

Plateforme SAP BusinessObjects Business Intelligence  
Version du document : 4.1 Support Package 6 – 2015-06-11

# Guide d'administration de la plateforme de Business Intelligence

# Contenu

<b>1</b>	<b>Historique du document.</b>	<b>19</b>
<b>2</b>	<b>Démarrage.</b>	<b>22</b>
2.1	A propos de ce guide.	22
	Public concerné par ce guide.	22
	A propos de la plateforme de Business Intelligence.	22
	Variables.	23
	Terminologie.	23
2.2	Avant de commencer.	25
	Notions clés.	25
	Outils d'administration clés.	28
	Tâches clés.	30
<b>3</b>	<b>Architecture.</b>	<b>33</b>
3.1	Présentation de l'architecture.	33
	Schéma des composants.	34
	Niveaux d'architecture.	35
	Bases de données.	36
	Serveurs, hôtes et clusters.	37
	Serveurs d'applications Web.	38
	Kits de développement logiciel.	43
	Sources de données.	45
	Authentification et connexion unique.	45
	Intégration SAP.	47
	Contrôle de version intégrée.	48
	Chemin de mise à niveau.	48
3.2	Serveurs, services, nœuds et hôtes.	49
	Modifications des serveurs depuis la version XI 3.1.	51
	Services.	52
	Catégories de service.	58
	Types de serveurs.	61
	Serveurs.	65
3.3	Applications client.	67
	Installées avec les outils client de la plateforme SAP BusinessObjects Business Intelligence.	68
	Installées avec la plateforme SAP BusinessObjects Business Intelligence.	71
	Disponibles séparément.	72
	Clients d'applications Web.	74

3.4	Workflows de traitement. . . . .	78
	Démarrage et authentification. . . . .	78
	Objets de programme. . . . .	80
	Crystal Reports. . . . .	81
	Web Intelligence. . . . .	85
	Analysis. . . . .	87
<b>4</b>	<b>Assistant de configuration du système. . . . .</b>	<b>89</b>
4.1	Introduction à l'Assistant de configuration du système. . . . .	89
4.2	Indication des produits utilisés. . . . .	89
4.3	Sélection d'un modèle de déploiement. . . . .	91
4.4	Indication des emplacements des dossiers de données. . . . .	93
4.5	Révision des modifications. . . . .	94
4.6	Fichiers journaux et fichiers de réponse. . . . .	95
	Utilisation d'un fichier de réponse. . . . .	95
<b>5</b>	<b>Gestion des licences. . . . .</b>	<b>99</b>
5.1	Gestion des clés de licence. . . . .	99
	Pour afficher les informations de licence. . . . .	99
	Pour ajouter une clé de licence. . . . .	99
	Pour visualiser l'activité du compte actuel. . . . .	100
<b>6</b>	<b>Gestion des utilisateurs et des groupes. . . . .</b>	<b>101</b>
6.1	Présentation de la gestion des comptes. . . . .	101
	Gestion des utilisateurs. . . . .	101
	Gestion des groupes. . . . .	102
	Types d'authentification disponibles. . . . .	103
6.2	Gestion des comptes Enterprise et des comptes généraux. . . . .	104
	Pour créer un compte d'utilisateur. . . . .	104
	Pour modifier un compte d'utilisateur. . . . .	105
	Pour supprimer un compte d'utilisateur. . . . .	106
	Pour créer un groupe. . . . .	106
	Pour modifier les propriétés d'un groupe. . . . .	107
	Pour afficher les membres d'un groupe. . . . .	107
	Pour ajouter des sous-groupes. . . . .	107
	Pour définir l'appartenance à un groupe. . . . .	108
	Pour supprimer un groupe. . . . .	108
	Pour ajouter des utilisateurs ou groupes d'utilisateurs en bloc. . . . .	109
	Pour activer le compte Guest. . . . .	110
	Ajout d'utilisateurs à des groupes. . . . .	110
	Modification des paramètres de mot de passe. . . . .	112
	Octroi d'un droit d'accès à des utilisateurs et à des groupes. . . . .	113

	Contrôle de l'accès aux boîtes de réception des utilisateurs. . . . .	114
	Configuration des options de la zone de lancement BI. . . . .	114
	Gestion des attributs des utilisateurs système . . . . .	117
	Classement des attributs utilisateur entre plusieurs options d'authentification. . . . .	119
	Pour ajouter un nouvel attribut utilisateur. . . . .	119
	Pour modifier les attributs utilisateur personnalisés. . . . .	120
6.3	Gestion des alias. . . . .	121
	Pour créer un utilisateur et ajouter un alias tiers. . . . .	121
	Pour créer un alias pour un utilisateur existant. . . . .	122
	Pour affecter un alias d'un autre utilisateur. . . . .	122
	Pour supprimer un alias. . . . .	123
	Pour désactiver un alias. . . . .	123
<b>7</b>	<b>Définition des droits. . . . .</b>	<b>125</b>
7.1	Fonctionnement des droits sur la plateforme de BI. . . . .	125
	Niveaux d'accès. . . . .	125
	Définition de droits avancés. . . . .	126
	Héritage. . . . .	127
	Droits spécifiques au type. . . . .	132
	Détermination des droits effectifs. . . . .	133
7.2	Gestion des paramètres de sécurité des objets dans la CMC. . . . .	134
	Pour visualiser les droits d'un utilisateur ou groupe principal sur un objet. . . . .	134
	Pour affecter des utilisateurs ou groupes principaux à une liste de contrôle d'accès d'un objet . . . . .	135
	Pour modifier les droits d'un utilisateur ou groupe principal sur un objet. . . . .	135
	Définition des droits sur un dossier de niveau supérieur dans la plateforme de BI. . . . .	136
	Vérification des paramètres de sécurité pour un utilisateur ou un groupe principal. . . . .	137
7.3	Utilisation des niveaux d'accès. . . . .	139
	Choisir entre les niveaux d'accès <i>Visualiser</i> et <i>Visualiser à la demande</i> . . . . .	141
	Pour copier un niveau d'accès existant. . . . .	142
	Pour créer un niveau d'accès . . . . .	142
	Pour renommer un niveau d'accès. . . . .	143
	Pour supprimer un niveau d'accès. . . . .	143
	Pour modifier les droits d'un niveau d'accès. . . . .	143
	Suivi de la relation entre niveaux d'accès et objets. . . . .	144
	Gestion des niveaux d'accès sur différents sites. . . . .	145
7.4	Rupture de l'héritage. . . . .	146
	Désactiver l'héritage. . . . .	147
7.5	Utilisation des droits pour déléguer l'administration. . . . .	148
	Choisir entre les options « <i>Modifier les droits des utilisateurs sur les objets</i> ». . . . .	149
	Droits de propriétaire. . . . .	151
7.6	Récapitulatif des recommandations concernant l'administration des droits. . . . .	151



<b>8</b>	<b>Sécurisation de la plateforme de BI . . . . .</b>	<b>152</b>
8.1	Présentation de la sécurité . . . . .	152
8.2	Planification de récupération d'urgence. . . . .	152
8.3	Recommandations générales pour la sécurité de votre déploiement. . . . .	153
8.4	Configuration de la sécurité pour les serveurs tiers fournis. . . . .	154
8.5	Relation de confiance active. . . . .	154
	Jetons de connexion. . . . .	155
	Système de ticket pour la sécurité distribuée. . . . .	155
8.6	Sessions et suivi de session. . . . .	156
	Suivi de session du CMS. . . . .	156
	Gestion des sessions. . . . .	157
8.7	Protection de l'environnement. . . . .	158
	Du navigateur Web au serveur Web. . . . .	158
	Serveur Web vers la plateforme de BI. . . . .	158
8.8	Audit des modifications de la configuration de sécurité . . . . .	159
8.9	Audit de l'activité Web. . . . .	159
	Protection contre les tentatives de connexion malveillantes. . . . .	159
	Restrictions relatives aux mots de passe. . . . .	159
	Restrictions relatives aux connexions. . . . .	160
	Restrictions relatives aux utilisateurs. . . . .	160
	Restrictions relatives au compte Guest. . . . .	161
8.10	Extensions de traitement. . . . .	161
8.11	Présentation de la sécurité des données de la plateforme de BI. . . . .	161
	Modes de sécurité du traitement des données. . . . .	162
8.12	Cryptographie sur la plateforme de BI. . . . .	164
	Utilisation de clés de cluster. . . . .	165
	Agents de cryptographie. . . . .	167
	Gestion des clés de cryptage dans la CMC. . . . .	168
8.13	Configuration des serveurs pour SSL. . . . .	172
	Création de fichiers de clé et de certificat. . . . .	173
	Configuration de SSL lorsque le certificat est géré par une autorité de certification. . . . .	175
	Configuration du protocole SSL. . . . .	177
8.14	Description de la communication entre les composants de la plateforme de BI. . . . .	182
	Présentation des serveurs de la plateforme de BI et des ports de communication. . . . .	182
	Communication entre les composants de la plateforme de BI . . . . .	184
8.15	Configuration de la plateforme de BI pour les pare-feu. . . . .	194
	Pour configurer le système pour des pare-feu. . . . .	194
	Débogage d'un déploiement équipé d'un pare-feu. . . . .	198
8.16	Exemples de scénarios classiques de pare-feu. . . . .	199
	Exemple - Niveau application déployé sur un réseau distinct. . . . .	199
	Exemple : Client lourd et niveau base de données séparés des serveurs de la plateforme de BI par un pare-feu. . . . .	202

