute sa session sur le disque dur. Il est recommandé d'indiquer une valeur inférieure à celle de la propriété *Intervalle (en secondes) entre chaque nettoyage d'accès aux données personnalisées*.	La valeur par défaut est 600 secondes.

Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

Propriétés du service de gestion des promotions

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service ClearCase de la gestion des promotions

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de différence visuelle

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Informations associées

Propriétés courantes du serveur [page 1176]

35.1.4 Propriétés des services Crystal Reports

La catégorie de service Crystal Reports comprend les serveurs suivants :

- Serveur de mise en cache Crystal Reports
- Serveur de traitement Crystal Reports
- Propriétés du Report Application Server Crystal Reports 2020
- Serveur de traitement Crystal Reports 2020

Propriétés du serveur de mise en cache Crystal Reports

Toutes les propriétés qui s'appliquent à la fois aux serveurs de mise en cache Crystal Reports et aux serveurs de traitement Crystal Reports doivent être définies sur la même valeur. Par exemple, si vous attribuez au paramètre *Toujours actualiser le visualiseur par rapport aux données actuelles* la valeur **TRUE** sur le serveur de mise en cache, vous devez également attribuer la valeur **TRUE** à ce même paramètre sur le Processing Server.

> **Remarque**
>
> Lorsque vous modifiez l'une de ces propriétés de serveur, redémarrez le serveur pour valider les modifications.

Propriétés du service de mémoire cache Crystal Reports

Propriété	Description	Valeur par défaut
Toujours actualiser le visualiseur par rapport aux données actuelles	Indique si toutes les pages mises en cache sont ignorées et si les données sont extraites directement de la base de données lorsque les utilisateurs actualisent explicitement un rapport. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur. Pour spécifier une valeur sur l'objet rapport, sélectionnez le rapport dans la CMC, puis cliquez sur *Paramètres par défaut* > *Groupe de serveurs de visualisation*.	La valeur par défaut est **FALSE**.
Partager les données des rapports entre les clients	Indique si les données des rapports sont partagées entre différents clients. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est **TRUE**.
Délai d'expiration de la connexion inactive (minutes)	Délai, en minutes, accordé par le serveur de mise en cache Crystal Reports pour qu'une requête émane d'une connexion inactive. Il n'est généralement pas nécessaire de modifier la valeur par défaut.	La valeur par défaut est 20 minutes.
Délai d'expiration du cache de sécurité (minutes)	Durée, en minutes, pendant laquelle le serveur utilise des références de connexion, des paramètres de rapport et des informations de connexion à la base de données mis en cache pour servir des requêtes avant d'interroger le CMS.	La valeur par défaut est 20 minutes.

Propriété	Description	Valeur par défaut
Ancienneté maximale des données à la demande envoyées aux clients (secondes)	Durée, en secondes, pendant laquelle le serveur utilise les données mises en cache pour répondre aux requêtes émanant de rapports à la demande. Si le serveur reçoit une nouvelle requête à laquelle il peut répondre avec des données générées pour une requête antérieure et si le délai écoulé depuis que ces données ont été générées est inférieur à la valeur définie pour ce paramètre, le serveur réutilise ces données pour répondre à la nouvelle requête. Réutiliser ainsi des données permet d'améliorer les performances du système de manière sensible lorsque plusieurs utilisateurs ont besoin des mêmes informations. Lorsque vous définissez cette valeur, évaluez dans quelle mesure il est important que les utilisateurs reçoivent des données à jour. S'il est capital que tous les utilisateurs reçoivent des données à jour (car des modifications importantes sont souvent apportées aux données par exemple), il peut être judicieux de désactiver la réutilisation des données en attribuant à ce paramètre la valeur 0 (zéro). **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est 0 seconde.
Taille maximale de la mémoire cache (Ko)	Espace disque (en kilo-octets) consacré à la mise en mémoire cache des rapports. Une taille importante peut être nécessaire si le serveur a besoin de gérer un grand nombre de rapports, ou des rapports particulièrement complexes.	La valeur par défaut est 256 000 Kilo-octets.
Répertoire de fichiers cache	Emplacement du répertoire de mémoire cache.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Arguments de la machine virtuelle Java	Indique les arguments de ligne de commande pouvant être fournis à la JVM.	La valeur par défaut est vide.
Nom de la DLL	Spécifie le nom du plug-in de type de document en cours de chargement. Cette propriété est en lecture seule.	rasprocReport

Propriétés du serveur de traitement Crystal Reports

Toutes les propriétés qui s'appliquent à la fois aux serveurs de mise en cache Crystal Reports et aux serveurs de traitement Crystal Reports doivent être définies sur la même valeur. Par exemple, si vous attribuez au paramètre *Toujours actualiser le visualiseur par rapport aux données actuelles* la valeur **TRUE** sur le serveur de mise en cache, vous devez également attribuer la valeur **TRUE** à ce même paramètre sur le Processing Server.

> **Remarque**
>
> Lorsque vous modifiez l'une de ces propriétés de serveur, redémarrez le serveur pour valider les modifications.

Propriétés du service de traitement Crystal Reports

Propriété	Description	Valeur par défaut
Délai d'expiration d'un travail inactif (minutes)	Indique, en minutes, la durée d'attente du serveur de traitement Crystal Reports entre les requêtes pour un travail donné.	La valeur par défaut est 20 minutes.
Nombre maximal de travaux à durée de vie par enfant	Nombre maximal de travaux que chaque processus enfant peut gérer par cycle de vie.	La valeur par défaut est de 1 000.
Toujours actualiser le visualiseur par rapport aux données actuelles	Indique si toutes les pages mises en cache sont ignorées et si les données sont extraites directement de la base de données lorsque les utilisateurs actualisent explicitement un rapport. Indique si les données des rapports sont partagées entre différents clients. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur. Pour spécifier une valeur sur l'objet rapport, sélectionnez le rapport dans la CMC, puis cliquez sur *Paramètres par défaut* > *Groupe de serveurs de visualisation*.	La valeur par défaut est **FALSE**.
Partager les données des rapports entre les clients	Indique si les données des rapports sont partagées entre différents clients. Indique si les données des rapports sont partagées entre différents clients. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est **TRUE**.
Délai d'expiration de la connexion inactive (minutes)	Durée en minutes de l'attente du serveur de traitement Crystal Reports pour une requête issue d'une connexion inactive. Il n'est généralement pas nécessaire de modifier la valeur par défaut.	La valeur par défaut est 20 minutes.
Nombre maximal de travaux simultanés (0 pour automatique)	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le serveur de traitement Crystal Reports. Si cette propriété a pour valeur « 0 », le serveur applique une valeur adaptée, en fonction de l'unité centrale et de la mémoire de l'ordinateur sur lequel le serveur s'exécute.	La valeur par défaut est de 0.

Propriété	Description	Valeur par défaut
Ancienneté maximale des données à la demande envoyées aux clients (secondes)	Durée, en secondes, pendant laquelle le serveur utilise les données mises en cache pour répondre aux requêtes émanant de rapports à la demande. Si le serveur reçoit une nouvelle requête à laquelle il peut répondre avec des données générées pour une requête antérieure et si le délai écoulé depuis que ces données ont été générées est inférieur à la valeur définie pour ce paramètre, le serveur réutilise ces données pour répondre à la nouvelle requête. Réutiliser ainsi des données permet d'améliorer les performances du système de manière sensible lorsque plusieurs utilisateurs ont besoin des mêmes informations. Lorsque vous définissez cette valeur, évaluez dans quelle mesure il est important que les utilisateurs reçoivent des données à jour. S'il est capital que tous les utilisateurs reçoivent des données à jour (car des modifications importantes sont souvent apportées aux données par exemple), il peut être judicieux de désactiver la réutilisation des données en attribuant à ce paramètre la valeur 0 (zéro). **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est de 0.
Nombre maximal d'enfants prédémarrés	Nombre maximal de processus enfant prédémarrés autorisés par le serveur. Si cette valeur est trop basse, le serveur crée des processus enfant dès que les requêtes sont effectuées, ce qui peut générer un temps d'attente pour les utilisateurs. Si cette valeur est trop élevée, les ressources système peuvent être exploitées inutilement par les processus enfant inactifs.	La valeur par défaut est 1 enfant.
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Chemin de classe Java	Nom et chemin des classes Java requises par le serveur.	%CommonJavaLibDir%/procCR.jar
Arguments de la machine virtuelle Java enfant	Indique les arguments de ligne de commande fournis aux processus enfant créés par le serveur.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86400 secondes.

Propriétés du Report Application Server Crystal Reports 2020

> **Remarque**
>
> Si vous modifiez l'une de ces propriétés, vous devez redémarrer le serveur pour valider les modifications.

Propriétés du service de modification et de visualisation Crystal Reports 2020

Propriété	Description	Valeur par défaut
Autoriser les travaux du rapport à rester connectés à la base de données jusqu'à la fermeture du travail du rapport	Indique si le travail du rapport reste connecté à la base de données jusqu'à ce que le processus ait été exécuté.	La valeur par défaut est **FALSE**.
Taille des données à parcourir (enregistrements)	Nombre d'enregistrements distincts renvoyés de la base de données lors du parcours des valeurs d'un champ particulier. Les données sont d'abord extraites de la mémoire cache du client, si celle-ci est disponible, puis de la mémoire cache du serveur. Si les données ne sont dans aucune mémoire cache, elles sont extraites de la base de données.	La valeur par défaut est 100 enregistrements.
Délai d'expiration de la connexion inactive (minutes)	Délai, en minutes, accordé par le RAS (Report Application Server) pour que des requêtes émanent d'un client inactif avant de considérer que la connexion est arrivée à expiration. L'attribution d'une valeur trop faible peut entraîner la fermeture prématurée d'une requête utilisateur et l'attribution d'une valeur trop élevée peut affecter l'extensibilité du serveur (par exemple, si l'objet `ReportClientDocument` n'est pas fermé de manière explicite, le serveur attendra inutilement qu'un travail inactif se ferme).	La valeur par défaut est 30 minutes.
Taille du lot (enregistrements)	Nombre de lignes provenant de l'ensemble des résultats renvoyées par la base de données lors du transfert de chaque donnée. Par exemple, si le nombre d'enregistrements demandé est de 500 et si la propriété Taille du lot a pour valeur 100 enregistrements, les données seront renvoyées en 5 lots distincts de 100 lignes chacun. Pour améliorer les performances de votre RAS, il est indispensable que vous compreniez l'environnement réseau, la base de données et le type de requêtes utilisés afin de pouvoir définir la taille de lot appropriée.	La valeur par défaut est 100 enregistrements.

Propriété	Description	Valeur par défaut
Nombre d'enregistrements de la base de données devant être lus lors de la prévisualisation ou de l'actualisation d'un rapport (-1 pour une configuration illimitée)	Nombre d'enregistrements de base de données devant être lus lors de la visualisation ou de l'actualisation d'un rapport. Ce paramètre permet de limiter le nombre d'enregistrements que le serveur extrait de la base de données lorsqu'un utilisateur exécute une requête ou un rapport. Ce paramètre est utile si vous souhaitez empêcher les utilisateurs d'exécuter des rapports à la demande qui contiennent des requêtes renvoyant un nombre trop élevé d'enregistrements. Il est préférable de planifier ce type de rapports, non seulement pour qu'ils soient plus rapidement accessibles aux utilisateurs, mais également pour alléger la charge qui pèse sur la base de données lors de l'exécution de ces requêtes complexes.	La valeur par défaut est 20000 enregistrements.
Nombre maximal de travaux simultanés (0 pour une configuration illimitée)	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le RAS.	La valeur par défaut est 75 enregistrements.
Ancienneté maximale des données à la demande envoyées à un client (minutes)	Délai, en minutes, accordé à un rapport à la demande pour servir les données de rapport mises en cache.	La valeur par défaut est 20 minutes.
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86400 secondes.

Propriétés du serveur de traitement Crystal Reports 2020

Remarque

Si vous modifiez l'une de ces propriétés, vous devez redémarrer le serveur pour valider les modifications.

Propriétés du service de traitement Crystal Reports 2020

Propriété	Description	Valeur par défaut
Délai d'expiration d'un travail inactif (minutes)	Indique, en minutes, la durée d'attente du serveur de traitement Crystal Reports entre les requêtes pour un travail donné.	La valeur par défaut est 20 minutes.

Propriété	Description	Valeur par défaut
Nombre maximal de travaux à durée de vie par enfant	Nombre maximal de travaux que chaque processus enfant peut gérer par cycle de vie.	La valeur par défaut est de 1 000.
Toujours actualiser le visualiseur par rapport aux données actuelles	Indique si toutes les pages mises en cache sont ignorées et si les données sont extraites directement de la base de données lorsque les utilisateurs actualisent explicitement un rapport. Indique si les données des rapports sont partagées entre différents clients. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur. Pour spécifier une valeur sur l'objet rapport, sélectionnez le rapport dans la CMC, puis cliquez sur *Paramètres par défaut* > *Groupe de serveurs de visualisation* >.	La valeur par défaut est **FALSE**.
Partager les données des rapports entre les clients	Indique si les données des rapports sont partagées entre différents clients. Indique si les données des rapports sont partagées entre différents clients. **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est **TRUE**.
Délai d'expiration de la connexion inactive (minutes)	Durée en minutes de l'attente du serveur de traitement Crystal Reports pour une requête issue d'une connexion inactive. Il n'est généralement pas nécessaire de modifier la valeur par défaut.	La valeur par défaut est 20 minutes.
Nombre maximal de travaux simultanés (0 pour automatique)	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le serveur de traitement Crystal Reports. Si cette propriété a pour valeur « 0 », le serveur applique une valeur adaptée, en fonction de l'unité centrale et de la mémoire de l'ordinateur sur lequel le serveur s'exécute.	La valeur par défaut est de 0.