8.17	Paramètres de pare-feu pour les environnements intégrés. . . . .	204
	Instructions propres au pare-feu pour l'intégration SAP. . . . .	205
	Configuration du pare-feu pour l'intégration JD Edwards EnterpriseOne. . . . .	206
	Instructions propres au pare-feu pour Oracle EBS. . . . .	208
	Configuration du pare-feu pour l'intégration PeopleSoft Enterprise . . . . .	209
	Configuration du pare-feu pour l'intégration Siebel. . . . .	210
8.18	Plateforme de BI et serveurs proxy inverses . . . . .	211
	Serveurs proxy inverses pris en charge . . . . .	212
	Description du déploiement des applications Web . . . . .	212
8.19	Configuration des serveurs proxy inverses pour les applications Web de la plateforme de Business Intelligence. . . . .	212
	Instructions détaillées relatives à la configuration des serveurs proxy inverses. . . . .	213
	Pour configurer le serveur proxy inverse. . . . .	214
	Pour configurer le serveur proxy inverse Apache 2.2 pour la plateforme de BI . . . . .	214
	Pour configurer le serveur proxy inverse WebSEAL 6.0 pour la plateforme de BI . . . . .	214
	Pour configurer Microsoft ISA 2006 pour la plateforme de BI . . . . .	215
8.20	Configuration spéciale de la plateforme de BI dans les déploiements de serveurs proxy inverses . . . . .	217
	Activation du proxy inverse pour les services Web. . . . .	217
	Activation du chemin racine des cookies de session pour ISA 2006. . . . .	219
	Activation du proxy inverse pour SAP BusinessObjects Live Office. . . . .	222
<b>9</b>	<b>Authentification. . . . .</b>	<b>223</b>
9.1	Options d'authentification dans la plateforme de BI. . . . .	223
	Authentification primaire. . . . .	223
	Plug-ins de sécurité. . . . .	224
	Connexion unique à la plateforme de BI. . . . .	225
9.2	Authentification Enterprise. . . . .	228
	Présentation de l'authentification Enterprise. . . . .	228
	Paramètres d'authentification Enterprise. . . . .	228
	Modification des paramètres d'Enterprise. . . . .	230
	Activation de l'authentification sécurisée. . . . .	231
	Configuration de l'authentification sécurisée pour l'application Web. . . . .	233
9.3	Authentification LDAP. . . . .	242
	Utilisation de l'authentification LDAP. . . . .	242
	Configuration de l'authentification LDAP. . . . .	244
	Mappage des groupes LDAP. . . . .	254
9.4	Authentification Windows AD. . . . .	264
	Utilisation de l'authentification Windows AD. . . . .	264
	Préparation du contrôleur de domaine. . . . .	265
	Configuration de l'authentification AD dans la CMC. . . . .	266
	Configuration du service de la plateforme de BI pour l'exécution du SIA. . . . .	274

	Configuration du serveur d'applications Web pour l'authentification AD. . . . .	277
	Configuration de la connexion unique. . . . .	286
	Dépannage de l'authentification Windows AD. . . . .	301
9.5	Authentification SAP. . . . .	303
	Configuration de l'authentification SAP. . . . .	303
	Création d'un compte utilisateur pour la plateforme de BI. . . . .	304
	Connexion aux systèmes d'autorisation de SAP. . . . .	305
	Définition des options d'authentification SAP. . . . .	307
	Importation de rôles SAP. . . . .	311
	Configuration de la communication réseau sécurisée (SNC). . . . .	315
	Configuration de la connexion unique au système SAP. . . . .	328
	Configuration de la connexion unique pour SAP Crystal Reports et SAP NetWeaver. . . . .	331
9.6	Authentification PeopleSoft. . . . .	332
	Présentation. . . . .	332
	Activation de l'authentification PeopleSoft Enterprise. . . . .	333
	Mappage de rôles PeopleSoft à la plateforme de BI. . . . .	333
	Planification de mises à jour utilisateur. . . . .	336
	Utilisation de la passerelle de sécurité PeopleSoft. . . . .	338
9.7	Authentification JD Edwards. . . . .	348
	Présentation générale. . . . .	348
	Activation de l'authentification JD Edwards EnterpriseOne. . . . .	348
	Mappage de rôles JD Edwards EnterpriseOne à la plateforme de BI. . . . .	349
	Planification de mises à jour utilisateur. . . . .	351
9.8	Authentification Siebel. . . . .	353
	Activation de l'authentification Siebel. . . . .	353
	Mappage de rôles à la plateforme de BI. . . . .	354
	Planification de mises à jour utilisateur. . . . .	357
9.9	Authentification Oracle EBS. . . . .	359
	Activation de l'authentification Oracle EBS. . . . .	359
	Mappage de rôles Oracle E-Business Suite à la plateforme de BI. . . . .	360
	Démappage de rôles . . . . .	364
	Personnalisation des droits pour les groupes et utilisateurs Oracle EBS mappés . . . . .	364
	Configuration de la connexion unique pour SAP Crystal Reports et Oracle EBS. . . . .	365
<b>10</b>	<b>Administration du serveur. . . . .</b>	<b>367</b>
10.1	Utilisation de la zone de gestion Serveurs de la CMC. . . . .	367
10.2	Gestion des serveurs à l'aide de scripts sous Windows . . . . .	370
10.3	Gestion des serveurs sous Unix . . . . .	370
10.4	Affichage et modification du statut d'un serveur. . . . .	370
	Visualisation de l'état des serveurs. . . . .	370
	Démarrage, arrêt et redémarrage d'un serveur. . . . .	372
	Arrêt d'un Central Management Server. . . . .	374

	Activation et désactivation de serveurs. . . . .	375
10.5	Ajout, clonage ou suppression de serveurs. . . . .	376
	Ajout, clonage et suppression de serveurs. . . . .	376
10.6	Mise en cluster de Central Management Servers. . . . .	379
	Mise en cluster de Central Management Servers. . . . .	379
10.7	Gestion des groupes de serveurs. . . . .	384
	Création d'un groupe de serveurs. . . . .	385
	Utilisation des sous-groupes de serveurs. . . . .	386
	Modification de l'appartenance d'un serveur à un groupe. . . . .	387
	Accès en administration à un serveur ou à un groupe de serveurs accordé aux utilisateurs. . . . .	388
10.8	Configuration des serveurs de traitement adaptatif (APS, Adaptive Processing Servers) pour les systèmes de production. . . . .	389
10.9	Évaluation des performances du système. . . . .	390
	Surveillance des serveurs de la plateforme de BI. . . . .	390
	Analyse des performances du serveur. . . . .	390
	Affichage des performances du système. . . . .	391
	Journalisation des activités du serveur. . . . .	391
10.10	Configuration des paramètres des serveurs. . . . .	392
	Pour modifier les propriétés d'un serveur. . . . .	393
	Pour appliquer les paramètres de service à plusieurs serveurs. . . . .	393
	Utilisation des modèles de configuration. . . . .	394
10.11	Configuration des paramètres réseau du serveur. . . . .	396
	Options d'environnement réseau. . . . .	397
	Options d'identification de l'hôte du serveur. . . . .	397
	Configuration d'un ordinateur multi-résident. . . . .	399
	Configuration des numéros de port. . . . .	402
10.12	Gestion des nœuds. . . . .	405
	Utilisation des nœuds. . . . .	405
	Ajout d'un nœud. . . . .	407
	Recréation d'un nœud. . . . .	411
	Suppression d'un nœud. . . . .	415
	Renommer un nœud. . . . .	417
	Déplacement d'un nœud. . . . .	419
	Paramètres de script. . . . .	423
	Ajout des dépendances de serveurs Windows. . . . .	427
	Modification des références de connexion utilisateur pour un nœud. . . . .	428
10.13	Renommage d'un ordinateur dans un déploiement de plateforme de BI. . . . .	429
	Modification du nom des clusters. . . . .	429
	Modification des adresses IP. . . . .	429
	Renommage des ordinateurs. . . . .	431
10.14	Utilisation des bibliothèques tierces 32 bits et 64 bits avec la plateforme de BI. . . . .	434

10.15	Gestion des espaces réservés de nœuds et de serveurs. . . . .	435
	Visualisation des espaces réservés de serveur. . . . .	435
	Visualisation et modification des espaces réservés d'un nœud. . . . .	435
<b>11</b>	<b>Gestion des bases de données du Central Management Server (CMS). . . . .</b>	<b>437</b>
11.1	Gestion des connexions à la base de données système du CMS. . . . .	437
	Sélection de SQL Anywhere comme base de données du CMS. . . . .	437
	Sélection de SAP HANA comme base de données du CMS. . . . .	438
11.2	Sélection d'une base de données CMS (nouvelle ou existante). . . . .	439
	Pour sélectionner une base de données de CMS nouvelle ou existante sous Windows. . . . .	440
	Pour sélectionner une base de données de CMS nouvelle ou existante sous UNIX. . . . .	441
11.3	Recréation de la base de données système du CMS. . . . .	441
	Pour recréer la base de données système du CMS sous Windows. . . . .	442
	Pour recréer la base de données système du CMS sous UNIX. . . . .	443
11.4	Copie de données d'une base de données système d'un CMS dans une autre. . . . .	444
	Préparation de la copie d'une base de données système du CMS. . . . .	444
	Pour copier une base de données système du CMS sous Windows. . . . .	445
	Copie de données d'une base de données système du CMS sous UNIX. . . . .	446
<b>12</b>	<b>Gestion des serveurs conteneurs d'applications Web (WACS). . . . .</b>	<b>447</b>
12.1	WACS. . . . .	447
	Serveur conteneur d'applications Web (WACS). . . . .	447
	Ajout ou suppression de serveurs WACS à votre déploiement. . . . .	450
	Ajout ou suppression de services aux serveurs WACS. . . . .	453
	Configuration HTTPS/SSL. . . . .	455
	Méthodes d'authentification prises en charge. . . . .	458
	Configuration d'AD Kerberos pour un serveur WACS. . . . .	459
	Configuration de la connexion unique Kerberos AD. . . . .	466
	Configuration des services Web RESTful. . . . .	468
	Configuration des serveurs WACS dans votre environnement informatique. . . . .	478
	Configuration des propriétés d'applications Web. . . . .	481
	Dépannage. . . . .	482
	Propriétés des serveurs WACS. . . . .	486
<b>13</b>	<b>Sauvegarde et restauration de votre système. . . . .</b>	<b>487</b>
13.1	Présentation de la sauvegarde et de la restauration. . . . .	487
13.2	Terminologie. . . . .	487
13.3	Cas d'utilisation de la sauvegarde et de la restauration. . . . .	488
13.4	Sauvegardes. . . . .	490
	Sauvegarde du système entier. . . . .	491
	Sauvegarde des paramètres du serveur. . . . .	494
	Sauvegarde du contenu BI. . . . .	497