Propriété	Description	Valeur par défaut
Ancienneté maximale des données à la demande envoyées aux clients (secondes)	Durée, en secondes, pendant laquelle le serveur utilise les données mises en cache pour répondre aux requêtes émanant de rapports à la demande. Si le serveur reçoit une nouvelle requête à laquelle il peut répondre avec des données générées pour une requête antérieure et si le délai écoulé depuis que ces données ont été générées est inférieur à la valeur définie pour ce paramètre, le serveur réutilise ces données pour répondre à la nouvelle requête. Réutiliser ainsi des données permet d'améliorer les performances du système de manière sensible lorsque plusieurs utilisateurs ont besoin des mêmes informations. Lorsque vous définissez cette valeur, évaluez dans quelle mesure il est important que les utilisateurs reçoivent des données à jour. S'il est capital que tous les utilisateurs reçoivent des données à jour (car des modifications importantes sont souvent apportées aux données par exemple), il peut être judicieux de désactiver la réutilisation des données en attribuant à ce paramètre la valeur 0 (zéro). **Remarque** Cette propriété peut avoir pour valeur un objet rapport lui-même et peut varier d'un rapport à un autre ; les valeurs spécifiées dans l'objet rapport remplacent les paramètres du serveur.	La valeur par défaut est de 0.
Nombre maximal d'enfants prédémarrés	Nombre maximal de processus enfant prédémarrés autorisés par le serveur. Si cette valeur est trop basse, le serveur crée des processus enfant dès que les requêtes sont effectuées, ce qui peut générer un temps d'attente pour les utilisateurs. Si cette valeur est trop élevée, les ressources système peuvent être exploitées inutilement par les processus enfant inactifs.	La valeur par défaut est 1 enfant.
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. **Remarque** Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultDataDir%/CrystalReports2020ProcessingServer/temp
Autoriser les travaux du rapport à rester connectés à la base de données jusqu'à la fermeture du travail du rapport	Indique si le travail du rapport reste connecté à la base de données jusqu'à sa fermeture.	La valeur par défaut est FALSE.

Propriété	Description	Valeur par défaut
Enregistrements de base de données lus lors de la prévisualisation ou de l'actualisation (0 pour une configuration illimitée)	Nombre d'enregistrements de base de données devant être lus lors de la visualisation ou de l'actualisation d'un rapport. Ce paramètre permet de limiter le nombre d'enregistrements que le serveur extrait de la base de données lorsqu'un utilisateur exécute une requête ou un rapport. Ce paramètre est utile si vous souhaitez empêcher les utilisateurs d'exécuter des rapports à la demande qui contiennent des requêtes renvoyant un nombre trop élevé d'enregistrements. Il est préférable de planifier ce type de rapports, non seulement pour qu'ils soient plus rapidement accessibles aux utilisateurs, mais également pour alléger la charge qui pèse sur la base de données lors de l'exécution de ces requêtes complexes.	La valeur par défaut est de 20000.

Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86400 secondes.

35.1.5 Propriétés d'Analysis Services

La catégorie des services d'Analysis comprend le serveur de traitement adaptatif :

Propriétés du service MDAS (Multi-Dimensional Analysis Service)

Propriété	Description	Valeur par défaut
Nombre maximal de sessions client	Spécifie le nombre maximal de sessions MDAS pouvant être ouvertes simultanément sur le serveur. Lorsque le nombre de sessions ouvertes atteint cette limite, toute nouvelle tentative d'ouverture de session MDAS se traduit par le message d'erreur « serveur indisponible ». En fonction de vos besoins et du matériel nécessaire, vous pouvez modifier cette valeur pour optimiser les performances du serveur MDAS. Cependant, plus la valeur est élevée, plus vous risquez de rencontrer des problèmes de performance au niveau du serveur MDAS et du serveur de base de données. La valeur par défaut de 15 sessions est une estimation moyenne. Pour les installations dans lesquelles les requêtes utilisateur sont peu volumineuses, vous pouvez augmenter cette valeur de façon significative ; en revanche, les installations dans lesquelles les requêtes utilisateur sont volumineuses requièrent une valeur plus faible.	La valeur par défaut est 15. La plage valide est comprise entre 1 et 100.

Propriété	Description	Valeur par défaut
Nombre maximal de cellules renvoyées par une requête	Spécifie le nombre de cellules renvoyées à l'utilisateur dans une requête unique. L'utilisateur ne peut pas exécuter de requête qui renvoie un très grand nombre de cellules consommant beaucoup de mémoire. Si la requête dépasse cette limite de cellules, l'utilisateur reçoit un message d'erreur.	La valeur par défaut est de 100 000 cellules.
Nombre maximal de membres renvoyés lors du filtrage	Spécifie le nombre de membres extraits lors du filtrage par membre. Un nombre important de membres extraits peut consommer beaucoup de mémoire.	La valeur par défaut est de 100 000 membres.

Propriétés de service des applications Web BEx

Propriété	Description	Valeur par défaut
Nombre maximal de sessions client	Nombre maximal de sessions client autorisées sur le service.	La valeur par défaut est 15 sessions.
Système maître SAP BW	Nom de la connexion OLAP au système BW que vous avez créée dans la plateforme de BI.	La valeur par défaut est SAP_BW.
Destination RFC du serveur JCo	Nom de destination RFC du serveur JCo que vous avez saisi dans le système BW.	Par défaut, cette valeur est vide.
Hôte passerelle du serveur JCo	Nom de l'hôte passerelle du serveur JCo que vous avez défini dans le système BW.	Par défaut, cette valeur est vide.
Service de passerelle du serveur JCo	Nom du service de passerelle du serveur JCo que vous avez défini dans le système BW.	Par défaut, cette valeur est vide.
Nombre de connexions du serveur JCo	Spécifie le nombre de programmes créés automatiquement pouvant être utilisés pour traiter les appels d'ABAP à Java concernant le service.	La valeur par défaut est 3 connexions.

35.1.6 Propriétés des services de fédération de données

La catégorie de service Data Federation inclut le serveur de traitement adaptatif :

Propriétés des services de fédération de données

Propriété	Description	Valeur par défaut
Nombre maximal de connexions	Nombre maximal de connexions autorisées sur le serveur.	La valeur par défaut est 32 767.
Taille du pool de threads d'exécution	Nombre maximal de requêtes pouvant être exécutées en parallèle à un moment donné.	La valeur par défaut est 10.
Délai d'inactivité de la connexion	Durée, en secondes, après laquelle une connexion inactive est fermée.	La valeur par défaut est de 10 800 secondes.
Délai d'inactivité de l'instruction	Durée, en secondes, après laquelle une instruction de requête est fermée.	La valeur par défaut est de 600 secondes.

35.1.7 Propriétés des services Web Intelligence

La catégorie de services Web Intelligence comprend les serveurs suivants :

- Adaptive Processing Server
- Web Intelligence Processing Server

Paramètres de l'Adaptive Processing Server

Paramètres de ligne de commande

Propriété	Description	Valeur par défaut
Développer jusqu'au niveau	Spécifie le niveau auquel les données sont récupérées à partir des requête BEx. Par défaut, les hiérarchies ne sont pas développées jusqu'à un niveau donné. Niveau100 est toujours le niveau par défaut. Vous pouvez modifier ce comportement en ajoutant ce paramètre à la ligne de commande, mais si la définition de cette valeur est trop élevée, Web Intelligence extrait toute les données de la hiérarchie, ce qui peut avoir une incidence sur les performances et la stabilité du système.	`-Dsap.sl.bics.expandToLevel=n` n peut être tout entier entre 0 et 99. Si n=0, ou si ce paramètre n'est pas spécifié, les hiérarchies n'utiliseront pas le paramètre Développer jusqu'au niveau.
Sélection de variables Option de sélection	Spécifie l'option de sélection pour la sélection de variables. Si cette propriété est définie sur un intervalle, la zone de texte n'est pas accessible et les utilisateurs ne peuvent saisir que des valeurs de début et de fin dans la boîte de dialogue Invites. Si cette propriété est définie sur valeurs multiples, la zone de texte "Saisissez une valeur" est disponible et les utilisateurs peuvent saisir des valeurs pour les variables Option de sélection BW. **Remarque** Cette propriété ne met pas à jour les installations locales de Web Intelligence Rich Client. Pour en savoir plus sur la mise à jour du registre local pour de telles installations, voir le "Guide d'installation de Web Intelligence Rich Client".	`-Dsap.sl.bics.variableComplexSelectionMapping=n` où n peut être intervalle ou valeurs multiples. **Remarque** Avant BI 4.1 SP05, la valeur par défaut pour cette option était intervalle. Si vous ajoutez cette propriété aux paramètres d'Adaptive Processing Server et la définissez sur valeurs multiples, procédez comme suit avec les documents existants : • Un document doit être purgé. • Les valeurs par défaut pour les invites de requête doivent être modifiées afin d'être compatibles avec la sélection de valeurs multiples.

Propriétés du service de surveillance de Web Intelligence

Propriété	Description	Valeur par défaut
Activer la surveillance	Spécifie si la surveillance est activée pour le service.	**TRUE**
Délai de boucle de thread de surveillance (en secondes)	Spécifie la durée en secondes entre les tentatives d'un service pour effectuer un test ping sur les clients.	300
Intervalle (en secondes) entre chaque nettoyage de ressource surveillée par défaut	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	1200
Intervalle (en secondes) entre chaque permutation de ressource surveillée par défaut	Temps d'attente, en secondes, avant que le service obtienne un client inactif et permute sa session sur le disque dur. Il est recommandé d'indiquer une valeur inférieure à celle de la propriété Intervalle (en secondes) entre chaque nettoyage de ressource surveillée par défaut.	600
Activer le profilage de service		**TRUE**
Activer la surveillance d'activité de service		**TRUE**

Propriétés du service de visualisation

Propriété	Description	Valeur par défaut
Délai d'expiration avant nettoyage du moteur de visualisation (en secondes)	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	1200
Délai d'expiration avant permutation du moteur de visualisation (en secondes)	Temps d'attente, en secondes, avant que le service obtienne un client inactif et permute sa session sur le disque dur. Il est recommandé d'indiquer une valeur inférieure à celle de la propriété *Délai d'expiration avant nettoyage du moteur de visualisation (en secondes)*.	600

Propriétés du service Rebean

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de récupération de documents

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Propriétés du service de pont DSL

Propriété	Description	Valeur par défaut
Intervalle (en secondes) entre chaque nettoyage du moteur du pont DSL	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	1200

Propriétés du Web Intelligence Processing Server

Les propriétés du Web Intelligence Processing Server sont regroupées selon les services suivants :

- Moteur d'informations
- Services principaux Web Intelligence
- Traitement Web Intelligence
- Services communs Web Intelligence

Les paramètres des seuils sont décrits dans un tableau distinct.

Propriétés du service du moteur d'informations

Propriété	Description	Valeur par défaut
Activer la mémoire cache des listes de valeurs	Indique si la mise en cache des listes de valeurs est activée sur le Web Intelligence Processing Server.	**TRUE**
Taille de lot de la liste des valeurs (entrées)	Nombre maximal d'entrées (ou de valeurs) pour chaque lot de listes de valeurs.	1000
Taille maximale du tri personnalisé (entrées)	Nombre maximal d'entrées du tri personnalisé.	100
Taille maximale du cache d'univers (univers)	Nombre d'univers à mettre en cache sur le Web Intelligence Processing Server.	20
Taille maximales de la liste de valeurs (entrées)	Nombre maximal d'entrées (ou de valeurs) pour chaque liste de valeurs.	50000

Propriétés des services principaux Web Intelligence

Propriété	Description	Valeur par défaut
Délai d'expiration avant recyclage (secondes)	Durée, en secondes, d'inactivité du serveur avant que le SIA ne l'arrête et ne le redémarre lorsque le nombre total de documents traités dépasse la valeur spécifiée par la propriété *Nombre maximal de documents avant recyclage*.	1200
Délai d'expiration pour inactivité de document (secondes)	Délai accordé avant que la session Web Intelligence Processing Server ne soit permutée (en secondes). Si le client ne génère pas de requêtes durant cette période, la session est permutée sur le disque dur, libérant ainsi des ressources pour une session active.	300 La plage valide est comprise entre 100 et 10 000 secondes.
Intervalle d'interrogation du serveur (secondes)	Intervalle, en secondes, attendu par le serveur avant d'interroger de nouvelles requêtes de thread. Si le serveur est en phase d'interrogation, il effectue des actions de nettoyage, par exemple la permutation des documents inutilisés, afin que la mémoire reste en dessous du seuil maximal.	120
Nombre maximal de documents par utilisateur	Nombre maximal de sessions actives (documents Web Intelligence) pouvant être associées à un utilisateur à un moment donné. Si la valeur est 5, l'utilisateur peut utiliser jusqu'à 5 sessions actives à la fois.	5 La plage valide est comprise entre 1 et 20.

Propriété	Description	Valeur par défaut
Nombre maximal de documents avant recyclage	Nombre de documents Web Intelligence pouvant être traités avant que le serveur ne soit recyclé. Si le nombre de documents traités est atteint et le serveur inactif, ce dernier est fermé et le SIA (Server Intelligence Agent) démarre une nouvelle instance du serveur. La nouvelle instance du serveur ne démarre toutefois pas immédiatement. Le délai est défini par la propriété *Délai d'expiration avant recyclage (secondes)*.	50
Activer les messages d'erreur en cas de taille maximale de carte de document	Indique si le `<Nombre maximal de connexions>` est restreint. Si cette propriété est activée, la valeur définie pour la propriété `<Nombre maximal de connexions>` est reconnue par le serveur, sinon elle est ignorée.	**TRUE**
Délai d'expiration de la connexion inactive (minutes)	Délai, en minutes, accordé par le serveur pour qu'une requête émane d'une connexion inactive. L'attribution d'une valeur trop faible peut entraîner la clôture prématurée d'une requête. L'attribution d'une valeur trop élevée peut entraîner la mise en file d'attente des requêtes pendant que le serveur attend la clôture des requêtes inactives.	20
Nombre maximal de connexions	Nombre maximal de connexions pouvant être ouvertes simultanément. Ce nombre est approximatif. Le paramètre ne prend pas en compte pas les sessions inactives qui sont permutées ou la session créée pour analyser le nombre de sessions. Si cette limite est atteinte et si aucun autre serveur n'est disponible pour gérer la requête, l'utilisateur reçoit un message d'erreur. **Remarque** Pour que cette propriété soit reconnue par le serveur, la propriété `<Activer les messages d'erreur en cas de taille maximale de carte de document>` doit être activée.	200 La plage valide est comprise entre 5 et 65 535.
Activer l'analyse de mémoire	Indique si l'analyse de mémoire est activée. Si tel est le cas, les propriétés suivantes sont également activées et reconnues par le serveur. • `<Seuil maximal de la mémoire (Mo)>` • `<Seuil supérieur de la mémoire (Mo)>` • `<Seuil inférieur de la mémoire (Mo)>` Lorsque la mémoire de traitement du serveur dépasse le `<Seuil supérieur de la mémoire>`, seul l'enregistrement de document est autorisé. Lorsque la mémoire de traitement dépasse le `<Seuil maximal de la mémoire>`, toutes les opérations s'arrêtent et échouent.	**TRUE**
Seuil inférieur de la mémoire (Mo)	Seuil inférieur de consommation de mémoire.	**3500**
Seuil supérieur de la mémoire (Mo)	Seuil supérieur de consommation de mémoire.	**4500**

Propriété	Description	Valeur par défaut
Seuil maximal de la mémoire (Mo)	Seuil maximal de consommation de mémoire.	**6000**
Activer la surveillance de service APS	Active la surveillance du serveur par le service APS hébergé sur le serveur de traitement adaptatif.	**TRUE**
Nombre de nouvelles tentatives sur échec du test Ping du service APS	Indique le nombre de fois où le serveur tente d'atteindre le service APS avant de décider que c'est impossible.	3
Période de thread de la surveillance de service APS	Spécifie le temps d'attente entre les tentatives pour joindre le service APS.	300
Activer les journaux d'activité actuels	Indique si des traces complètes sont générées dans les fichiers journaux du serveur. **Remarque** Cette propriété doit être activée uniquement à des fins de débogage lors du dépannage des problèmes. Défini sur **FALSE** pendant le fonctionnement normal.	**FALSE**

Propriétés du service de traitement Web Intelligence

Propriété	Description	Valeur par défaut
Activer l'utilisation de l'URL HTTP	Spécifie si le serveur peut accéder à des fichiers stockés à distance.	**TRUE**
Valeur proxy	Indique l'adresse du serveur proxy de votre réseau. Spécifiez une valeur uniquement si votre réseau contient un serveur proxy et que vous tentez d'accéder à des fichiers stockés à distance.	Vierge

Propriétés des service communs Web Intelligence

Propriété	Description	Valeur par défaut
Délai d'expiration de la mémoire cache (minutes)	Délai, en minutes, avant que le contenu de la mémoire cache de document ne soit effacé. Ce délai dépend de la date d'accès la plus récente de chaque document.	4370
Intervalle de nettoyage de la mémoire cache de document (minutes)	Intervalle, en minutes, entre chaque analyse et vérification de la mémoire cache de document par rapport aux paramètres `<Taille maximale de la mémoire cache du document>`, `<Espace maximum de réduction du cache du document>` et `<Nombre maximal de documents dans la mémoire cache>`.	120
Désactiver le partage de la mémoire cache	Indique si le partage de la mémoire cache est désactivé. Par défaut, ce partage est activé. Toutes les instances du Web Intelligence Processing Server partagent donc la même mémoire cache. Toutefois, si vous préférez avoir une mémoire cache par instance de Web Intelligence Processing Server, activez cette propriété.	**FALSE**
Activer la mémoire cache de document	Indique si la mémoire cache de document est activée. Si cette propriété est activée, la mémoire cache peut être préchargée avec des documents Web Intelligence planifiés.	**TRUE**

Propriété	Description	Valeur par défaut
Activer la mémoire cache en temps réel	Indique si la mémoire cache en temps réel est activée. Si cette propriété est activée, la mémoire cache peut être chargée dynamiquement. Le Web Intelligence Processing Server place donc les documents Web Intelligence en mémoire cache lorsqu'ils sont visualisés. Le serveur met également en cache les documents lorsqu'ils sont exécutés en tant que travail planifié si le premier cache a été activé dans le document.	**TRUE**
Taille maximale de la mémoire cache du document (Ko)	Taille maximale du document mis en cache. Une fois cette limite atteinte, la mémoire cache de document est effacée en fonction de la propriété `<Espace de réduction max du cache de document (Mo)>`.	1000000
Espace maximum de réduction du cache du document (pourcentage)	Pourcentage de mémoire cache devant être vidé afin de pouvoir stocker des actions et des résultats plus récents dans cette mémoire cache. Les documents dont l'« heure du dernier accès » est la plus ancienne sont purgés.	70
Taille maximale du flux de caractères (Mo)	Taille maximale du flux de caractères envoyé au client Web Intelligence. **Remarque** Si la propriété *Taille maximale du flux de caractères (Mo)* est dépassée, le document Web Intelligence n'est pas créé et le client reçoit un message d'erreur.	5 La plage valide est comprise entre 1 et 4 095 Mo.
Taille maximale des flux binaires (Mo)	Taille maximale, en Mo, du flux binaire envoyé au client Web Intelligence. **Remarque** Si la propriété *Taille maximale des flux binaires (Mo)* est dépassée, le document Web Intelligence n'est pas créé et le client reçoit un message d'erreur.	50 La plage valide est comprise entre 1 et 4 095 Mo.
Répertoire des images	Emplacement du répertoire des images.	Vierge
Répertoire de la mémoire cache de sortie	Emplacement de la mémoire cache.	Vierge

Propriétés générales

Propriété	Description	Valeur par défaut
Délai d'expiration de la connexion unique (secondes)	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	86400

Informations associées

Paramètres des seuils de mémoire du serveur Web Intelligence [page 1210]

35.1.7.1 Paramètres des seuils de mémoire du serveur Web Intelligence

Les sections suivantes décrivent ce qui se passe sur un serveur Web Intelligence lorsque le seuil maximal, le seuil supérieur et le seuil inférieur de la mémoire sont atteints.

Seuil inférieur de la mémoire (Mo)

Si la limite `<Seuil inférieur de la mémoire>` est atteinte, le serveur permute les documents inactifs sur le disque dur, ce qui permet d'allouer de la mémoire supplémentaire pour les documents actifs. Chaque utilisateur est autorisé à avoir un seul document actif au lieu du `<Nombre maximal de documents par utilisateur>`.

Seuil supérieur de la mémoire (Mo)

Si le `<Seuil supérieur de la mémoire>` est atteint, les actions de serveur suivantes sont exécutées afin de libérer des ressources et de protéger le serveur.

- Le serveur refuse les nouvelles connexions et les nouveaux appels de clients. Seule l'option *Enregistrer* est autorisée pour les documents Web Intelligence. Les utilisateurs ayant besoin d'effectuer une action reçoivent un message `Serveur occupé` leur demandant d'enregistrer les modifications en cours.
- Le serveur active le nettoyage du système de façon à libérer suffisamment de ressources afin que le volume de mémoire alloué soit inférieur à la limite définie par la propriété `<Seuil supérieur de la mémoire (Mo)>`.
- Le serveur essaie de fermer les documents en lecture seule.
- Si la mémoire libérée lors du nettoyage du système n'est pas suffisante, le serveur commence à fermer les documents qui se trouvent en mode *Modification*. Il ferme les documents en appliquant le protocole LIFO (Last In First Out) : le document actif le plus récent est purgé de la mémoire en premier. Il continue à fermer les documents jusqu'à ce qu'un niveau de sécurité soit atteint. Ce niveau est calculé de la façon suivante : `<Seuil supérieure de la mémoire>` - (20 % *(`<Seuil supérieur de la mémoire>`)). Par exemple, si la propriété Seuil supérieur de la mémoire a pour valeur 4 500 Mo, le niveau de sécurité est :

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  Le serveur ne peut pas fermer les documents quand un appel de client est exécuté. Aucun document actualisé ou exporté dans un autre format ou aucune autre opération prenant du temps ne sera fermé quand le serveur atteint ce seuil. Si le serveur ne récupère pas suffisamment de mémoire et reste au-dessus du `<Seuil supérieur de la mémoire>`, il redémarre.

Seuil maximal de la mémoire (Mo)

Si la limite <Seuil maximal de la mémoire> est atteinte, toutes les opérations en cours sont abandonnées. Tous les appels de clients sont interrompus. Après interruption d'un appel, le document correspondant est fermé.

36 Annexe métrique système

36.1 A propos de l'annexe Métriques du serveur

Dans cette annexe, sauf mention contraire, le terme serveur fait référence à un serveur SAP BusinessObjects et non à l'ordinateur où est installée ou exécutée la plateforme de BI.

Les métriques de serveur ne sont pas disponibles sur les serveurs qui ne fonctionnent pas.

En plus des métriques décrites dans cette annexe, l'application de surveillance peut également surveiller ces états de serveur :

Etat des serveurs	Description
État	Etat indique l'état général d'un serveur Valeurs possibles : • 0 = Rouge (Danger) • 1 = Orange (Attention) • 2 = Vert (Sain)
État activé du serveur	Cet état indique si un serveur est activé ou désactivé. Valeurs possibles : • 0 = Désactivé • 1 = Activé
État d'exécution du serveur	Cet état indique l'état d'exécution du serveur. Valeurs possibles : • 0 = ARRETE • 1 = DEMARRAGE EN COURS • 2 = INITIALISATION EN COURS • 3 = EXECUTION EN COURS • 4 = ARRET EN COURS • 5 = ECHEC • 6 = EXECUTION_AVEC_ERREURS • 7 = EXECUTION_AVEC_AVERTISSEMENTS

36.1.1 Métriques communes du serveur

Ces métriques décrivent l'ordinateur sur lequel s'exécute le serveur spécifié.

Métriques spécifiques à l'ordinateur

Métrique	Description
Nom de l'ordinateur	Nom d'hôte de l'ordinateur sur lequel s'exécute le serveur.
Système d'exploitation	Système d'exploitation de l'ordinateur sur lequel s'exécute le serveur.
Type de processeur	Type des processeurs de l'ordinateur sur lequel s'exécute le serveur. Cette métrique n'est pas disponible sur les serveurs de traitement adaptatif ou les serveurs conteneurs d'applications Web (WACS).
Processeurs	Nombre de processeurs disponibles sur le serveur. Sur du matériel multicœur, cette métrique peut faire référence au nombre d'unités logiques et non pas au nombre de processeurs physiques. Cette métrique n'est pas disponible sur les serveurs de traitement adaptatif ou les serveurs conteneurs d'applications Web (WACS).
Nombre de cœurs de processeur	Affiche le nombre de cœurs de processeur dans un ordinateur où le serveur de la plateforme de BI est hébergé.
RAM (Mo)	Quantité de mémoire en mégaoctets disponible sur l'ordinateur sur lequel s'exécute le serveur. Cette métrique n'est pas disponible sur les serveurs de traitement adaptatif ou les serveurs conteneurs d'applications Web (WACS).
Heure locale	Heure locale.
Taille du disque (Go)	Taille du disque sur lequel la plateforme de BI est installée, en giga-octets. Cette métrique n'est pas disponible sur les serveurs de traitement adaptatif ou les serveurs conteneurs d'applications Web (WACS).
Espace disque utilisé (Go)	Espace utilisé sur le disque sur lequel la plateforme de BI est installée, en giga-octets. Cette valeur comprend l'espace disque utilisé par la plateforme de BI ainsi que celui qu'utilisent d'autres programmes sur l'ordinateur. Cette métrique n'est pas disponible sur les serveurs de traitement adaptatif ou les serveurs conteneurs d'applications Web (WACS).

Les métriques suivantes décrivent le serveur SAP BusinessObjects spécifié.

Métriques spécifiques au serveur

Métrique	Description
Nom du serveur	Nom et numéro de port du serveur CMS sur lequel ce serveur publie son adresse.
Nom enregistré	Nom interne du serveur. Il ne s'agit pas du nom qui figure dans l'écran *Serveurs* de la CMC.
Version	Version du serveur.
Heure de début	Heure de démarrage du serveur la plus récente.
PID	Numéro d'identification unique du processus du serveur. Le système d'exploitation de l'ordinateur sur lequel s'exécute le serveur génère le PID. Le PID peut être utilisé pour identifier un serveur particulier.
Nom d'hôte	Liste au format CSV de tous les noms d'hôte actuellement utilisés sur le serveur.
Adresse IP de l'hôte	Liste au format CSV des adresses IP pour lesquelles le serveur est à l'écoute des requêtes.