13.5	Restauration du système. . . . .	497
	Restauration de votre système entier. . . . .	497
	Restauration des paramètres de serveur. . . . .	503
	Restauration du contenu BI. . . . .	506
13.6	Scripts BackupCluster et RestoreCluster. . . . .	506
<b>14</b>	<b>Copie de votre déploiement de la plateforme de BI. . . . .</b>	<b>509</b>
14.1	Présentation de la copie du système. . . . .	509
14.2	Terminologie. . . . .	509
14.3	Cas d'utilisation de la copie du système. . . . .	509
14.4	Planification de la copie du système. . . . .	510
14.5	Remarques et restrictions. . . . .	511
14.6	Procédure de copie de système. . . . .	513
	Pour exporter depuis un système source. . . . .	513
	Pour importer dans un système cible. . . . .	517
<b>15</b>	<b>Gestion des promotions. . . . .</b>	<b>521</b>
15.1	Bienvenue dans la gestion des promotions. . . . .	521
	Présentation. . . . .	521
	Fonctionnalités. . . . .	521
	Droits d'accès à l'application. . . . .	522
	Prise en charge de WinAD dans la gestion des promotions. . . . .	523
	Remplacement des informations dans la plateforme de BI 4.1 SP3 et version ultérieure. . . . .	523
	Remplacement des connexions entre le serveur d'applications et le serveur de messagerie. . . . .	524
15.2	Introduction à l'outil de gestion des promotions. . . . .	524
	Accès à l'outil de gestion de la promotion. . . . .	524
	Composants de l'interface utilisateur. . . . .	525
	Utilisation de l'option Paramètres. . . . .	527
15.3	Utilisation de l'outil de gestion des promotions. . . . .	533
	Création et suppression de dossiers. . . . .	534
	Permet de créer un travail. . . . .	535
	Pour créer un travail en copiant un travail existant. . . . .	537
	Pour rechercher un travail. . . . .	538
	Pour modifier un travail. . . . .	538
	Pour ajouter un InfoObject à un travail. . . . .	539
	Pour gérer les dépendances d'un travail. . . . .	540
	Pour rechercher des objets dépendants. . . . .	541
	Pour promouvoir un travail quand les référentiels sont connectés. . . . .	542
	Promotion d'un travail à l'aide d'un fichier LCMBIAR. . . . .	544
	Pour planifier une promotion de travail. . . . .	546
	Pour afficher l'historique d'un travail. . . . .	548
	Pour reprendre un travail. . . . .	548



15.4	Pour gérer différentes versions d'un InfoObject. . . . .	551
	Droits d'accès à l'application de la gestion des versions. . . . .	551
	Sauvegarde et restauration des fichiers Subversion. . . . .	552
15.5	Promotion du contenu d'un référentiel entier à l'aide de l'outil de gestion des promotions. . . . .	553
	Pour préparer les systèmes source et cible. . . . .	553
	Stratégies de migration. . . . .	555
15.6	Étapes de promotion d'un système entier. . . . .	556
	Pour promouvoir les utilisateurs et les groupes d'utilisateurs (Travail 1). . . . .	557
	Pour promouvoir des objets dépendants (Travail 2). . . . .	557
	Pour promouvoir des objets principaux (Travail 3). . . . .	558
	Post-promotion. . . . .	559
15.7	Utilisation de l'option Ligne de commande. . . . .	559
	Pour exécuter l'outil de ligne de commande sous Windows. . . . .	560
	Pour exécuter l'outil de ligne de commande sous Unix. . . . .	561
	Paramètres d'outil de ligne de commande. . . . .	561
	Exemple de fichier de propriétés. . . . .	567
15.8	Utilisation du CTS (Change and Transport System) amélioré. . . . .	568
	Prérequis. . . . .	568
	Pour configurer la plateforme de BI et l'intégration CTS+. . . . .	569
	Pour promouvoir un travail à l'aide de CTS. . . . .	576
<b>16</b>	<b>Gestion des versions. . . . .</b>	<b>580</b>
16.1	Pour gérer différentes versions de ressources BI. . . . .	580
16.2	Démarrage et arrêt manuels de Subversion sous Unix. . . . .	581
16.3	Fichiers requis pour Subversion sous Solaris 10 et RedHat Linux 5. . . . .	582
16.4	Utilisation de l'option Paramètres du système de gestion des versions. . . . .	582
	Paramètres du système de gestion des versions par défaut. . . . .	583
	Configuration du système de gestion des versions ClearCase dans Windows. . . . .	584
	Configuration du système de gestion des versions ClearCase dans Unix. . . . .	584
16.5	Comparaison de différentes versions du même travail. . . . .	584
16.6	Mise à niveau du contenu de SubVersion. . . . .	585
16.7	Configuration de Subversion pour les Job Server de traitement groupés. . . . .	586
	Option A : configurer l'ordinateur Subversion principal avant de réaliser une opération du système de gestion des versions. . . . .	586
	Option B : configurer Subversion après la création d'un répertoire de copie de travail par le système de gestion des versions. . . . .	586
	Configuration d'autres ordinateurs Subversion. . . . .	587
16.8	Pour accéder à la même vue ClearCase depuis plusieurs serveurs de gestion des versions. . . . .	588
<b>17</b>	<b>Différence visuelle. . . . .</b>	<b>589</b>
17.1	Différence visuelle dans l'outil de gestion des promotions. . . . .	589
	Comparaison d'objets ou de fichiers à l'aide de la différence visuelle. . . . .	590

	Comparaison d'objets ou de fichiers à l'aide du système de gestion des versions. . . . .	591
	Planification de la comparaison. . . . .	592
<b>18</b>	<b>Gestion des applications. . . . .</b>	<b>594</b>
18.1	Gestion des applications via la CMC. . . . .	594
	Présentation. . . . .	594
	Paramètres courants pour les applications. . . . .	595
	Paramètres spécifiques aux applications. . . . .	596
18.2	Gestion des applications via les propriétés du fichier BOE.war. . . . .	636
	Fichier war BOE. . . . .	636
18.3	Personnalisation des points d'entrée de connexion de la zone de lancement BI et OpenDocument . . . . .	645
	Emplacements des fichiers Zone de lancement BI et OpenDocument. . . . .	645
	Pour définir une page de connexion personnalisée. . . . .	646
	Pour ajouter l'authentification sécurisée à la connexion. . . . .	647
18.4	Personnalisation des interfaces utilisateur d'application. . . . .	648
	Web Intelligence. . . . .	648
	Zone de lancement BI. . . . .	662
<b>19</b>	<b>Gestion des connexions et des univers. . . . .</b>	<b>663</b>
19.1	Gestion des connexions. . . . .	663
	Pour supprimer une connexion d'univers. . . . .	663
19.2	Gestion des univers. . . . .	664
	Pour supprimer des univers. . . . .	664
<b>20</b>	<b>Surveillance. . . . .</b>	<b>666</b>
20.1	A propos de la surveillance. . . . .	666
20.2	Terminologie de la surveillance. . . . .	667
	Architecture. . . . .	669
20.3	Configuration de la prise en charge de la base de données pour la surveillance . . . . .	670
	Configuration pour l'utilisation de la base de données Derby. . . . .	671
	Configuration pour utiliser la base de données d'audit. . . . .	671
20.4	Propriétés de configuration. . . . .	678
	URL du point de terminaison JMX. . . . .	682
	Authentification HTTPS pour les métriques de surveillance. . . . .	683
	Cryptage des mots de passe pour les tests. . . . .	683
20.5	Intégration à d'autres applications. . . . .	683
	Intégration de l'application de surveillance à IBM Tivoli. . . . .	683
	Intégration de l'application de surveillance à SAP Solution Manager . . . . .	686
20.6	Prise en charge de cluster pour serveur de surveillance. . . . .	687
20.7	Dépannage. . . . .	687
	Tableau de bord. . . . .	687
	Alertes. . . . .	688

	Liste de veille. . . . .	689
	Tests. . . . .	689
	Métriques. . . . .	690
	Graphique. . . . .	691
<b>21</b>	<b>Audit. . . . .</b>	<b>692</b>
21.1	Présentation. . . . .	692
21.2	Page Audit de la CMC. . . . .	698
	Statut de l'audit. . . . .	698
	Configuration des événements d'audit. . . . .	700
	Paramètres de configuration des magasins de données d'audit. . . . .	703
21.3	Événements d'audit. . . . .	704
	Événements et détails d'audit. . . . .	713
<b>22</b>	<b>Recherche de plateformes. . . . .</b>	<b>733</b>
22.1	Description de la recherche de plateformes. . . . .	733
	SDK de recherche de plateformes. . . . .	733
	Environnement en cluster. . . . .	734
22.2	Installation de la recherche de plateformes. . . . .	734
	Déploiement d'OpenSearch. . . . .	734
	Configuration du proxy inverse. . . . .	736
	Configuration des propriétés de l'application dans la CMC. . . . .	736
22.3	Utilisation de la recherche de plateformes. . . . .	741
	Indexation de contenu dans le référentiel CMS. . . . .	741
	Liste d'échecs d'indexation. . . . .	742
	Recherche des résultats. . . . .	743
22.4	Intégration de la recherche de plateformes à SAP NetWeaver Enterprise Search. . . . .	750
	Création d'un connecteur dans SAP NetWeaver Enterprise Search . . . . .	750
	Importation du rôle d'un utilisateur dans la plateforme de BI. . . . .	751
22.5	Recherche depuis SAP NetWeaver Enterprise Search. . . . .	751
22.6	Audit. . . . .	752
22.7	Dépannage. . . . .	753
	Auto-guérison. . . . .	753
	Scénarios de problèmes. . . . .	753
<b>23</b>	<b>Fédération. . . . .</b>	<b>756</b>
23.1	Fédération. . . . .	756
23.2	Terminologie Fédération. . . . .	757
23.3	Gestion des droits de sécurité. . . . .	759
	Droits requis sur le site d'origine. . . . .	759
	Droits requis sur le site de destination. . . . .	760
	Droits spécifiques à Fédération. . . . .	761

	Réplication de la sécurité sur un objet. . . . .	762
	Réplication de la sécurité à l'aide des niveaux d'accès.. . . .	763
23.4	Options de types et de mode de réplication. . . . .	763
	Réplication unidirectionnelle . . . . .	763
	Réplication bidirectionnelle . . . . .	764
	Actualiser à partir du site d'origine ou Actualiser à partir de la destination. . . . .	764
23.5	Réplication d'utilisateurs et de groupes tiers. . . . .	766
23.6	Réplication des univers et des connexions d'univers. . . . .	767
23.7	Gestion des listes de réplication. . . . .	768
	Création de listes de réplication. . . . .	769
	Modification des listes de réplication. . . . .	771
23.8	Gestion des connexions à distance. . . . .	772
	Création de connexions à distance. . . . .	772
	Modification des connexions à distance. . . . .	774
23.9	Gestion des travaux de réplication. . . . .	775
	Création de travaux de réplication. . . . .	775
	Planification de travaux de réplication. . . . .	777
	Modification des travaux de réplication. . . . .	777
	Visualisation d'un journal après un travail de réplication. . . . .	778
23.10	Gestion du nettoyage des objets. . . . .	779
	Utilisation du nettoyage des objets. . . . .	779
	Limites du nettoyage des objets. . . . .	780
	Fréquence de nettoyage des objets. . . . .	780
23.11	Gestion de la détection et de la résolution des conflits. . . . .	781
	Résolution des conflits de réplication unidirectionnelle. . . . .	781
	Résolution des conflits de réplication bidirectionnelle. . . . .	783
23.12	Utilisation des services Web dans Fédération. . . . .	786
	Variables de session . . . . .	787
	Mise en cache des fichiers . . . . .	787
	Déploiement personnalisé . . . . .	788
23.13	Planification à distance et instances exécutées localement. . . . .	789
	Planification à distance. . . . .	789
	Instances exécutées localement. . . . .	790
	Partage d'instances. . . . .	791
23.14	Importation et promotion de contenu répliqué. . . . .	792
	Importation de contenu répliqué. . . . .	792
	Importation de contenu répliqué et réplication continue . . . . .	793
	Promotion de contenu à partir d'un environnement de test. . . . .	793
	Redirection d'un site de destination. . . . .	794
23.15	Meilleures pratiques. . . . .	794
	Limites de la version actuelle. . . . .	797

	Dépannage des messages d'erreur. . . . .	798
<b>24</b>	<b>Configurations supplémentaires pour les environnements Enterprise Resource Planning. . . . .</b>	<b>803</b>
24.1	Configurations pour l'intégration SAP NetWeaver. . . . .	803
	Intégration avec SAP Business Warehouse (BW). . . . .	803
24.2	Configuration pour l'intégration JD Edwards. . . . .	846
	Configuration de la connexion unique pour SAP Crystal Reports. . . . .	846
	Configuration de SSL (Secure Sockets Layer) pour les intégrations JD Edwards. . . . .	847
24.3	Configuration pour l'intégration PeopleSoft Enterprise. . . . .	848
	Configuration de la connexion unique pour SAP Crystal Reports et PeopleSoft Enterprise. . . . .	848
	Configuration de la communication Secure Sockets Layer. . . . .	849
	Ajustement des performances pour les systèmes PeopleSoft. . . . .	851
24.4	Configuration pour l'intégration Siebel. . . . .	852
	Configuration de Siebel pour l'intégration à la plateforme SAP BI. . . . .	852
	Création de l'élément de menu Crystal Reports. . . . .	853
	Reconnaissance contextuelle. . . . .	855
	Configuration de la connexion unique pour SAP Crystal Reports et Siebel. . . . .	857
	Configuration de la communication Secure Sockets Layer. . . . .	857
<b>25</b>	<b>Gestion et configuration des journaux. . . . .</b>	<b>860</b>
25.1	Journalisation des traces de composant. . . . .	860
25.2	Niveaux du journal de suivi. . . . .	860
25.3	Configuration du suivi pour les serveurs. . . . .	861
	Pour définir le niveau de journalisation dans la CMC. . . . .	862
	Pour définir le niveau de journalisation de plusieurs serveurs dans la CMC. . . . .	862
	Pour configurer le suivi de serveur à l'aide du fichier Bo_trace.ini. . . . .	863
25.4	Configuration du suivi pour les applications Web. . . . .	865
	Pour définir le niveau du journal de suivi des applications Web dans la CMC. . . . .	866
	Configuration des paramètre de suivi de serveur à l'aide du fichier BO_trace.ini. . . . .	866
25.5	Configuration du suivi pour l'outil de gestion de mise à niveau. . . . .	871
	Pour configurer le suivi pour l'outil de gestion de mise à niveau. . . . .	871
25.6	Configuration du traçage pour les applications clientes de la plateforme de BI . . . . .	872
<b>26</b>	<b>Intégration à SAP Solution Manager. . . . .</b>	<b>873</b>
26.1	Présentation de l'intégration. . . . .	873
26.2	Liste de vérification de l'intégration SAP Solution Manager. . . . .	873
26.3	Gestion de l'enregistrement du répertoire du paysage système. . . . .	874
	Enregistrement de la plateforme de BI dans le paysage système. . . . .	874
	Déclenchement de l'enregistrement SLD. . . . .	876
	Connexion de la connectivité SLD. . . . .	876
26.4	Gestion des agents Solution Manager Diagnostics. . . . .	877
	Présentation de Solution Manager Diagnostics (SMD). . . . .	877

	Utilisation des agents SMD. . . . .	877
	Compte utilisateur SMAAdmin. . . . .	878
26.5	Gestion de l'instrumentation des performances. . . . .	878
	Instrumentation de performances pour la plateforme de BI. . . . .	878
	Configuration de l'instrumentation de performances pour la plateforme de BI. . . . .	879
	Instrumentation de performances pour le niveau Web. . . . .	880
	Fichiers journaux d'instrumentation . . . . .	880
26.6	Suivi avec le Passeport SAP. . . . .	881
<b>27</b>	<b>Administration de la ligne de commande. . . . .</b>	<b>882</b>
27.1	Scripts UNIX. . . . .	882
	Utilitaires de script. . . . .	882
	Modèles de scripts. . . . .	888
	Scripts utilisés par la plateforme de BI. . . . .	888
27.2	Scripts Windows. . . . .	890
	ccm.exe. . . . .	890
27.3	Lignes de commande des serveurs. . . . .	893
	Présentation des lignes de commande. . . . .	893
	Options standard communes à tous les serveurs. . . . .	894
	Central Management Server . . . . .	894
	Crystal Reports Processing Server et Crystal Reports Cache Server. . . . .	896
	Serveur de traitement Dashboards et Dashboards Cache Server. . . . .	897
	Job Servers. . . . .	898
	Serveur de traitement adaptatif. . . . .	899
	Report Application Server. . . . .	899
	Web Intelligence Processing Server. . . . .	902
	Input et Output File Repository Servers. . . . .	903
	Event Server. . . . .	904
<b>28</b>	<b>Repository Diagnostic Tool. . . . .</b>	<b>906</b>
28.1	Présentation du Repository Diagnostic Tool. . . . .	906
28.2	Utilisation du Repository Diagnostic Tool (RDT, outil de diagnostic de référentiel). . . . .	906
	Pour utiliser l'outil de diagnostic de référentiel. . . . .	907
	Paramètres de l'outil de diagnostic de référentiel. . . . .	908
28.3	Incohérences entre le CMS et le FRS. . . . .	914
28.4	Incohérences dans les métadonnées du CMS. . . . .	915
<b>29</b>	<b>Annexe relative aux droits. . . . .</b>	<b>919</b>
29.1	A propos de l'annexe relative aux droits. . . . .	919
29.2	Droits généraux. . . . .	919
29.3	Droits sur les types d'objet spécifiques. . . . .	921
	Droits d'accès aux dossiers. . . . .	921