Métrique	Description
Port de requêtes	Port à partir duquel le serveur reçoit les requêtes émanant d'autres serveurs. Si le serveur est à l'écoute des requêtes sur plusieurs adresses IP, le port de requêtes du serveur sera toujours le même. Si un autre processus utilise ce port de requêtes, le serveur ne démarre pas. Assurez-vous qu'aucun autre processus n'utilise ce port.
Threads serveur occupé	Nombre de threads serveur assurant simultanément un service pour une requête. Si ce nombre est le même que le volume maximal du pool de threads du serveur, cela signifie que le système ne peut pas traiter parallèlement d'autres requêtes et qu'il est possible que les nouvelles requêtes doivent attendre que le thread occupé se libère.

Métriques d'audit

Métrique	Description
Nombre actuel d'événements d'audit en attente	Nombre d'événements d'audit enregistrés par un candidat à l'audit, mais n'ayant pas encore été extraits par l'auditeur CMS. Si ce nombre augmente sans limites, cela peut signifier que les audits ne sont pas correctement configurés ou que le système a une charge importante et génère des événements d'audit plus vite que l'auditeur ne peut les extraire. **Remarque** Lorsque vous arrêtez un serveur, désactivez-le dans un premier temps, puis attendez que sa métrique soit à « 0 ». Sinon, des événements d'audit pourraient rester dans la file d'attente et ne pas atteindre le magasin de données d'audit tant que le serveur n'a pas été redémarré et que la CMC ne les a pas interrogés.

Journalisation des métriques de service

Métrique	Description
Répertoire de journalisation	Les fichiers journaux du serveur se trouvent à cet emplacement.

36.1.2 Métriques du Central Management Server

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* pour les serveurs CMS (Central Management Server).

Métriques du Central Management Server

Métrique	Description
La connexion à la base de données d'audit est établie	Indique si le CMS a une connexion de qualité à la base de données d'audit. La valeur « 1 » indique qu'il existe une connexion. La valeur « 0 » indique qu'il n'existe pas de connexion à la base de données d'audit. Si le CMS est un auditeur, cette valeur doit être « 1 ». Si c'est « 0 », recherchez pourquoi aucune connexion à la base de données d'audit ne peut être établie.

Métrique	Description
Auditeur CMS	Indique si le CMS agit en tant qu'auditeur. La valeur « 1 » indique que le CMS agit en tant qu'auditeur. La valeur « 0 » indique que le CMS n'agit pas en tant qu'auditeur.
Nom de la connexion à la base de données d'audit	Nom de la connexion à la base de données d'audit. Ce n'est pas obligatoirement le nom de la base de données d'audit elle-même. Si cette métrique est vide, elle indique qu'une connexion à la base de données d'audit ne peut être établie.
Nom d'utilisateur de la base de données d'audit	Nom du compte utilisateur utilisé pour se connecter à la base de données d'audit.
Date de la dernière mise à jour de la base de données d'audit	Date et heure les plus récentes où le CMS a commencé avec succès l'extraction d'événements d'un candidat à l'audit. Si le CMS est un auditeur, cette métrique doit afficher une heure proche de celle à laquelle est chargé l'écran « Métriques ». Si cette valeur est supérieure à deux heures avant l'heure à laquelle est chargé l'écran, il se peut que l'audit ne fonctionne pas correctement.
Durée du dernier cycle d'interrogation du thread d'audit (secondes)	Durée du dernier cycle d'interrogation en secondes. Il s'agit du délai maximum nécessaire pour que les données d'événement atteignent la base de données d'audit durant le cycle d'interrogation précédent. • Une valeur inférieure à 20 minutes indique que le système est sain. • Une valeur comprise entre 20 minutes et 2 heures indique que le système est occupé. • Une valeur supérieure à 2 heures indique que le système est très occupé. Si cet état persiste et que vous estimez que le délai est trop long, il est recommandé de mettre à jour le déploiement pour que toutes les bases de données d'audit reçoivent les données avec un meilleur débit ou de diminuer le nombre d'événements d'audit suivis par le système.
Utilisation du thread d'audit	Pourcentage du temps du cycle d'interrogation que l'auditeur CMS passe à recueillir les données des candidats à l'audit. Le reste du temps se passe en attente entre les interrogations. Si cette valeur atteint 100 %, cela signifie que l'auditeur continue à collecter des données auprès des candidats à l'audit alors que l'interrogation suivante devrait commencer. Ceci peut entraîner des retards sur le moment où les événements atteignent la base de données d'audit. Si l'utilisation du thread atteint souvent 100 % et reste à ce niveau pendant plusieurs jours, il est recommandé de mettre à jour le déploiement pour que la base de données d'audit reçoivent les données avec un meilleur débit ou de diminuer le nombre d'événements d'audit suivis par votre système.
Serveurs CMS en cluster	Liste séparée par des points-virgules des noms d'hôte et numéros de port des serveurs CMS en cours de fonctionnement dans le cluster.
Nombre de sessions établies par des utilisateurs simultanés	Total des sessions des utilisateurs ayant une licence d'accès simultané.
Nombre de sessions établies par des utilisateurs nommés	Total des sessions des utilisateurs ayant une licence nommée.
Nombre maximum de sessions depuis le démarrage	Nombre maximum de sessions utilisateur simultanées gérées par le CMS depuis son démarrage.

Métrique	Description
Nombre de sessions établies par des serveurs	Nombre des sessions simultanées que les serveurs de la plateforme de BI ont créées avec le CMS. Si ce nombre est supérieur à 250, créez un autre CMS.
Nombre de sessions établies par tous les utilisateurs	Nombre de sessions utilisateur simultanées gérées par le CMS lors du chargement de l'écran *Métriques*. Plus le nombre est important, plus le nombre d'utilisateurs du système l'est également. Si ce nombre est supérieur à 250, créez un autre CMS.
Travaux en échec	Nombre de travaux échoués sur le système.
Travaux en suspens	Nombre de travaux planifiés, mais pas prêts à s'exécuter parce que l'heure planifiée est à venir ou l'événement ne s'est pas produit.
Travaux en cours d'exécution	Nombre de travaux s'exécutant actuellement.
Travaux terminés	Nombre de travaux réalisés sur le système.
Travaux en attente	Nombre de travaux dans le système qui sont planifiés et en attente de ressources disponibles.
Licences Utilisateur simultané	Nombre de licences Utilisateurs simultané indiqué par le code clé.
Licences Utilisateur nommé	Nombre de licences Utilisateur nommé indiqué par le code clé.
Date de version	Date de version du CMS.
Nom de la connexion à la base de données système	Nom de la connexion à la base de données système du CMS. Il ne s'agit pas obligatoirement du nom de la base de données système du CMS elle-même.
Nom du serveur de la base de données système	Nom du serveur sur lequel est exécutée la base de données système du CMS. Il ne s'agit pas obligatoirement du nom de la base de données système du CMS elle-même.
Nom de l'utilisateur de la base de données système	Nom du compte utilisateur utilisé pour se connecter à la base de données système du CMS.
Nom de la source de données	Nom de la connexion à la base de données système du CMS.
Numéro de version	Numéro de version du CMS. Ce numéro peut être utilisé pour identifier la version de la plateforme SAP BusinessObjects Business Intelligence qui est installée.
Version du produit	Version du produit du CMS.
Version de la ressource	Version de la ressource du CMS.
Temps de réponse moyen de validation depuis le démarrage (ms)	Durée moyenne en millisecondes nécessaire au CMS pour exécuter des opérations de validation depuis que le serveur a été démarré. Un temps de réponse supérieur à 1 000 millisecondes peut indiquer qu'il faut ajuster la configuration du CMS ou de la base de données système du CMS.
Temps de réponse moyen des requêtes depuis le démarrage (ms)	Durée moyenne en millisecondes nécessaire au CMS pour exécuter des opérations de requête depuis que le serveur a été démarré. Un temps de réponse supérieur à 1 000 millisecondes peut indiquer qu'il faut ajuster la configuration du CMS ou de la base de données système du CMS.
Temps de réponse maximum de validation depuis le démarrage (ms)	Durée maximale en millisecondes nécessaire au CMS pour exécuter des opérations de validation depuis que le serveur a été démarré. Un temps de réponse supérieur à 1 000 millisecondes peut indiquer qu'il faut ajuster la configuration du CMS ou de la base de données système du CMS.

Métrique	Description
Temps de réponse maximum des requêtes depuis le démarrage (ms)	Durée maximale en millisecondes nécessaire au CMS pour exécuter des opérations de requête depuis le démarrage du serveur. Un temps de réponse supérieur à 1 000 millisecondes peut indiquer qu'il faut ajuster la configuration du CMS ou de la base de données système du CMS.
Nombre de validations depuis le démarrage	Nombre de validations sur la base de données système du CMS depuis le démarrage du serveur.
Nombre de requêtes depuis le démarrage	Nombre total des requêtes sur la base de données depuis le démarrage du serveur. Un nombre important peut indiquer un système plus actif ou fortement chargé.
Nombre de connexions utilisateur depuis le démarrage	Nombre total de connexions des utilisateurs depuis le démarrage du serveur. Un nombre important peut indiquer un système plus actif ou fortement chargé.
Connexions à la base de données système établies	Nombre de connexions à la base de données système du CMS que le CMS a pu établir. Si une connexion à la base de données est interrompue, le CMS tente de la restaurer. Si le nombre de connexions établies à la base de données est nettement inférieur au nombre indiqué par la propriété *Connexions à la base de données système requises* (zone *Central Management Service* de l'écran *Propriétés*), cela peut signifier que le CMS ne peut pas acquérir d'autres connexions et que le système ne fonctionne pas de façon optimale. Dans ce cas, une solution consiste à configurer le serveur de base de données de sorte à permettre plus de connexions à la base de données pour le CMS.
Connexions à la base de données système en cours d'utilisation	Nombre de connexions à la base de données système du CMS que le CMS utilise actuellement. Le nombre de connexions en cours d'utilisation peut être inférieur ou égal au nombre de connexions établies à la base de données système. Si le nombre de connexions établies et le nombre de connexions utilisées sont identiques pendant un certain temps, cela peut indiquer un goulot d'étranglement. L'augmentation de la valeur de la propriété *Connexions à la base de données système requises* dans l'écran *Propriétés* peut améliorer les performances du CMS. L'ajustement de la configuration de la base de données système du CMS peut également améliorer les performances.
Demandes à la base de données système en suspens	Nombre de requêtes à la base de données système du CMS en attente d'une connexion disponible. Si ce nombre est élevé, envisagez d'augmenter la valeur de la propriété *Connexions à la base de données système requises*. L'ajustement de la configuration de la base de données système du CMS peut également améliorer les performances.
Nombre d'objets dans le cache système du CMS	Nombre total d'objets actuellement dans le cache système du CMS.
Nombre d'objets dans la BD système du CMS	Nombre total d'objets actuellement dans la base de données système du CMS.
Comptes utilisateur simultané existants	Nombre total des utilisateurs existants ayant une licence d'accès simultané dans le cluster.
Comptes utilisateur nommé existants	Nombre total des utilisateurs existants ayant une licence nommée dans le cluster.

36.1.3 Métrique du serveur de connexion

La métrique suivante est propre au Connection Server.

Métriques du service de connectivité

Métrique	Description
Sources de données	Répertorie dans un tableau les sources de données activées via la page *Propriétés*. Affiche les informations suivantes pour chaque couche réseau et paire de bases de données : • *Statut* (*Chargé* ou *Echec*) : statut actuel du pilote • *Connexions disponibles : nombre de connexions pouvant être utilisées dans le pool* • *Travaux (CORBA) : nombre de travaux en cours de traitement (déploiement à 2 niveaux)* • *Travaux (HTTP) : nombre de travaux en cours de traitement (déploiement de niveau Web)* **Remarque** Pour plus d'informations sur les pools de connexion, voir le *Guide d'accès aux données*.

36.1.4 Métriques de l'Event Server

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* pour les serveurs Event Server.

Métrique de service d'événement

Métrique	Description
Liste des fichiers contrôlés	Tableau répertoriant les fichiers contrôlés par l'Event Server. La colonne « Nom du fichier » affiche le nom et le chemin d'accès du fichier. La colonne « Heure de la dernière notification » affiche le dernier horodatage d'interrogation et de détection du fichier par le serveur.
Fichiers contrôlés	Nombre total des fichiers contrôlés par l'Event Server.

36.1.5 Métriques du File Repository Server

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* pour les serveurs Input File Repository Server et Output File Repository Server.

Métrique de service de stockage de fichiers

Métrique	Description
Fichiers actifs	Nombre de fichiers du File Repository Server actuellement en cours d'accès.
Données écrites (Mo)	Total des mégaoctets écrits dans les fichiers du serveur.
Données envoyées (Mo)	Total des mégaoctets lus dans les fichiers du serveur.
Liste des fichiers actifs	Tableau affichant les fichiers du File Repository Server actuellement en cours d'accès.
Connexions actives	Nombre total de connexions actives à partir des clients et vers les autres serveurs.
Espace disque disponible dans le répertoire racine (Go)	Volume total d'espace disponible sur le disque contenant le fichier exécutable du serveur, en giga-octets.
Espace disque libre dans le répertoire racine (Go)	Volume total d'espace libre sur le disque contenant le fichier exécutable du serveur, en giga-octets.
Espace disque total dans le répertoire racine (Go)	Espace disque total sur le disque contenant le fichier exécutable du serveur, en giga-octets.
Espace disque disponible dans le répertoire racine (%)	Volume d'espace disque, en pourcentage, disponible sur le disque contenant le fichier exécutable du serveur.