Catégories. . . . .	921
Documents Desktop Intelligence. . . . .	922
Remarques. . . . .	923
Rapports Crystal. . . . .	924
Documents Web Intelligence. . . . .	924
Utilisateurs et groupes. . . . .	926
Niveaux d'accès. . . . .	927
Droits d'univers (.unv). . . . .	928
Droits d'univers (.unx). . . . .	929
Niveaux d'accès aux objets d'univers. . . . .	930
Droits de connexion. . . . .	932
Applications. . . . .	933
<b>30   Annexe relative aux propriétés des serveurs. . . . .</b>	<b>948</b>
30.1 A propos de l'annexe relative aux propriétés des serveurs. . . . .	948
Propriétés courantes du serveur. . . . .	948
Propriétés des services principaux. . . . .	950
Propriétés des services de connectivité. . . . .	962
Propriétés des services Crystal Reports. . . . .	966
Propriétés d'Analysis Services. . . . .	974
Propriétés des services de fédération de données. . . . .	975
Propriétés des services Web Intelligence. . . . .	976
Propriétés de Dashboards Services. . . . .	984
<b>31   Annexe métrique système. . . . .</b>	<b>986</b>
31.1 A propos de l'annexe Métriques du serveur. . . . .	986
Métriques communes du serveur . . . . .	987
Métriques du Central Management Server. . . . .	988
Métrique du serveur de connexion. . . . .	991
Métriques de l'Event Server . . . . .	992
Métriques du File Repository Server. . . . .	992
Métriques du serveur de traitement adaptatif. . . . .	993
Métriques de serveurs conteneurs d'applications Web. . . . .	997
Métriques d'Adaptative Job Server. . . . .	998
Métriques de Crystal Reports Server. . . . .	1000
Métriques de Web Intelligence Server . . . . .	1002
Métriques du serveur Dashboards. . . . .	1004
<b>32   Annexe relative aux espaces réservés de nœuds et de serveurs. . . . .</b>	<b>1006</b>
32.1 Espaces réservés de nœud et de serveur. . . . .	1006
<b>33   Annexe relative au schéma de magasin de données d'audit. . . . .</b>	<b>1015</b>
33.1 Présentation. . . . .	1015

---

33.2	Diagramme de schéma. . . . .	1015
33.3	Tables du magasin de données d'audit. . . . .	1015
<b>34</b>	<b>Annexe relative au schéma de la base de données de surveillance. . . . .</b>	<b>1024</b>
34.1	Schéma de la base de données des tendances. . . . .	1024
<b>35</b>	<b>Annexe relative à la feuille de calcul Copie du système. . . . .</b>	<b>1027</b>
35.1	Feuille de calcul Copie du système. . . . .	1027

# 1 Historique du document

Le tableau suivant fournit une présentation des principales modifications du document.

Table 1 :

Version	Date	Description
Plateforme SAP BusinessObjects BI 4.1	Mai 2013	Première version de ce document.
Plateforme SAP BusinessObjects BI 4.1 Support Package 1	Août 2013	<ul style="list-style-type: none"><li>Le chapitre « Gestion des promotions » a été mis à jour.</li><li>Le chapitre « Gestion des licences » a été mis à jour.</li><li>Autres corrections et mises à jour secondaires.</li></ul>
Plateforme SAP BusinessObjects BI 4.1 Support Package 2	Novembre 2013	<ul style="list-style-type: none"><li>Le chapitre « Gestion des versions » a été mis à jour.<ul style="list-style-type: none"><li>La section « Pour lancer la gestion des versions sous Solaris 10 » a été ajoutée.</li><li>La section « Démarrage et arrêt manuels de Subversion sous Unix » a été ajoutée.</li><li>La section « Paramètres système par défaut de la gestion des versions » a été ajoutée.</li><li>La section « Pour utiliser l'option des paramètres système de gestion des versions » a été mise à jour.</li></ul></li><li>Le chapitre « Gestion de la promotion » a été mis à jour.<ul style="list-style-type: none"><li>La section « Utilisation des paramètres de remplacement du cycle de vie » a été mise à jour.</li><li>La section « Utilisation de l'option de ligne de commande » a été mise à jour.</li><li>La section « Paramètres de l'outil de ligne de commande » a été mise à jour.</li></ul></li><li>Le chapitre « Repository Diagnostic Tool » a été mis à jour.</li><li>La section « Personnalisation de l'interface Web Intelligence » a été mise à jour.</li><li>Autres corrections et mises à jour secondaires.</li></ul>
Plateforme SAP BusinessObjects BI 4.1 Support Package 3	Mars 2014	<ul style="list-style-type: none"><li>Section « Gestion des sessions » ajoutée.</li><li>Section « Personnalisation des interfaces utilisateur d'application » réorganisée et mise à jour.</li><li>Audit Design Studio ajouté.</li><li>Section décrivant la méthode de modification de port de demande du CMS ajoutée.</li><li>Informations ajoutées sur l'utilisation des bases de données Oracle pour la surveillance.</li></ul>
Plateforme SAP BusinessObjects BI 4.1 Support Package 4	Juin 2014	<ul style="list-style-type: none"><li>Zone de lancement BI ajoutée à la section « Gestion des applications ».</li><li>Ajout d'un paramètre de ligne de commande – <code>legacymode</code> pour le File Repository Server.</li></ul>

Version	Date	Description
Plateforme SAP BusinessObjects BI 4.1 Support Package 5	Novembre 2014	<ul style="list-style-type: none"> <li>• Une section SAP Lumira a été ajoutée sous "Architecture &gt; Applications client &gt; Disponibles séparément".</li> <li>• SAP Lumira a été ajouté à la section « Gestion des applications &gt; Gestion des applications via la CMC &gt; Présentation ».</li> <li>• La section "Gestion des paramètres SAP Lumira" a été ajoutée sous "Gestion des applications &gt; Gestion des applications via la CMC &gt; Paramètres spécifiques aux applications".</li> <li>• Section "Interfaces utilisateur de l'application de personnalisation" mise à jour avec la fonctionnalité de personnalisation de dossier.</li> <li>• Les types Analysis Office et Lumira document ont été ajoutés aux sections "Types de contenu" et "Types de contenu pouvant être recherchés".</li> <li>• Une note sur la prise en charge de l'indexation de contenu complète a été ajoutée à la section "Configuration des propriétés de l'application dans la CMC".</li> <li>• Une note a été ajoutée sur la recherche de métadonnées dans la section "Facettes".</li> <li>• La section "Configuration de fichiers SBO" a été mise à jour.</li> <li>• La valeur par défaut a été mise à jour pour l'option <code>-maxobjectsincache</code> dans la section « Central management Server ».</li> <li>• La section "Propriétés des services Web Intelligence" a été mise à jour avec le paramètre de ligne de commande <code>-Dsap.sl.bics.variableComplexSelectionMapping=n</code>.</li> <li>• La section "Paramètres du Repository Diagnostic Tool" a été mise à jour avec le paramètre de ligne de commande <code>-trace</code>.</li> <li>• La valeur maximale pour le champ <i>Supprimer les événements datant de plus de (jours)</i> a été mise à jour dans la section "Configuration des paramètres de base de données du magasin de données d'audit".</li> </ul>

Version	Date	Description
Plateforme SAP BusinessObjects BI 4.1 Support Package 6	Juin 2015	<ul style="list-style-type: none"> <li>• La section "Authentification" a été mise à jour avec le nouveau niveau de sécurité du mot de passe sous "Authentification &gt; Authentification Enterprise &gt; Modification des paramètres d'Enterprise &gt; Pour modifier les paramètres généraux de mot de passe".</li> <li>• Le serveur SFTP a été ajouté à la description du service sous "Architecture &gt; Serveurs, services, nœuds et hôtes &gt; Services &gt; Table 4 &gt; Service de planification de livraison vers la destination".</li> <li>• Le serveur SFTP a été ajouté à la description du service sous "Architecture &gt; Serveurs, services, nœuds et hôtes &gt; Services &gt; Table 4 &gt; Service de publication".</li> <li>• Le serveur SFTP a été ajouté comme application tierce sous "Sécurisation de la plateforme de BI &gt; Description de la communication entre les composants de la plateforme de BI &gt; Communication entre les composants de la plateforme de BI &gt; Ports requis pour la plateforme de BI &gt; Ports requis pour les applications tierces".</li> <li>• "Envoyer vers l'emplacement SFTP" a été ajouté comme droit sous "Annexe relative aux droits &gt; Droits sur les types d'objet spécifiques &gt; Applications &gt; Zone de lancement BI".</li> <li>• "Paramètres par défaut valides pour la destination SFTP" a été ajouté comme métrique sous "Annexe relative aux métriques de serveur &gt; À propos de l'annexe Métriques de serveur &gt; Métriques de l'Adaptive Job Server &gt; Table 240 : Métriques de Job Server".</li> <li>• La description de "Serveur de messagerie" a été mise à jour sous "Sécurisation de la plateforme de BI &gt; Description de la communication entre les composants de la plateforme de BI &gt; Communication entre les composants de la plateforme de BI &gt; Ports requis pour la plateforme de BI &gt; Ports requis pour les applications tierces" avec les étapes pour configurer SMTP sur SSL.</li> <li>• La section "Activation de la connexion unique pour la CMC" a été ajoutée sous "Authentification &gt; Options d'authentification sur la plateforme de BI &gt; Connexion unique sur la plateforme de BI &gt; Prise en charge de la connexion unique".</li> <li>• La section "Mise en cluster de Central Management Servers" a été mise à jour sous "Administration du serveur &gt; Mise en cluster de Central Management Servers".</li> <li>• La section "Restrictions relatives aux mots de passe" a été mise à jour sous "Sécurisation de la plateforme de BI &gt; Audit de l'activité Web".</li> <li>• La section "Espaces de travail BI" a été mise à jour sous "Architecture &gt; Applications clientes &gt; Clients d'applications Web".</li> <li>• "Script de requête : activer la modification (SQL, MDX, etc.)" a été ajouté comme droit sous "Annexe relative aux droits &gt; Droits sur les types d'objet spécifiques &gt; Documents Web Intelligence".</li> </ul>

## 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 :

- planifiez votre premier déploiement ;
- configurez votre premier déploiement ;
- apportez d'importantes modifications à l'architecture d'un déploiement existant ;
- améliorez les performances de votre 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 permet aux utilisateurs finaux d'augmenter leur productivité tout en réduisant les tâches administratives. Qu'elle soit utilisée pour diffuser des rapports de ventes hebdomadaires, fournir aux clients des services personnalisés ou intégrer des informations importantes dans des portails d'entreprise, la plateforme offre des avantages concrets qui dépassent le simple cadre de l'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 : <ul style="list-style-type: none"><li>• aix_rs6000_64</li><li>• linux_x64</li><li>• solaris_sparcv9</li><li>• hpux_ia64</li></ul>
<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 :