36.1.6 Métriques du serveur de traitement adaptatif

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* pour les serveurs de traitement adaptatif.

Métriques du serveur de traitement adaptatif

Métrique	Description
Threads de la couche de transport	Nombre total de threads dans l'ensemble des pools de la couche de transport.
Taille du pool de threads de la couche de transport	Nombre total de threads partagés de la couche de transport. Ces threads peuvent être utilisés par n'importe quel service hébergé sur le serveur de traitement adaptatif.
Processeurs disponibles	Nombre de processeurs disponibles pour la machine virtuelle Java (JVM) sur laquelle le serveur est exécuté.
Taille maximale de la mémoire (Mo)	Mémoire maximale en mégaoctets que la machine virtuelle Java va tenter d'utiliser.
Mémoire libre (Mo)	Quantité de mémoire (en mégaoctets) disponible sur la JVM pour l'allouer à de nouveaux objets.
Mémoire totale (Mo)	Mémoire totale en mégaoctets dans la machine virtuelle Java. Cette valeur peut varier au cours du temps selon l'environnement hôte.
Pourcentage d'utilisation du processeur (les 5 dernières minutes)	Pourcentage du temps processeur total utilisé par le serveur au cours des cinq dernières minutes. Par exemple, si un seul thread utilise entièrement un processeur d'un système à 4 processeurs, l'utilisation est de 25 %. Tous les processeurs affectés à la JVM sont pris en compte. Une valeur supérieure à 80 % peut indiquer un goulot d'étranglement au niveau du processeur.

Métrique	Description
Pourcentage d'utilisation du processeur (les 15 dernières minutes)	Pourcentage du temps processeur total utilisé par le serveur au cours des quinze dernières minutes. Par exemple, si un seul thread utilise entièrement un processeur d'un système à 4 processeurs, l'utilisation est de 25 %. Tous les processeurs affectés à la JVM sont pris en compte. Une valeur supérieure à 70 % peut indiquer un goulot d'étranglement.
Pourcentage d'utilisation du système interrompu lors du GC (les 5 dernières minutes)	Pourcentage d'utilisation du système interrompu pendant l'exécution des Garbage Collections (GC) au cours des cinq dernières minutes. Dans cet état, les services APS ne peuvent pas s'exécuter lorsque la machine virtuelle effectue l'étape critique de rassemblement des données erronées, qui requiert un accès exclusif. Normalement, une valeur basse à un seul chiffre doit être le comportement normal, même avec de la charge. Une valeur à deux chiffres en permanence peut indiquer un problème de faiblesse du débit qui impose d'effectuer des recherches.
Pourcentage d'utilisation du système interrompu lors du GC (les 15 dernières minutes)	Pourcentage d'utilisation du système interrompu pendant l'exécution des Garbage Collections (GC) au cours des quinze dernières minutes. Dans cet état, les services APS ne peuvent pas s'exécuter lorsque la machine virtuelle effectue l'étape critique de rassemblement des données erronées, qui requiert un accès exclusif. Normalement, une valeur basse à un seul chiffre doit être le comportement normal, même avec de la charge. Une valeur à deux chiffres en permanence peut indiquer un problème de faiblesse du débit qui impose d'effectuer des recherches.
Nombre d'erreurs de page lors du GC (les 5 dernières minutes)	Nombre d'erreurs de page s'étant produites pendant l'exécution des Garbage Collections au cours des cinq dernières minutes. Toute valeur supérieure à 0 indique que le système est en état de charge importante et de faiblesse mémoire.
Nombre d'erreurs de page lors du GC (les 15 dernières minutes)	Nombre d'erreurs de page s'étant produites pendant l'exécution des Garbage Collections au cours des quinze dernières minutes. Toute valeur supérieure à 0 indique que le système est en état de charge importante et de faiblesse mémoire.
Nombre de GC complets	Nombre de Garbage Collections complètes depuis le démarrage du serveur. Une augmentation rapide de cette valeur peut indiquer que le système est en état de faiblesse mémoire.
Nombre de contentions de verrouillage de la JVM	Nombre d'objets synchronisés ayant des threads en attente d'accès. Toute valeur nettement supérieure à 0 peut indiquer des threads qui ne s'exécuteront pas à nouveau. Lancez un vidage des thread pour obtenir des informations sur la cause du problème.
Informations de débogage de la JVM	Informations de débogage sur la machine virtuelle Java SAP comprenant l'état, le port et éventuellement le client associé.
Informations de version de la JVM	Informations de version sur la machine virtuelle Java SAP.
Nombre de threads bloqués de la JVM	Nombre de threads bloqués. Toute valeur supérieure à 0 indique des threads qui ne s'exécuteront pas à nouveau. Lancez un vidage des thread pour obtenir des informations sur la cause du problème.
Indicateurs de trace JVM	Les indicateurs de trace actuellement activés pour la JVM. Ceci indique le niveau de traçage de la JVM.

Métrique	Description
Services	Liste au format CSV des services hébergés par le serveur.

Métriques de service DSL Bridge

Métrique	Description
DSLServiceMetrics.queryCount	Nombre de requêtes de données ouvertes entre les clients et le service.
DSLServiceMetrics.activeConnectionCount	Nombre de connexions actuellement ouvertes entre les clients et le service.
DSLServiceMetrics.activeSessionCount	Nombre de sessions actuellement ouvertes entre les clients et le service.
DSLServiceMetrics.activeOLAPConnection Count	Nombre de connexions actuellement ouvertes entre les clients OLAP et le service.

Métriques de service proxy d'audit client

Métrique	Description
Nombre d'événements d'audit reçus depuis le démarrage du serveur	Nombre d'événements d'audit client reçus par le service depuis son démarrage. Cette métrique peut être utilisée pour vérifier que l'audit client a été configuré correctement. Les valeurs supérieures à « 0 » indiquent que les événements d'audit client sont correctement acheminés par le biais du service d'audit client.

Métriques du service de recherche de plateformes

Métrique	Description
Nombre de tentatives d'extraction réussies depuis le démarrage du service	Nombre de tentatives réussies d'extraction des documents depuis le démarrage du service de recherche de plateformes.
Horodatage de la dernière mise à jour de l'index	Date et heure de la dernière mise à jour de l'index
Horodatage de la dernière génération de stockage de contenus	Date et heure de la génération du dernier stockage du contenu.
Nombre de tentatives d'extraction échouées depuis le démarrage du service	Nombre de tentatives échouées d'extraction des documents depuis le démarrage du service de recherche de plateformes.
Service disponible	TRUE si le service est disponible. Sinon, FALSE.
Exécution de l'indexation	TRUE si l'indexation est en cours d'exécution. Sinon, FALSE.
Nombre de documents indexés	Affiche le nombre de documents ayant été annexés depuis le démarrage du service.

Métriques du service MDAS (Multi-Dimensional Analysis Service)

Métrique	Description
Nombre de sessions	Nombre actuel de connexions entre les clients MDAS et le serveur.
Nombre de cubes	Nombre de sources utilisées pour fournir des données aux connexions n'ayant pas expiré.
Nombre de requêtes	Nombre de requêtes de données ouvertes entre les clients MDAS et le serveur.

Métriques du service de fédération de données

Métrique	Description
Nombre de requêtes en cours d'exécution	Nombre total de requêtes en cours (consommant ou non de la mémoire).
Nombre de connexions	Nombre total de connexions d'utilisateur au moteur de requête de fédération de données.
Nombre total d'octets transférés des sources de données	Volume des données lues à partir des sources de données (en octets).
Nombre total d'enregistrements transférés des sources de données	Nombre total de lignes lues à partir des sources de données.
Nombre total d'octets produits par l'exécution de la requête	Volume des données de sortie des requêtes (en octets).
Nombre total d'enregistrements produits par l'exécution de la requête	Nombre total de lignes de sortie des requêtes.
Nombre de requêtes consommant de la mémoire	Nombre de requêtes en cours consommant de la mémoire.
Nombre total d'octets de mémoire utilisés par l'exécution de la requête	Volume de mémoire actuellement utilisé par les requêtes en cours d'exécution (en octets).
Nombre total d'octets du disque utilisés par l'exécution de la requête	Volume du disque actuellement utilisé par les requêtes en cours d'exécution (en octets).
Nombre de requêtes utilisant le disque	Nombre total de requêtes en cours utilisant le disque.
Nombre de requêtes en attente de ressources	Nombre total de requêtes en cours en attente d'exécution
Nombre de threads actifs	Nombre total de threads actifs utilisés pour l'exécution des requêtes.
Nombre total d'octets de mémoire utilisés par le cache des métadonnées	Volume de mémoire utilisé pour la mise en cache de la configuration connecteurs, des métadonnées et des statistiques (en octets).
Nombre d'échecs de requêtes	Nombre total de requêtes échouées (exceptions survenues).
Nombre de requêtes dans l'étape d'analyse des requêtes	Nombre total de requêtes en cours d'exécution actuellement à l'étape d'analyse.
Nombre de requêtes dans l'étape d'optimisation de la requête	Nombre total de requêtes en cours actuellement à l'étape d'optimisation.
Nombre de requêtes dans l'étape d'exécution de la requête	Nombre total de requêtes en cours actuellement à l'étape d'exécution.
Nombre de connecteurs chargés	Nombre total de connecteurs chargés dans le service.
Nombre de connexions actives aux connecteurs chargés	Nombre total de connexions actives aux connecteurs chargés dans le service.
Le service de fédération de données est disponible	*TRUE* si le service est disponible. Sinon, *FALSE*.

Métriques du service de connectivité

Métrique	Description
Sources de données	Répertorie dans un tableau les sources de données activées dans la page *Propriétés*. Affiche les informations suivantes pour chaque couche réseau et paire de bases de données : • Statut (« Chargé » ou « Echec ») : statut actuel du pilote • Connexions disponibles : nombre de connexions pouvant être utilisées dans le pool • Travaux (CORBA) : nombre de travaux en cours de traitement (déploiement à 2 niveaux) • Travaux (HTTP) : nombre de travaux en cours de traitement (déploiement de niveau Web) Pour plus d'informations sur les pools de connexion, voir le *Guide d'accès aux données*.

service de surveillance des métriques

Métrique	Description
Durée moyenne de l'état de la veille pour les 15 derniers cycles (msec)	Durée moyenne requise pour le calcul de l'état de la veille pour les 15 derniers cycles, pour ce service de gestion de l'instance.
Nombre de métriques créées par l'utilisateur	Nombre total de métriques créées par l'utilisateur dans le cluster, pour tous les utilisateurs.
Nombre de veilles	Nombre total de veilles dans le cluster, y compris les veilles désactivées et activées.
serviceBean.monitoringAppPropEnabled	TRUE si l'application de surveillance est activée. Sinon, FALSE. Cette métrique correspond aux paramètres de la page Surveillance des propriétés de l'application dans la CMC.
Intervalle d'actualisation des métriques de surveillance (en secondes)	Intervalle d'actualisation actuellement utilisé par cette instance du service de surveillance. Au démarrage du service, cette métrique est initialisée sur le paramètre de la page Surveillance des propriétés de l'application dans la CMC à ce moment précis et peut donc, à d'autres moments, être différente des paramètres de la page de la CMC.
Service disponible	TRUE si le service de surveillance est actif. Sinon, FALSE. Seul le service de surveillance est actif dans le cluster.
Nombre de métriques de tendances	Nombre total de métriques actuellement enregistrées dans la base de données de surveillance.

Métriques de service des applications Web BEx

Métrique	Description
Nombre de sessions	Nombre total de sessions actives dans le service des applications Web BEx.

36.1.7 Métriques de serveurs conteneurs d'applications Web

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* pour les serveurs conteneurs d'applications Web.

> **Remarque**
>
> Les serveurs conteneurs d'applications Web possèdent également toutes les métriques décrites à la section Métriques du serveur de traitement adaptatif.

Métriques de serveurs conteneurs d'applications Web

Métrique	Description
Liste des connecteurs WACS en cours d'exécution	Liste de tous les connecteurs en cours d'exécution sur le serveur. Si vous ne voyez pas l'ensemble des connecteurs (HTTP, HTTPS et HTTP via proxy), cela indique que le connecteur n'est pas activé ou qu'il y a eu un échec au démarrage.
Echecs des connecteurs WACS au démarrage	Signale des défaillances de connecteurs. Si cette option a pour valeur True, cela signifie qu'au moins un connecteur n'a pas pu démarrer. Si elle a pour valeur False, tous les connecteurs fonctionnent. N'exécutez pas un serveur lorsqu'un ou plusieurs connecteurs n'ont pas réussi à démarrer ; vous devez dépanner le serveur pour vous assurer que tous les connecteurs démarrent correctement.

Informations associées

Métriques du serveur de traitement adaptatif [page 1219]

36.1.8 Métriques d'Adaptative Job Server

Métriques de Job Server

Métrique	Description
Demandes de travaux reçues	Nombre de travaux supposés s'être exécutés sur le serveur.
Travaux simultanés	Nombre de travaux s'exécutant simultanément sur le serveur. Si ce nombre est élevé, le serveur est occupé.
Nombre maximal de travaux	Nombre maximal de travaux simultanés exécutés en même temps sur le serveur. Ce nombre ne diminue jamais jusqu'au redémarrage du serveur.
Échecs de création de travaux	Nombre de travaux ayant échoué sur le serveur.
Répertoire temporaire	Répertoire dans lequel les fichiers temporaires sont créés. Il peut être spécifié dans l'écran *Propriétés* du serveur. Vous pouvez rencontrer des problèmes si ce répertoire ne dispose pas d'un espace disque suffisant.
Paramètres par défaut valides pour la destination Système de fichiers	*TRUE* si le serveur peut envoyer des documents à la destination Système de fichiers spécifiée dans l'écran *Destination* du serveur. Sinon, *FALSE*.
Paramètres par défaut valides pour la destination FTP	*TRUE* si le serveur peut envoyer des documents à la destination FTP spécifiée dans l'écran *Destination* du serveur. Sinon, *FALSE*.