Table 2 :

Terme	Définition
produits de modules complémentaires	Produits utilisant la plateforme de BI mais disposant de leur propre programme d'installation, tels que SAP BusinessObjects Explorer.
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
base de données fournie, serveur d'applications Web fourni	Base de données ou serveur d'applications Web accompagnant la plateforme de BI

Terme	Définition
cluster	Au moins deux serveurs CMS (Central Management Servers) travaillant ensemble et utilisant une seule base de données du CMS.
mettre en cluster	Pour créer un cluster.  Par exemple, pour créer un cluster :  <ol style="list-style-type: none"> <li>1. Installez un CMS et une base de données du CMS sur l'ordinateur A.</li> <li>2. Installez un CMS sur l'ordinateur B.</li> <li>3. Dirigez le CMS installé sur l'ordinateur B vers la base de données du CMS installée sur l'ordinateur A.</li> </ol>
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.
l'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, telle que 4.0
migration	Processus de transfert de contenu BI depuis une version principale précédente (par exemple, depuis XI 3.1) à l'aide de l'outil de gestion de mise à niveau.  Ce terme ne concerne pas les déploiements de même version principale. Voir promotion.
version secondaire	Version comportant certains composants, telle que 4.1
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)

Terme	Définition
Correctif	Petite mise à jour concernant une version de Support Package spécifique
promotion	Processus de transfert de contenu BI entre des déploiements de même version principale (par exemple, de 4.0 vers 4.0) 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
Serveurs d'applications Web	Serveur traitant du contenu dynamique. Par exemple, le serveur d'applications Web fourni pour 4.1 est Tomcat 7.
mise à niveau	La planification, la préparation, la migration et le post-traitement nécessaires à la réalisation d'un processus de migration

## 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.

#### **i** 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 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.

## Informations associées

[Serveurs, hôtes et clusters \[page 37\]](#)

### 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.

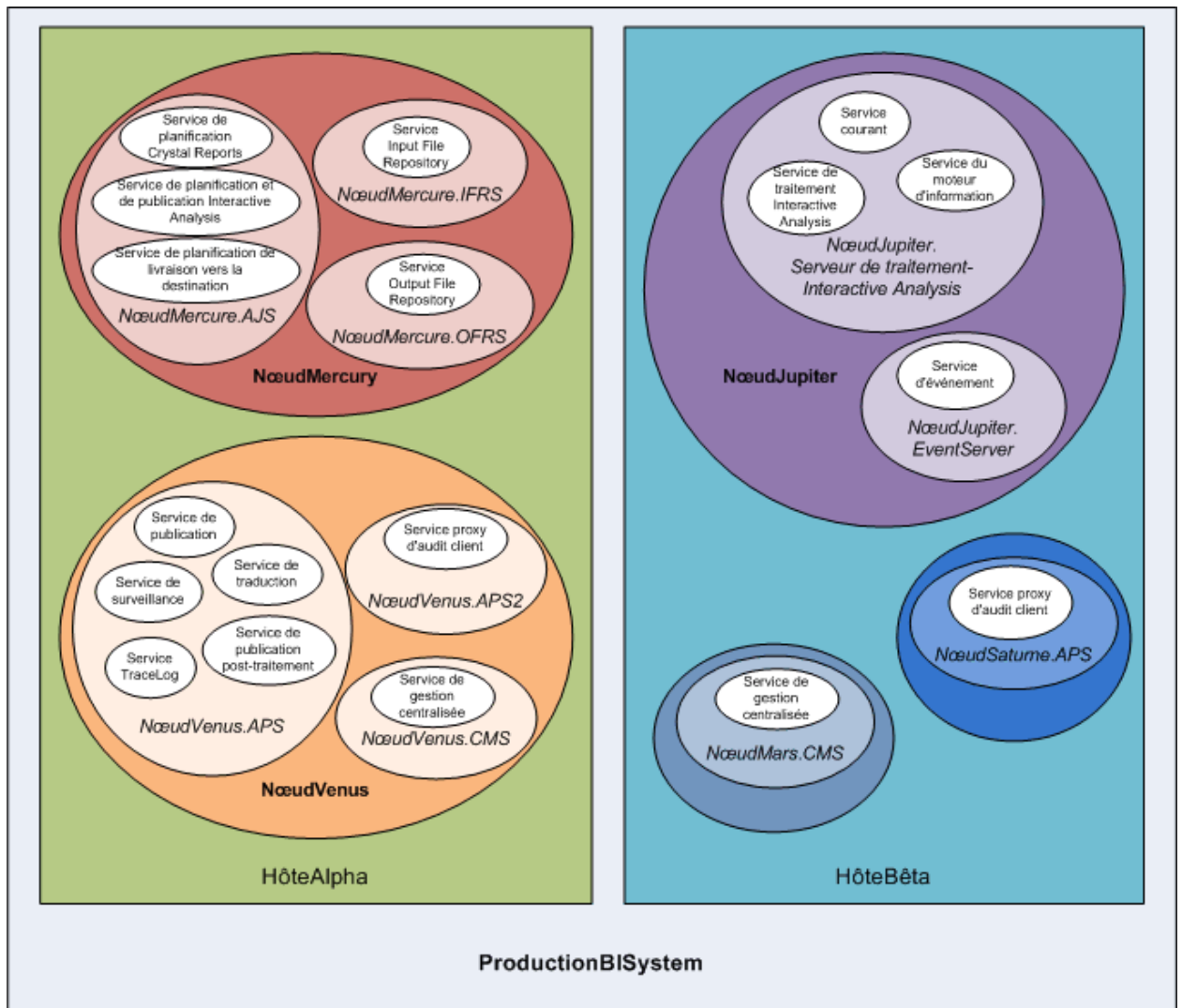
Le terme « serveur » sert à décrire un processus au niveau du système d'exploitation (appelé démon sur certains systèmes) qui héberge un ou plusieurs services. Par exemple, le Central Management Server (CMS) et le serveur de traitement adaptatif sont des serveurs. Un serveur s'exécute sous un compte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

L'outil de gestion de mise à niveau (anciennement une fonction de l'Assistant d'importation) est installé dans le cadre de la plateforme de BI et guide les administrateurs tout au long du processus d'importation des utilisateurs, groupes et dossiers depuis les versions précédentes de la plateforme de BI. Il permet également l'importation et la mise à niveau des événements, groupes de serveurs, objets de référentiel et calendriers.

Pour en savoir plus sur la mise à niveau à partir d'une version antérieure de la plateforme de BI, voir le *Guide de mise à niveau de la plateforme de Business Intelligence*.

## 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 \[page 30\]](#)

[Configuration de votre déploiement \[page 31\]](#)

[Amélioration des performances du système \[page 31\]](#)

[Central Management Console \(CMC\) \[page 28\]](#)

### 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 \[page 33\]](#)

[Communication entre les composants de la plateforme de BI \[page 184\]](#)

[Présentation de la sécurité \[page 152\]](#)

[Options d'authentification dans la plateforme de BI \[page 223\]](#)

[Utilisation de la zone de gestion Serveurs de la CMC \[page 367\]](#)

## 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 \[page 89\]](#)

[Communication entre les composants de la plateforme de BI \[page 184\]](#)

[Présentation de la sécurité \[page 152\]](#)

[A propos de la surveillance \[page 666\]](#)

## 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 \[page 89\]](#)

[A propos de la surveillance \[page 666\]](#)

[Utilisation de la zone de gestion Serveurs de la CMC \[page 367\]](#)

## 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 \[page 101\]](#)


[Fonctionnement des droits sur la plateforme de BI \[page 125\]](#)

## 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 conversion de rapport
  - 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)
  - Widgets (anciennement BI Widgets)
- Clients disponibles séparément :
  - SAP Crystal Reports
  - SAP BusinessObjects Dashboards (anciennement Xcelsius)

- 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 gestion de mise à niveau (ancienne fonction de l'Assistant d'importation)
- 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.

Ce schéma d'architecture, sur le SAP Community Network, 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 : <http://scn.sap.com/docs/DOC-43663>.

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).

### 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 (32 et 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 gestion du cycle de vie**  
La base de données de gestion du cycle de vie trace les informations de configuration et de version relatives à une installation de la plateforme de BI, ainsi que les mises à jour.
- **Base de données de surveillance**  
La surveillance utilise la base de données Java Derby pour stocker les informations de composants et de configuration système relatives aux modalités de prise en charge SAP.

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.

## 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 serveur 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 serveur 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.
- **Équilibrage 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).