Métrique	Description
Paramètres par défaut valides pour la destination SFTP	*TRUE* si le serveur peut envoyer des documents à la destination SFTP spécifiée dans l'écran *Destination* du serveur. Sinon, *FALSE*. Vous pouvez rencontrer des problèmes si l'empreinte ne correspond pas exactement au serveur SFTP.
Paramètres par défaut valides pour la destination boîte de réception	*TRUE* si le serveur peut envoyer des documents à la destination boîte de réception spécifiée dans l'écran *Destination* du serveur. Sinon, *FALSE*.
Paramètres par défaut valides de la destination Courrier électronique	*TRUE* si le serveur peut envoyer des documents à la destination courrier électronique spécifiée dans l'écran *Destination* du serveur. Sinon, *FALSE*.
Services de planification	Tableau affichant les services en cours d'exécution sur le serveur.
Enfants	Tableau affichant les processus enfant en cours d'exécution sur le serveur.

Le tableau suivant décrit les métriques de chaque service de planification en cours d'exécution sur le serveur.

Planification des métriques de service

Métrique	Description
Service de planification	Nom du service.
Demandes de travaux reçues	Nombre de travaux supposés s'être exécutés sur le service.
Travaux simultanés	Nombre de travaux simultanés s'exécutant simultanément sur le service. Si ce nombre est élevé, le service est occupé.
Nombre maximal de travaux	Nombre maximal de travaux simultanés exécutés en même temps sur le service.
Nombre maximal de travaux simultanés autorisés	Nombre de processus indépendants simultanés (processus enfant) autorisés par le service. Il peut être spécifié dans l'écran *Propriétés* du serveur.
Échecs de création de travaux	Nombre de travaux ayant échoué sur le service.

Le tableau suivant décrit les métriques de chaque processus enfant en cours d'exécution sur le serveur.

Métriques enfant

Métrique	Description
Service de planification	Nom du processus enfant.
PID	Identifiant du processus enfant.
Demandes de travaux reçues	Nombre de travaux supposés s'être exécutés sur le processus enfant.
Travaux simultanés	Nombre de travaux simultanés s'exécutant simultanément sur le processus enfant. Normalement, ce nombre doit être de « 1 ».
Nombre maximal de travaux	Nombre maximal de travaux simultanés exécutés en même temps sur le processus enfant.
Nombre maximal de travaux autorisés	Nombre de travaux simultanés autorisés par le processus enfant.
Échecs de communication	Nombre d'échecs de communication s'étant produits avec l'Adaptive Job Server. Si ce nombre est important, le processus enfant va redémarrer.

Métrique	Description
Initialisation en cours	*TRUE* si le processus enfant est en cours d'initialisation. Sinon, *FALSE*.
Arrêt en cours	*TRUE* si le processus enfant est en cours d'arrêt. Sinon, *FALSE*.

36.1.9 Métriques de Crystal Reports Server

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* des serveurs de traitement Crystal Reports et Crystal Reports 2020.

Métriques de Crystal Reports Processing Server

Métrique	Description
Travaux en cours	Liste sous forme de tableau des travaux en cours d'exécution sur le serveur. Le tableau inclut l'ID et le nom du document, le nom de l'utilisateur exécutant le travail, la date du dernier accès au document et le temps d'exécution du travail.
Nombre de requêtes servies	Nombre total de requêtes servies par le serveur depuis son démarrage.
Nombre de travaux en cours	Nombre de travaux en cours que le serveur et ses processus enfant sont en train de traiter.
Type d'objet	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
Durée de traitement moyenne (ms)	Temps moyen (en millisecondes) passé par le serveur à traiter les 500 dernières requêtes reçues. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Durée de traitement maximale (ms)	Temps maximal (en millisecondes) passé par le serveur à traiter l'une des dernières 500 requêtes. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Durée de traitement minimale (ms)	Temps minimal (en millisecondes) passé par le serveur à traiter l'une des dernières 500 requêtes. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Nombre de requêtes en attente	Nombre de requêtes en attente de traitement ou en train d'être traitées. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Nom de la DLL de l'objet	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
Nombre de connexions ouvertes	Nombre de connexions actuellement ouvertes entre le serveur et les clients.
Taux d'échec des requêtes	Nombre de requêtes que le serveur n'a pas pu traiter en tant que pourcentage des 500 dernières requêtes reçues par le serveur.
Données transférées (Ko)	Total des données (en kilo-octets) transmises aux clients depuis le démarrage du serveur.

Métrique	Description
Nombre de requêtes ayant échoué	Nombre de requêtes que le serveur n'a pas pu finaliser depuis son démarrage.
Nombre maximal de processus enfant	Nombre maximal de processus enfant simultanés autorisés sur le serveur.

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* des Crystal Reports Cache Servers.

Métriques de Crystal Reports Cache Server

Métrique	Description
Taux d'accès à la mémoire cache (%)	Pourcentage de requêtes sur les 500 dernières, qui ont été servies avec des données cachées.
Serveurs de traitement connectés	Tableau répertoriant les serveurs de traitement Crystal Reports de votre déploiement. Ce tableau indique le nom du serveur et le nombre de connexions ouvertes avec le serveur.
Nombre de requêtes servies	Nombre total de requêtes servies par le serveur depuis son démarrage.
Type d'objet	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
Durée de traitement moyenne (msec)	Temps moyen (en millisecondes) passé par le serveur à traiter les 500 dernières requêtes reçues. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Durée de traitement maximale (msec)	Temps maximal (en millisecondes) passé par le serveur à traiter l'une des dernières 500 requêtes. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Durée de traitement minimale (msec)	Temps minimal (en millisecondes) passé par le serveur à traiter l'une des dernières 500 requêtes. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Nombre de requêtes en attente	Nombre de requêtes en attente de traitement ou en train d'être traitées. Si ce chiffre est particulièrement élevé et continue d'augmenter, envisagez la création de serveurs supplémentaires sur d'autres ordinateurs.
Nom de la DLL de l'objet	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
Taille de la mémoire cache	Volume de données (en kilo-octets) actuellement mises en cache par le serveur sur le disque.
Nombre de connexions ouvertes	Nombre de connexions actuellement ouvertes entre le serveur et les clients.
Données transférées (Ko)	Total des données (en kilo-octets) transmises aux clients depuis le démarrage du serveur.

Le tableau suivant décrit les métriques de serveur figurant dans l'écran *Métriques* du Report Application Server Crystal Reports 2020.

Métriques du Report Application Server Crystal Reports 2020

Métrique	Description
metric_currentdoccount **Remarque** Cette métrique apparaît en tant que « document_s_ » sur la page de surveillance de la CMC.	Nombre de documents actuellement traités par le serveur.
metric_totaldoccount **Remarque** Cette métrique apparaît en tant que « document_s_ » sur la page de surveillance de la CMC.	Nombre de documents traités par le serveur depuis son démarrage.
metric_currentagentthreadcount **Remarque** Cette métrique apparaît en tant que « agent thread_s_ » sur la page de surveillance de la CMC.	Nombre de threads actuellement traités par le serveur.
metric_totalagentthreadcount **Remarque** Cette métrique apparaît en tant que « agent thread_s_ » sur la page de surveillance de la CMC.	Nombre de threads traités par le serveur depuis son démarrage.

36.1.10 Métriques de Web Intelligence Server

Métriques du service de traitement Web Intelligence

Métrique	Description
Cache size (Kb) (Taille de la mémoire cache (Ko))	Volume actuel en kilo-octets de données stockées dans le cache.
Number of out-of-date documents in cache (Nombre maximum de documents dans le cache)	Nombre de documents supprimés du cache en raison de leur ancienneté depuis le démarrage du serveur.
Cache high mark count (Nombre de marques supérieures du cache)	Nombre de fois où le cache a atteint la taille maximale autorisée sur le serveur depuis son démarrage.
CPU usage (%) (Utilisation du processeur (%))	Pourcentage du temps processeur total utilisé par le serveur depuis son démarrage.

Métrique	Description
Total CPU time (seconds) (Temps total du processeur (secondes))	Temps processeur total utilisé par le serveur depuis son démarrage, exprimé en secondes.
Memory high threshold count (Nombre de seuils supérieurs de la mémoire)	Nombre de fois où le seuil supérieur de la mémoire a été atteint sur le serveur depuis son démarrage.
Memory max threshold count (Nombre de seuils maximaux de la mémoire)	Nombre de fois où le seuil maximal de la mémoire a été atteint sur le serveur depuis son démarrage.
Virtual memory size (Mb) (Taille de la mémoire virtuelle (Mo))	Volume total de la mémoire en mégaoctets affecté au serveur.
Current number of client calls (Nombre actuel d'appels client)	Nombre actuel d'appels CORBA traités par le serveur.
Nombre d'erreurs d'extension distante	Nombre de fois où le serveur n'a pas pu se connecter à un service d'extension distante hébergé par un serveur de traitement adaptatif.
Current number of tasks (Nombre actuel de tâches)	Nombre actuel de tâches exécutées sur le serveur.
Total number of client calls (Nombre total d'appels client)	Nombre total d'appels CORBA reçus par le serveur depuis son démarrage.
Total number of tasks (Nombre total de tâches)	Nombre total de tâches exécutées sur le serveur depuis son démarrage.
Délai d'inactivité (secondes)	Temps écoulé, en secondes, depuis la dernière requête d'un client reçue par le serveur.
Current number of active sessions (Nombre actuel de sessions actives)	Nombre actuel de sessions pouvant accepter des requêtes de la part de clients.
Nombre de documents ouverts à partir du cache	Nombre de documents pour lesquels le dernier résultat de demande a été lu directement à partir du cache.
Number of documents (Nombre de documents)	Nombre de documents ouverts sur le serveur.
Current number of sessions (Nombre actuel de sessions)	Nombre actuel de sessions créées sur le serveur.
Number of document swap (Nombre de permutations de documents)	Nombre de documents pour lesquels un thread de nettoyage a planifié des requêtes de permutation.
Number of swapped documents (Nombre de documents permutés)	Nombre de documents permutés par des requêtes de permutation.
Number of sessions timeout (Nombre d'expirations de session)	Nombre de sessions ayant expiré depuis le démarrage du serveur.
Total number of sessions (Nombre total de sessions)	Nombre de sessions créées sur le serveur depuis son démarrage.
Number of users (Nombre d'utilisateurs)	Nombre total d'utilisateurs connectés au serveur.
Nombre de threads actifs	Nombre de demandes de prise en charge de threads reçues par le serveur (pool de threads asynchrone)
Nombre total de threads	Nombre total de threads ayant été créés depuis le démarrage du serveur (pool de threads asynchrone)

37 Annexe relative aux espaces réservés de nœuds et de serveurs

37.1 Espaces réservés de nœud et de serveur

A l'exception de *%NOM_CONVIVIAL_SERVEUR%* et *%NOM_SERVEUR%*, ces espaces réservés s'appliquent à tous les serveurs du même nœud.

> **Remarque**
>
> Les espaces réservés suivants peuvent être modifiés au niveau du nœud. Le tableau ci-dessous contient les descriptions et les valeurs par défaut. Les espaces réservés qui n'apparaissent pas dans cette liste sont en lecture seule.
>
> - *%DefaultAuditingDir%*
> - *%DefaultDataDir%*
> - *%DefaultLoggingDir%*
> - *%IntroscopeAgentEnableInstrumentation%*
> - *%IntroscopeAgentEnterpriseManagerHost%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **Attention**
>
> Les espaces réservés non destinés à la modification ne doivent en aucun cas être modifiés. L'administrateur système doit s'assurer que seule la personne appropriée du groupe d'administrateurs (qui assure la gestion des nœuds) dispose de droits de modification sur le nœud. Tous les autres utilisateurs, y compris les autres membres du groupe d'administrateurs, doivent disposer de droits limités à l'affichage/la gestion des objets du nœud. Les droits de sécurité appropriés doivent donc s'appliquer. Si l'une des valeurs d'espace réservé est accidentellement corrompue et que le CMS n'apparaît pas, reportez-vous à la note SAP 3269127.

> **Remarque**
>
> Reportez-vous à l'article 3278916 de la base de connaissances SAP pour savoir comment limiter la modification des espaces réservés et ainsi éviter toute interférence malveillante avec l'infrastructure BI.

Espaces réservés

Espace réservé	Description	Valeurs par défaut
%AuditingDatabaseConnection%	Connexion à la base de données d'audit utilisée par le CMS.	Cette valeur est spécifiée lors de l'installation.
%AuditingDatabaseDriver%	Type de pilote de base de données utilisé pour la connexion à la base de données d'audit.	Sous Windows, la valeur par défaut est sqlserverauditdbss.
%BINDIR%	Le dossier où les fichiers binaires 64 bits de la plateforme SAP BusinessObjects de Business Intelligence sont situés.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>/`
%BINDIR32%	Le dossier où les fichiers binaires 32 bits de la plateforme SAP BusinessObjects de Business Intelligence sont situés.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>/`
%CACHESERVER_EXE%	Nom du fichier exécutable du Crystal Reports Cache Server.	Sous Windows, `crcache.exe`. Sous UNIX : `boe_crcached.bin`
%CMS_EXE%	Nom du fichier exécutable du serveur Central Management Server.	Sous Windows, `cms.exe`. Sous UNIX, `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	Nom du fichier exécutable du Connection Server 32 bits.	Sous Windows, `ConnectionServer32.exe`. Sous UNIX, `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	Dossier racine du serveur de connexion.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
%CONNECTIONSERVER_EXE%	Nom du fichier exécutable du Connection Server 64 bits.	Sous Windows, `ConnectionServer.exe`. Sous UNIX, `ConnectionServer`.
%CRCPP_BINDIR%	Répertoire dans lequel se trouvent les fichiers binaires du serveur Crystal Reports C++.	Sous Windows, `<REPINSTALL>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. Sous UNIX, le répertoire sera similaire à : `<REPINSTALL>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.