### 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.

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 distribuible 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.

```
<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.
5. Stockez ce fichier dans le dossier tomcat/lib pour chaque instance.
6. Redémarrez tous les serveurs.

#### **i** 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

Vous pouvez télécharger l'installation du cluster Websphere sur VCloud. Dans l'installation, le serveur HTTP Websphere est déjà configuré avec l'équilibreur de charge, deux instances du serveur d'applications Websphere et une installation complète de BOE. Vérifiez que tous les ordinateurs exécutent les commandes ping à l'aide de leur IP interne. Le cas échéant, passez à la configuration.

## Configuration de Websphere

Pour configurer Websphere, procédez comme suit :

1. Ajoutez une balise distribuible 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 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, voir <http://help.sap.com>.



---

## 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

#### **i** 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

### i 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 répertoire du paysage système de SAP NetWeaver est la source centrale des informations de paysage 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.

### 3.1.11 Chemin de mise à niveau

Il est possible d'effectuer une mise à niveau à partir d'une version antérieure de SAP BusinessObjects Enterprise (par exemple XI 3.x), mais vous devez d'abord installer la plateforme SAP BusinessObjects Business Intelligence 4.x, puis migrer les paramètres et les données de votre système existant à l'aide de l'outil de gestion de mise à niveau.

Pour en savoir plus sur la mise à niveau à partir d'une version antérieure, voir le *Guide de mise à niveau de la plateforme SAP BusinessObjects Business Intelligence*.

---

## 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.

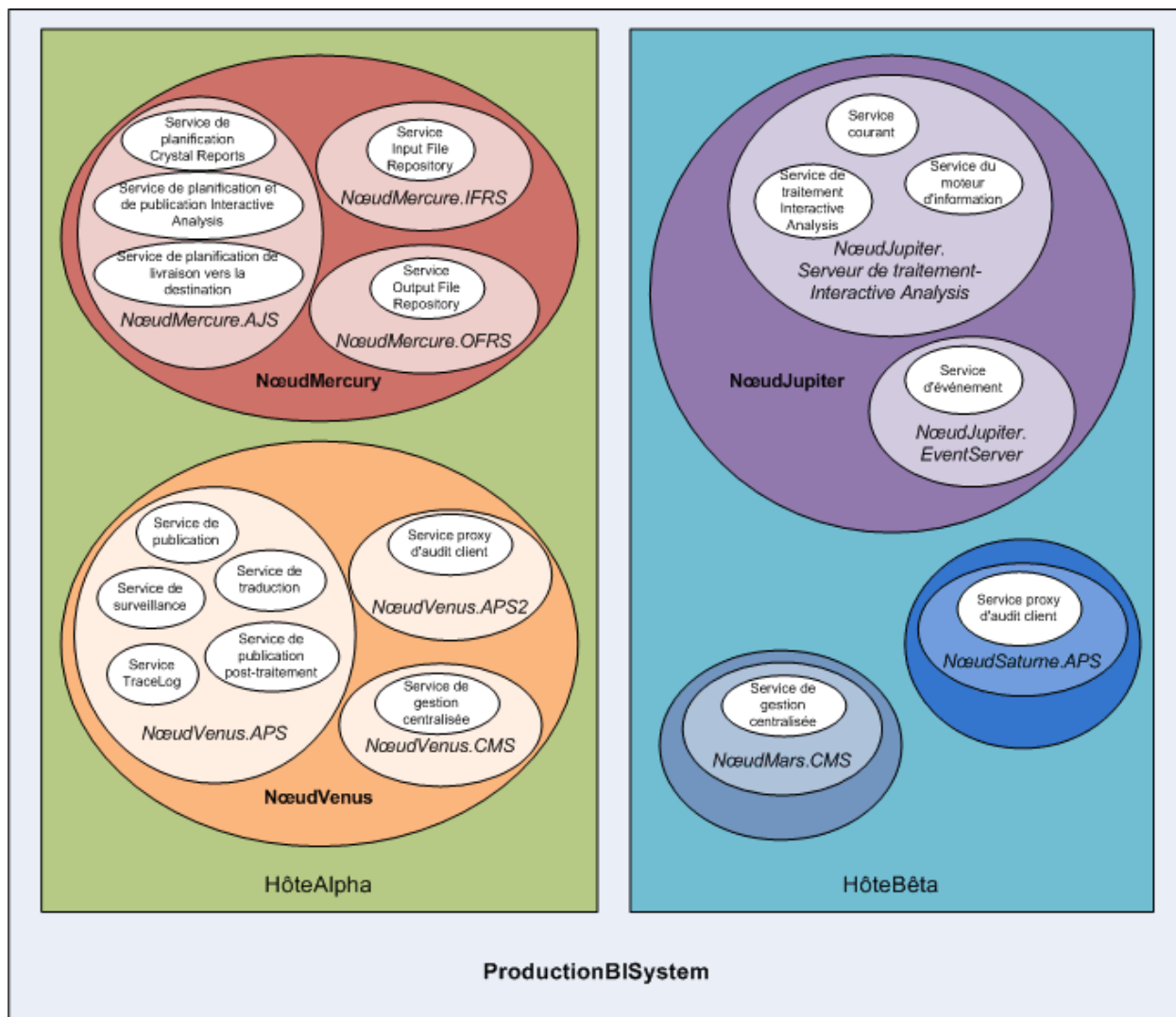
Le terme « serveur » sert à décrire un processus au niveau du système d'exploitation (appelé démon sur certains systèmes) qui héberge un ou plusieurs services. Par exemple, le Central Management Server (CMS) et le serveur de traitement adaptatif sont des serveurs. Un serveur s'exécute sous un compte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

Table 3 : Modifications de serveur

XI 3.1	4.0	4.0 Feature Pack 3	4.1
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
Crystal Reports Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server
Crystal Reports Processing Server	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)
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
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
Desktop Intelligence Cache Server [3]	Non disponible depuis la version 4.0	Non disponible depuis la version 4.0	Non disponible dans la version 4.1 [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]
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]
Destination Job Server	Adaptative Job Server	Adaptative Job Server	Adaptative Job Server

XI 3.1	4.0	4.0 Feature Pack 3	4.1
List of Values Server (LOV)	Web Intelligence Processing Server	Web Intelligence Processing Server	Web Intelligence Processing Server
Serveur Multi-Dimensional Analysis Services	Serveur de traitement adaptatif	Serveur de traitement adaptatif	Serveur de traitement adaptatif
Program 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
Web Intelligence 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 traitement Xcelsius [4]	Serveur de traitement Dashboard Design (Xcelsius) [5]	Serveur de traitement Dashboards (Xcelsius)	Serveur de traitement Dashboards (Xcelsius)

- [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] Le cache Xcelsius et les services de traitement 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.

## 3.2.2 Services

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

### i Remarque

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



Table 4 :

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 de planification de la 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.
Service de l'application Web BOE	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 Open-Document.
Business Process BI Services	Services principaux	Serveur conteneur d'applications Web	Fournit les Business Process BI Web Services pour le WACS, permettant l'incorporation de la technologie BI aux applications Web. Business Process BI Service est obsolète.
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.
Service de traitement Crystal Reports 2013	Services Crystal Reports	Crystal Reports Processing Server	Accepte et traite les rapports Crystal Reports 2013 ; il peut partager des données entre les rapports pour réduire le nombre d'accès à la base de données.
Service de planification Crystal Reports 2013	Services Crystal Reports	Adaptative Job Server	Exécute les travaux Crystal Reports antérieurs planifiés et publie les résultats à un emplacement de sortie.

Service	Catégorie de service	Type de serveur	Description du service
Service de modification et de visualisation Crystal Reports 2013	Services Crystal Reports	Report Application Server (RAS)	Traite les demandes d'affichage et de modification des rapports Crystal Reports 2013.
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 <i>Guide de l'utilisateur SAP BusinessObjects Web Intelligence Rich Client</i> pour en savoir plus sur l'élaboration d'une requête ou l'actualisation d'un document basé sur un fichier texte.
Service de mémoire cache des tableaux de bord	Services Dashboards	Dashboards Cache Server	Limite le nombre d'accès à la base de données générés à partir des contenus Dashboards et accélère le reporting en gérant un cache des rapports
Service de traitement Dashboards	Services Dashboards	Serveur de traitement Dashboards	Accepte et traite les contenus Dashboards ; il peut partager des données entre les rapports pour réduire le nombre d'accès à la base de données

Service	Catégorie de service	Type de serveur	Description du service
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 de planification de livraison vers la destination	Services principaux	Adaptative Job Server	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>Lors de l'ajout de serveurs, vous devez inclure certains services d'Adaptive Job Server, y compris ce service.</p> </div>
Service de récupération de documents	Services Web Intelligence	Serveur de traitement adaptatif	Enregistrement automatique et récupération de documents Web Intelligence
Service DSL Bridge	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 <i>Guide de l'utilisateur SAP BusinessObjects Web Intelligence Rich Client</i> 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 Gestion du cycle de vie	Services de gestion du cycle de vie	Serveur de traitement adaptatif	Fournit une prise en charge ClearCase pour LCM
Service de planification de Gestion du cycle de vie	Services de gestion du cycle de vie	Adaptative Job Server	Exécute les travaux de gestion du cycle de vie planifiés
Service de Gestion du cycle de vie	Services de gestion du cycle de vie	Serveur de traitement adaptatif	Service principal de gestion du cycle de vie
Service de surveillance	Services principaux	Serveur de traitement adaptatif	Fournit les fonctions de surveillance
Service d'analyse multidimensionnelle	Analysis Services	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 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	Catégorie de service	Type de serveur	Description du service
Service de planification de la différence visuelle	Services de gestion du cycle de vie	Adaptative Job Server	Exécute les travaux de requête de différence visuelle (Gestion du cycle de vie) et publie les résultats à un emplacement de sortie
Service de différence visuelle	Services de gestion du cycle de vie	Serveur de traitement adaptatif	Détermine si les documents sont visuellement identiques pour la promotion de documents et la gestion du cycle de vie
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
Services Web SDK et QaaWs	Services principaux	Serveur conteneur d'applications Web	Services Web sur le WACS

### 3.2.3 Catégories de service

#### i Remarque

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

Table 5 :

Catégorie de service	Service	Type de serveur
Analysis Services	Service d'applications Web BEx	Serveur de traitement adaptatif
Analysis Services	Service d'analyse multidimensionnelle	Serveur de traitement adaptatif
Services de connectivité	Adaptive Connectivity Service	Serveur de traitement adaptatif
Services de connectivité	Service de connectivité natif	Serveur de connexion
Services de connectivité	Service de connectivité natif (32 bits)	Serveur de connexion

Catégorie de service	Service	Type de serveur
Services principaux	Service de planification de la mise à jour de l'authentification	Adaptative Job Server
Services principaux	Service de gestion centralisée	Central Management Server
Services principaux	Service proxy d'audit client	Serveur de traitement adaptatif
Services principaux	Service de tableau de bord	Dashboard 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	Serveur de traitement adaptatif
Services principaux	Service de stockage des fichiers d'entrée	Input File Repository Server
Services principaux	Service de surveillance	Serveur de traitement adaptatif
Services principaux	Service de stockage des fichiers de sortie	Output File Repository Server
Services principaux	Service de planification de recherche de plateforme	Adaptative Job Server
Services principaux	Service de recherche de plateformes	Serveur de traitement adaptatif
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	Serveur de traitement adaptatif
Services principaux	Service de réplication	Adaptative Job Server
Services principaux	Service Web RESTful	Serveur conteneur d'applications Web
Services principaux	Service de planification des requêtes de sécurité	Adaptative Job Server
Services principaux	Service de jetons de sécurité	Serveur de traitement adaptatif
Services principaux	Service de connexion unique*	Central Management Server, Serveur de connexion, serveur de traitement Crystal Reports, RAS, serveur de traitement Dashboards et serveur de traitement Web Intelligence
Services principaux	Service de journal de suivi	N'importe quel serveur
Services principaux	Service de traduction	Serveur de traitement adaptatif
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

Catégorie de service	Service	Type de serveur
Services Crystal Reports	Service de traitement Crystal Reports 2013	Crystal Reports Processing Server