Espace réservé	Description	Valeurs par défaut
%CRCPP_DefaultWorkingDir%	Répertoire de travail par défaut des serveurs Crystal Reports C++.	Sous Windows, `<REPINSTALL>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. Sous UNIX, le répertoire sera similaire à : `<REPINSTALL>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRYSTALRAS_EXE%	Nom du fichier exécutable du serveur Report Application Server.	Sous Windows, `crystalras.exe`. Sous UNIX, `boe_crystalrasd`.
%CR_ODBCINI%	Nom et chemin du fichier `.odbc.ini`.	Sous UNIX, `<REPINSTALL>/bobje/odbc.ini`. Sous Windows, il s'agit d'une chaîne vide.
%CommonJavaBundlesDir%	Dossier où se trouvent les packages OSGI partagés.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/lib/bundles`.
%CommonJavaLibDir%	Dossier où se trouvent les bibliothèques communes Java.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/lib`.
%DLLEXT%	Extension par défaut d'un fichier `.dll` ou `.so`.	Sous Windows, `.dll`. Sous UNIX, `.so`.
%DLLPATH%	Sur l'ordinateur où est installée la plateforme SAP BusinessObjects de Business Intelligence, nom de la variable d'environnement qui spécifie les répertoires où l'interpréteur recherchera les fichiers exécutables.	Sous Windows, « Path ». Sous UNIX, « LD_LIBRARY_PATH ».
%DLLPATH32%	Sur les systèmes Solaris 32 bits : sur l'ordinateur où est installée la plateforme SAP BusinessObjects de Business Intelligence, nom de la variable d'environnement qui spécifie les répertoires où l'interpréteur recherchera les fichiers exécutables.	Sur les ordinateurs Solaris, « LD_LIBRARY_PATH_32 ». Cet espace réservé est une chaîne vide sur d'autres systèmes d'exploitation.

Espace réservé	Description	Valeurs par défaut
%DLLPATH64%	Sur les systèmes Solaris 64 bits : sur l'ordinateur où est installée la plateforme SAP BusinessObjects de Business Intelligence, nom de la variable d'environnement qui spécifie les répertoires où l'interpréteur recherchera les fichiers exécutables.	Sur les ordinateurs Solaris, « LD_LIBRARY_PATH_64 ». Cet espace réservé est une chaîne vide sur d'autres systèmes d'exploitation.
%DLLPREFIX%	Préfixe par défaut d'un fichier `.dll` or `.so`.	Sous UNIX, « lib ». Cet espace réservé est une chaîne vide sur les ordinateurs Windows.
%DLLPRELOAD%	Nom de la variable d'environnement LD_PRELOAD pour la plateforme.	Sous UNIX *LD_PRELOAD*. Cet espace réservé est une chaîne vide sur les ordinateurs Windows.
%DLLPRELOAD32%	Nom de la variable d'environnement LD_PRELOAD sur les systèmes AIX 32 bits.	Sous AIX, *LDR_PRELOAD*. Cet espace réservé est une chaîne vide sur d'autres ordinateurs.
%DLLPRELOAD64%	Nom de la variable d'environnement LD_PRELOAD sur les systèmes AIX 64 bits.	Sous AIX, *LDR_PRELOAD64*. Cet espace réservé est une chaîne vide sur d'autres ordinateurs.
%DP%	Délimiteur de chemin.	Sous Windows, « ; ». Sous UNIX, « : ».
%DefaultAuditingDir%	Répertoire dans lequel les fichiers temporaires d'audit sont créés. Pour une performance optimale, cet emplacement doit être sur le lecteur local du serveur.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Auditing`. Sous UNIX, `<REPINSTALL>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	Répertoire temporaire utilisé par le Job Server.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Data`. Sous UNIX, `<REPINSTALL>/sap_bobj/data`.
%DefaultInputFRSDir%	Dossier racine du serveur Input File Repository Server.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. Sous UNIX, `<REPINSTALL>/sap_bobj/data/frsinput`.
%DefaultLoggingDir%	Emplacement de stockage des fichiers journaux.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\logging`. Sous UNIX, `<REPINSTALL>/sap_bobj/logging`.

Espace réservé	Description	Valeurs par défaut
%DefaultOutputFRSDir%	Dossier racine du serveur Output File Repository Server.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. Sous UNIX, `<REPINSTALL>/sap_bobj/data/frsoutput`.
%DefaultWorkingDir%	Répertoire de travail des serveurs 64 bits	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>`.
%DefaultWorkingDir32%	Répertoire de travail des serveurs 32 bits	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/<plateforme>`.
%EPM_LD_PRELOAD_ONCE%	Nom de la variable d'environnement LD_PRELOAD_ONCE pour la plateforme.	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	Nom du fichier exécutable du serveur Event Server.	Sous Windows, `EventServer.exe`. Sous UNIX, `boe_eventsd`.
%EXEEXT%	Extension par défaut des fichiers exécutables.	Sous Windows, `.exe`. Cet espace réservé n'est pas disponible sous UNIX.
%EXEPATH%	Sur l'ordinateur où est installée la plateforme SAP BusinessObjects de Business Intelligence, nom de la variable d'environnement qui spécifie les répertoires où l'interpréteur recherchera les fichiers exécutables.	Sous Windows, « Path ». Sous UNIX, « PATH ».
%EnterpriseDir%	L'emplacement où la plateforme SAP BusinessObjects de Business Intelligence 64 bit est installée.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/`.
%EnterpriseDir32%	L'emplacement où la plateforme SAP BusinessObjects de Business Intelligence 32 bits est installée.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/`.

Espace réservé	Description	Valeurs par défaut
%ExternalJavaLibDir%	Dossier où se trouvent les bibliothèques Java tierces.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/lib/external`.
%FILESERVER_EXE%	Nom du fichier exécutable du serveur de fichiers.	Sous Windows, `fileserver.exe`. Sous UNIX, `boe_filesd`.
%HOARD_PATH%	Emplacement du gestionnaire de mémoire.	Par défaut, cette valeur est vide.
%HOARD_PRELOAD%	Indique s'il faut précharger le gestionnaire de mémoire.	Par défaut, cette valeur est vide.
%INSTALLROOTDIR%	Dossier où est installée la plateforme SAP BusinessObjects Business Intelligence 64 bits.	Cette valeur est spécifiée lors de l'installation.
%INSTALLROOTDIR32%	Dossier où est installée la plateforme SAP BusinessObjects Business Intelligence 32 bits.	Cette valeur est spécifiée lors de l'installation.
%IntroscopeAgentEnableInstrumentation%	Indique si l'instrumentation des serveurs Java utilisant Introscope Agent Enterprise Manager est activée.	Les valeurs possibles sont TRUE ou FALSE, selon que Introscope Agent Enterprise Manager a été activé ou non lors de l'installation de la plateforme SAP BusinessObjects de Business Intelligence.
%IntroscopeAgentEnterpriseManagerHost%	Nom d'hôte d'Introscope Agent Enterprise Manager vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
%IntroscopeAgentEnterpriseManagerPort%	Port d'Introscope Agent Enterprise Manager vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
%IntroscopeAgentEnterpriseManagerTransport%	Transport utilisé pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager. Les valeurs possibles sont : • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via HTTP.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via HTTPS.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory

Espace réservé	Description	Valeurs par défaut
%IntroscopeAgentEnterpriseManagerTransportSSL%	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via SSL.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via TCP.	com.wily.isengard.postoffice-hub.link.net.DefaultSocketFactory
%IntroscopeDir%	Dossier où est installé Introscope Agent Enterprise Manager.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/wily`.
%JAVAW_EXE%	Nom du fichier exécutable de la JVM sans fenêtre de console.	Sous Windows, `javaw.exe`. Sous UNIX, `java`.
%JAVA_EXE%	Nom du fichier exécutable de la JVM.	Sous Windows, `java.exe`. Sous UNIX, `java`.
%JOBSERVERCHILD_EXE%	Nom du fichier exécutable du serveur Adaptive Job Server Child.	Sous Windows, `JobServerChild.exe`. Sous UNIX, `boe_jobcd`.
%JOBSERVER_EXE%	Nom du fichier exécutable du serveur Adaptive Job Server.	Sous Windows, `JobServer.exe`. Sous UNIX, `boe_jobsd`.
%JdkBinDir%	Dossier où se trouvent les fichiers binaires JDK.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. Sous UNIX, `<REPINSTALL>/sap_bobj/<PLATEFORME>/sapjvm/bin`.
%JreBinDir%	Dossier où se trouvent les fichiers binaires JRE.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. Sous UNIX, `<REPINSTALL>/sap_bobj/<PLATEFORME>/sapjvm/jre/bin`.
%JVM_ARCH_ENVIRONMENT%	Indique si l'ordinateur est exécuté sur une JVM 32 bits ou 64 bits.	Pour les ordinateurs UNIX 32 bits, la valeur par défaut est « -d32 ». Pour les ordinateurs UNIX 64 bits, la valeur par défaut est « -d64 ». Sous Windows, il s'agit d'une chaîne vide.
%JVM_HEADLESS_MODE%	Argument de la ligne de commande qui spécifie si la JVM travaille en mode headless (sans tête).	Sous Windows, -Djava.awt.headless=false. Sous UNIX, -Djava.awt.headless=true

Espace réservé	Description	Valeurs par défaut
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	Paramètres de la ligne de commande spécifiant les opérations exécutées par la JVM lorsque des erreurs de mémoire insuffisante se produisent.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	Paramètres de la ligne de commande activant les extensions de la JVM et définissant le numéro d'instance de la JVM.	Par défaut, cet espace réservé est vide.
%LANGUAGEPACKSDIR%	Dossier où sont installés les packs linguistiques du déploiement.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Languages`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	Dossier où sont installés les packs linguistiques du déploiement sur des systèmes 32 bits.	. Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\Languages`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/Languages/`.
%LSTDir%	Dossier où sont stockés les fichiers de configuration LST.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/lst`.
%MDAS_JVM_OS_STACK_SIZE%	Spécifie la taille de pile de la JVM pour le service d'analyse multidimensionnelle.	Par défaut, cet espace réservé est vide.
%NCSInstrumentLevelThreshold%	Niveau de seuil de la journalisation d'événements de la bibliothèque NCS.	La valeur par défaut est 0.
%PAGESERVER_EXE%	Nom du fichier exécutable du serveur de traitement Crystal Reports 2020.	Sous Windows, `crproc.exe`. Sous UNIX, `boe_crprocd.bin`.
%PJSContainerDir%	Dossier où se trouvent les fichiers JAR de conteneur de serveur de traitement adaptatif.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/pjs/container`.

Espace réservé	Description	Valeurs par défaut
%PJSServicesDir%	Dossier où se trouvent les fichiers JAR de service de serveur de traitement adaptatif.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/java/pjs/services`.
%Platform%	Système d'exploitation de l'ordinateur sur lequel la plateforme de BI est exécutée.	Système d'exploitation de l'ordinateur sur lequel la plateforme de BI est exécutée.
%Platform32%	Système d'exploitation de l'ordinateur sur lequel la plateforme de BI 32 bits est exécutée.	Système d'exploitation de l'ordinateur sur lequel la plateforme de BI est exécutée.
%RasBinDir%	Dossier racine du serveur Report Application Server.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATFEORME>/ras`.
%SERVER_FRIENDLY_NAME%	Nom complet du serveur.	Nom complet du serveur.
%SERVER_NAME%	Nom complet du serveur.	Nom complet du serveur.
%SMDAgentHost%	Nom d'hôte SMD Agent vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
%SMDAgentPort%	Port SMD Agent vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
%TRACE_CONFIGFILE_INI%	Nom et chemin d'accès au fichier `BO_Trace.ini`.	Sous Windows, `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/conf/BO-trace.ini`.
%WarFilesDir%	L'emplacement des fichiers d'applications Web.	Sous Windows `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`. Sous UNIX, `<REPINSTALL>/sap_bobj/enterprise_xi40/warfiles/webapps`.
%WEBI_LD_PRELOAD%	Nom de la variable d'environnement LD_PRELOAD pour la plateforme.	$LD_PRELOAD$
%WEBISERVER_EXE%	Nom du fichier exécutable du Web Intelligence Processing Server.	Sous Windows, `wireportserver.exe`. Sous UNIX, `WIReportServer`.

Espace réservé	Description	Valeurs par défaut
%WEBI_LD_PRELOAD_ONCE%	Nom de la variable d'environnement LD_PRELOAD_ONCE pour la plate-forme.	$LD_PRELOAD_ONCE$

Informations associées

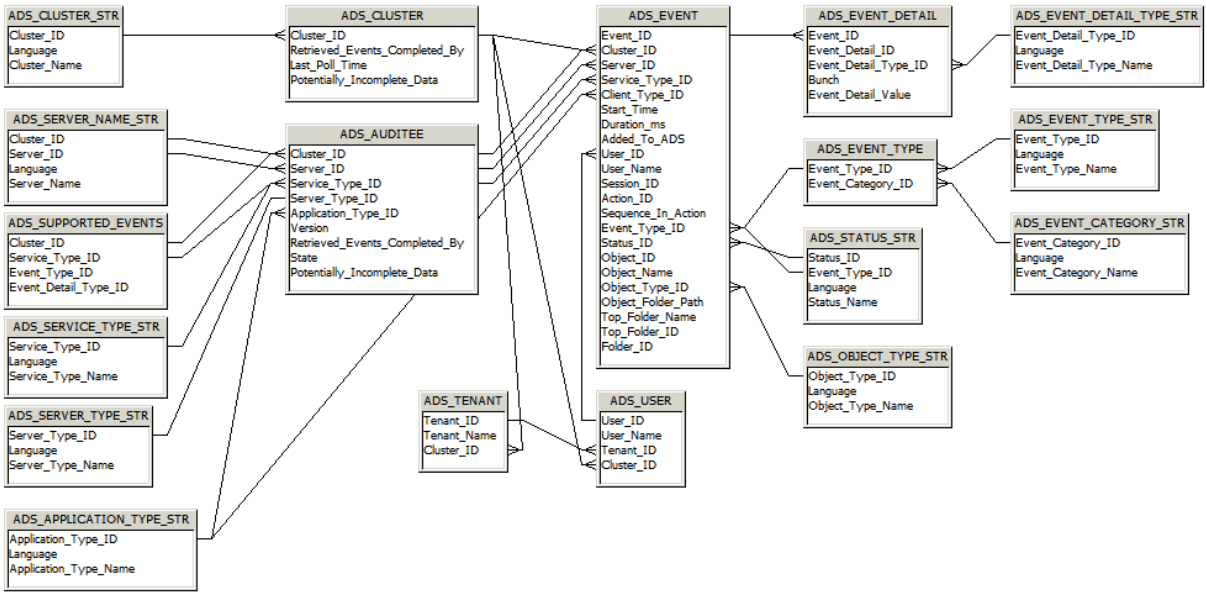
Visualisation et modification des espaces réservés d'un nœud [page 511]

38 Annexe relative au schéma de magasin de données d'audit

38.1 Présentation

Cette annexe constitue une référence pour tous les concepteurs de rapports qui accéderont aux tables du magasin de données d'audit et effectueront un reporting à partir d'elles. Le diagramme suivant et les explications des tables vous indiquent les tables où les données d'audit seront enregistrées et comment ces tables sont associées.

38.2 Diagramme de schéma



38.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example `<EN>`, or `<DE>`.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (long-text)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example <EN>, or <DE>.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example <EN>, or <DE>.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example <EN>, or <DE>.
Object_Type_Name	Character (255)	Name of the object type.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example `<EN>`, or `<DE>`.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example `<EN>`, or `<DE>`.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example `<EN>`, or `<DE>`.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

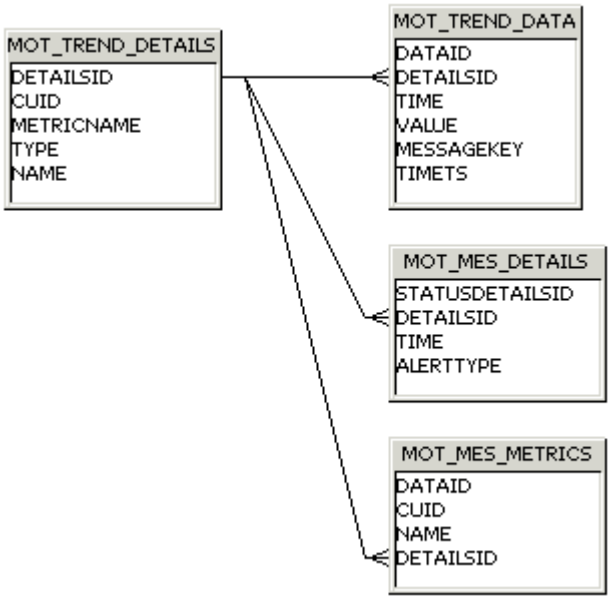
This table records the relationship between users and tenants.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

39 Annexe relative au schéma de la base de données de surveillance

39.1 Schéma de la base de données des tendances

Le diagramme de base de données des tendances suivant et les explications des tables vous indiquent les tables où les données de métriques, tests et veilles seront enregistrées et comment ces tables sont mises en relation.



MOT_TREND_DETAILS

Cette table enregistre des informations relatives aux entités gérées, tests et veilles. Par exemple, les CUID et noms de métriques.

Nom de colonne	Type	Clé	Description
DetailsId	INTEGER	Clé primaire Générée automatiquement	
CUID	VARCHAR(64)	NA	CUID de l'InfoObject qui expose la métrique ou y est associé

Nom de colonne	Type	Clé	Description
MetricName	VARCHAR(255)	NA	Nom de la métrique
Type	VARCHAR(32)	NA	"Subscription", "ManagedEntityStatus" ou "Probe"
Nom	VARCHAR(255)	NA	Nom de la veille quand le type est "ManagedEntityStatus". Sinon, par défaut la même chaîne que dans Type, sauf tout en majuscules, par exemple, "PROBE" ou "SUBSCRIPTION".

MOT_TREND_DATA

Cette table enregistre les données de tendances à partir des métriques, veilles et tests. Par exemple, la valeur de métrique et l'heure.

Nom de colonne	Type	Clé	Description
DataId	INTEGER	Clé primaire Générée automatiquement	
DetailsId	INTEGER	Clé étrangère (de MOT_TREND_DETAILS)	
Time ou TimeT	BIGINT, NUMBER ou FIXED Date Unix Epoch	NA	Heure à laquelle les données ont été recueillies
Valeur	FLOAT, DOUBLE ou NUMBER	NA	Valeur de la métrique ou inscription
MessageKey	VARCHAR(32)	NA	Clé de message d'erreur ou valeur nulle en cas de réussite. Pour la veille, ce peut être "watchEnabled" ou "watchDisabled". Il s'agit d'une "clé" parce qu'elle est utilisée à la fin pour extraire les messages localisés avant leur affichage dans l'interface utilisateur.
Ts	DATETIME ou TIMESTAMP	NA	Heure à laquelle les données sont écrites dans la base de données

MOT_MES_DETAILS

Cette table enregistre les informations relatives aux franchissements d'inscriptions et aux informations de remise d'alerte. Par exemple, l'heure de franchissement et l'heure de remise d'alerte.

Nom de colonne	Type	Clé	Description
StatusDetailsId	INTEGER	Clé primaire Générée automatiquement	
DetailsId	INTEGER	Clé étrangère (de MOT_TREND_DETAILS)	
Heure	BIGINT ou NUMBER Date Unix Epoch	NA	Heure à laquelle les données ont été recueillies
AlerteType	SMALLINT ou NUMBER	NA	Type de remise de notification d'inscription (par exemple, courrier électronique)

MOT_MES_METRICS

Cette table enregistre des informations sur les veilles et les métriques appartenant aux équations des veilles. Chaque métrique appartenant à la veille comportera une entrée dans cette table.

Nom de colonne	Type	Clé	Description
DataId	INTEGER	Clé primaire Générée automatiquement	
DetailsId	INTEGER	Clé étrangère (de MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	NA	CUID de la veille
Nom	VARCHAR(255)	NA	Nom de la veille

40 Annexe relative à la feuille de calcul Copie du système

40.1 Feuille de calcul Copie du système

Propriété	Valeur
Clé de cluster.	
Noms des nœuds.	
Nom d'ordinateur et dossier d'installation de la plateforme de BI pour chaque ordinateur du déploiement.	
Le mot de passe de l'administrateur de la plateforme de BI.	
Connexions de la base de données du CMS, noms d'utilisateur et mots de passe associés à ces connexions pour chaque ordinateur du déploiement.	
Connexions de la base de données d'audit, noms d'utilisateur et mots de passe associés à ces connexions pour chaque ordinateur du déploiement.	
Pour chaque ordinateur du déploiement, détails de toute autre connexion de base de données client pour chaque ordinateur du système source utilisé par les univers et les rapports.	
Pour chaque ordinateur du déploiement, types et versions des clients de bae de données.	
Niveau de version, Support Package et correctif.	
Emplacements de stockage de fichiers de chaque Input FRS et Output FRS du déploiement.	
Si vous prévoyez de copier Gestion des promotions, l'emplacement du dossier de la base de données Gestion des promotions et des dossiers Subversion.	
Si vous prévoyez de copier la base de données de surveillance, le dossier de celle-ci.	
Chemin du dossier de la couche sémantique.	

Clauses de non-responsabilité importantes et informations juridiques

Liens hypertexte

Certains liens affichent une icône et/ou du texte contextuel. Ils fournissent des informations complémentaires.
Explication des icônes :

- Liens accompagnés de l'icône : vous accédez à un site Web non hébergé par SAP. En utilisant de tels liens, vous acceptez (sauf indication contraire expresse dans vos contrats avec SAP) ce qui suit :
  - Le contenu du site vers lequel redirige le lien n'est pas de la documentation SAP. Vous ne pouvez émettre aucune réclamation produit auprès de SAP sur la base de ces informations.
  - SAP n'accepte pas ou désapprouve le contenu affiché sur le site vers lequel vous êtes redirigé, ni ne garantit la disponibilité et l'exactitude dudit contenu. SAP ne saurait être tenue responsable des dommages causés par l'utilisation dudit contenu sauf si de tels dommages étaient causés par une négligence grave ou une faute intentionnelle de SAP.
- Liens accompagnés de l'icône : vous quittez la documentation associée à un produit ou service SAP en particulier et accédez à un site Web hébergé par SAP. En utilisant lesdits liens, vous convenez (sauf indication contraire expresse dans vos contrats avec SAP) que vous ne pourrez pas émettre de réclamation produit auprès de SAP sur la base de ces informations.

Vidéos hébergées sur des plateformes externes

Certaines vidéos peuvent pointer vers des plateformes d'hébergement de vidéos tierces. SAP ne garantit pas la disponibilité future des vidéos stockées sur ces plateformes. Par ailleurs, toute annonce ou tout autre contenu hébergé(e) sur ces plateformes (par exemple, suggestions de vidéos ou navigation vers d'autres vidéos hébergées sur le même site) ne relève ni du contrôle ni de la responsabilité de SAP.

Fonctionnalités Beta et expérimentales

Les fonctionnalités expérimentales ne font pas partie des éléments officiellement fournis par SAP et garantis pour les versions à venir. Cela signifie que les fonctionnalités expérimentales peuvent être modifiées par SAP à tout moment pour quelle que raison que ce soit, sans préavis. Les fonctionnalités expérimentales ne sont pas conçues pour être utilisées en production. Vous ne pouvez pas faire la démonstration, tester, examiner, évaluer ou utiliser d'une quelconque autre manière les fonctionnalités expérimentales dans un environnement productif ou avec des données n'ayant pas été suffisamment sauvegardées.
Le but des fonctionnalités expérimentales est d'obtenir rapidement des avis afin que les clients et partenaires puissent influencer le produit futur. En partageant votre avis (par exemple sur SAP Community), vous acceptez que les droits de propriété intellectuelle des contributions ou œuvres dérivées constituent la propriété exclusive de SAP.

Exemple de code

Les codes et/ou fragments de code ne sont que des exemples. Ils ne sont pas destinés à une utilisation en production. L'exemple de code est utilisé uniquement pour mieux expliquer et visualiser les règles de syntaxe. SAP ne garantit pas l'exactitude ni l'exhaustivité de l'exemple de code. SAP ne saurait être tenue responsable des erreurs ou dommages causés par l'utilisation dudit exemple de code sauf si de tels dommages étaient causés par une négligence grave ou une faute intentionnelle de SAP.

Langage sans préjugés

SAP soutient une culture de diversité et d'inclusion. Chaque fois que cela est possible, nous utilisons un langage impartial dans notre documentation pour faire référence aux personnes de toutes cultures, ethnies, genres et capacités.

www.sap.com/contactsap

© 2024 SAP SE ou société affiliée SAP. Tous droits réservés.

Toute reproduction ou communication de la présente publication, même partielle, par quelque procédé et à quelque fin que ce soit, est interdite sans l'autorisation expresse et préalable de SAP SE ou d'une société affiliée SAP. Les informations du présent document sont susceptibles d'être modifiées sans préavis.

Certains logiciels commercialisés par SAP SE et ses distributeurs contiennent des composants logiciels qui sont la propriété d'éditeurs tiers. Les spécifications des produits peuvent varier d'un pays à l'autre.

Les informations du présent document sont fournies par SAP SE ou par une société affiliée SAP uniquement à titre informatif, sans engagement ni garantie d'aucune sorte. SAP SE ou ses sociétés affiliées ne pourront en aucun cas être tenues responsables des erreurs ou omissions relatives à ces informations. Les seules garanties fournies pour les produits et les services de SAP SE ou d'une société affiliée SAP sont celles énoncées expressément à titre de garantie accompagnant, le cas échéant, lesdits produits et services. Aucune des informations contenues dans le présent document ne saurait constituer une garantie supplémentaire.

SAP et tous les autres produits et services SAP mentionnés dans ce document, ainsi que leurs logos respectifs, sont des marques commerciales ou des marques déposées de SAP SE (ou d'une société affiliée SAP) en Allemagne ainsi que dans d'autres pays. Tous les autres noms de produit et service mentionnés sont des marques commerciales de leurs sociétés respectives.

Veuillez consulter https://www.sap.com/france/about/legal/trademark.html pour plus d'informations sur les marques déposées.

THE BEST RUN SAP