Services Crystal Reports	Service de planification Crystal Reports 2013	Adaptative Job Server
Services Crystal Reports	Service de modification et de visualisation Crystal Reports 2013	Report Application Server (RAS)
Services Crystal Reports	Service de mémoire cache Crystal Reports	Crystal Reports Cache Server
Services Crystal Reports	Service de traitement Crystal Reports	Crystal Reports Processing Server
Services Crystal Reports	Service de planification Crystal Reports	Adaptative Job Server
Services Dashboards	Service de mémoire cache des tableaux de bord	Dashboards Cache Server
Services Dashboards	Service de traitement Dashboards	Serveur de traitement Dashboards
Services de fédération de données	Service de fédération de données	Serveur de traitement adaptatif
Services de gestion du cycle de vie	Service ClearCase de la gestion du cycle de vie	Serveur de traitement adaptatif
Services de gestion du cycle de vie	Service de planification de Gestion du cycle de vie	Adaptative Job Server
Services de gestion du cycle de vie	Service de Gestion du cycle de vie	Serveur de traitement adaptatif
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	Serveur de traitement adaptatif
Services Web Intelligence	Service d'accès aux données personnalisé	Serveur de traitement adaptatif
Services Web Intelligence	Service de récupération de documents	Serveur de traitement adaptatif
Services Web Intelligence	Service DSL Bridge	Serveur de traitement adaptatif
Services Web Intelligence	Service d'accès aux données Excel	Serveur de traitement adaptatif
Services Web Intelligence	Service du moteur d'informations	Web Intelligence Processing Server
Services Web Intelligence	Service Rebean	Serveur de traitement adaptatif
Services Web Intelligence	Service de visualisation	Serveur de traitement adaptatif
Services Web Intelligence	Service commun Web Intelligence	Web Intelligence Processing Server
Services Web Intelligence	Service principal Web Intelligence	Web Intelligence Processing Server
Services Web Intelligence	Service de surveillance Web Intelligence*	Serveur de traitement adaptatif
Services Web Intelligence	Service de traitement Web Intelligence	Web Intelligence Processing Server
Services Web Intelligence	Service de planification Web Intelligence	Adaptative Job 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.

### **i** Remarque

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

Table 6 :

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 2013	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 Gestion du cycle de vie	Services de gestion du cycle de vie
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 d'importation d'utilisateurs et groupes*	Services principaux
Adaptative Job Server	Service de planification de la différence visuelle	Services de gestion du cycle de vie
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

Type de serveur	Service	Catégorie de service
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 Gestion du cycle de vie	Services de gestion du cycle de vie
Serveur de traitement adaptatif	Service de Gestion du cycle de vie	Services de gestion du cycle de vie
Serveur de traitement adaptatif	Service de surveillance	Services principaux
Serveur de traitement adaptatif	Service d'analyse multidimensionnelle	Analysis Services
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 traduction	Services principaux
Serveur de traitement adaptatif	Service de différence visuelle	Services de gestion du cycle de vie
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 2013	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
Dashboards Cache Server	Service de mémoire cache des tableaux de bord	Services Dashboards
Serveur de traitement Dashboards	Service de traitement Dashboards	Services Dashboards
Serveur de traitement Dashboards	Service de connexion unique*	Services principaux
Dashboard Server	Service de tableau de bord	Services principaux

Type de serveur	Service	Catégorie de service
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 2013	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

Table 7 :

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 2013	Services Crystal Reports
Adaptative Job Server	Service de planification Crystal Reports	Services Crystal Reports
Adaptative Job Server	Service de planification de livraison vers la destination	Services principaux
Adaptative Job Server	Service de planification de Gestion du cycle de vie	Services de gestion du cycle de vie
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 du cycle de vie
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

Type de serveur	Service	Catégorie de service
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 Gestion du cycle de vie	Services de gestion du cycle de vie
Serveur de traitement adaptatif	Service de Gestion du cycle de vie	Services de gestion du cycle de vie
Serveur de traitement adaptatif	Service de surveillance	Services principaux
Serveur de traitement adaptatif	Service d'analyse multidimensionnelle	Analysis Services
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 traduction	Services principaux
Serveur de traitement adaptatif	Service de différence visuelle	Services de gestion du cycle de vie
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 2013	Services Crystal Reports
Crystal Reports Processing Server	Service de traitement Crystal Reports	Services Crystal Reports
Dashboards Cache Server	Service de mémoire cache des tableaux de bord	Services Dashboards
Serveur de traitement Dashboards	Service de traitement Dashboards	Services Dashboards
Dashboard Server	Service de tableau de bord	Services principaux
Event Server	Service d'événement	Services principaux
Input File Repository Server	Service de stockage des fichiers d'entrée	Services principaux

Type de serveur	Service	Catégorie de service
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 2013	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 de traitement adaptatif	<p>Serveur générique qui héberge les services responsables du traitement des demandes provenant de diverses sources.</p> <p>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.</p> <p>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 <a href="#">Introduction à l'Assistant de configuration du système [page 89]</a> et <a href="#">Configuration des serveurs de traitement adaptatif (APS, Adaptive Processing Servers) pour les systèmes de production [page 389]</a>.</p>
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

Serveur	Description
	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.
Dashboards Cache Server	Intercepte les demandes de rapport envoyées par les clients au Dashboard 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 Dashboard Server, 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.
Serveur de traitement Dashboards	Répond aux demandes de Dashboards 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 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.

Serveur	Description
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).

### 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

L'outil de conversion de rapport convertit les rapports au format Web Intelligence et les publie sur un CMS (Central Management Server).

Les rapports peuvent être extraits des dossiers `Publics`, `Favoris` ou `Boîte de réception` du CMS. Une fois les rapports convertis, vous pouvez les publier dans le même dossier que le rapport Web Intelligence d'origine ou dans un autre dossier. L'outil ne convertit pas tous les rapports et toutes les fonctionnalités de Web Intelligence. Le niveau de conversion dépend des fonctions présentes dans le rapport d'origine. Certaines d'entre elles empêchent la conversion du rapport. D'autres sont modifiées, implémentées de nouveau ou supprimées par l'outil pendant la conversion.

L'outil de conversion de rapport vous permet également de réaliser l'audit de vos rapports convertis. Vous pouvez ainsi identifier les rapports qui ne peuvent pas être totalement convertis par l'outil de conversion de rapport et en expliquer la raison.



### 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 Query as a Web Service

Query as a Web Service est une application de type assistant qui permet d'adresser des requêtes à un service Web et de les intégrer à des applications Web. Les requêtes peuvent être enregistrées pour créer un catalogue de requêtes standard que les composants de génération d'applications peuvent sélectionner en fonction des besoins.

Le contenu Business Intelligence est généralement lié à une interface utilisateur spécifique composée d'outils de Business Intelligence. Avec Query as a Web Service, le contenu BI est livré dans toute interface utilisateur capable de traiter des services Web.

Query as a Web Service est conçu pour être exécuté avec une application Microsoft Windows quelconque, comme tout autre service Web. Query as a Web Service est basé sur les spécifications W3C de service Web SOAP, SDL et XML. Il comprend deux principaux composants :

- **Composant serveur**  
Le composant serveur (intégré à la plateforme de BI) stocke le catalogue Query as a Web Service et héberge les services Web publiés.
- **Outil client**  
C'est l'outil avec lequel les utilisateurs créent et publient leurs requêtes Query as a Web Service. Vous pouvez installer l'outil client sur plusieurs ordinateurs pouvant accéder au même catalogue stocké sur le serveur et partager. L'outil client communique avec les composants serveur via les services Web.

Query as a Web Service permet d'utiliser les requêtes Web dans toute une gamme de solutions côté client, y compris :

- Microsoft Office, Excel et InfoPath
- Plateforme technologique SAP NetWeaver
- OpenOffice
- Applications de gestion de processus et de règles de gestion
- Plateformes Enterprise Service Bus

### 3.3.1.6 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.

### 3.3.1.7 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.

### 3.3.1.8 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.

### 3.3.1.9 Indicateurs de la plateforme de BI

Les indicateurs sont des mini-applications permettant d'accéder rapidement et facilement aux fonctions souvent utilisées et fournissant des informations visuelles à partir de votre bureau. Les indicateurs de la plateforme de BI (anciennement BI Widgets) permettent à votre entreprise d'offrir un accès au contenu Business Intelligence (BI) existant de la plateforme de BI, ou vous pouvez ajouter des applications Web Dynpro enregistrées sous forme d'indicateurs XBCML (Extensible Business Client Markup Language) sur les composants de SAP NetWeaver Application Server en tant qu'indicateurs de bureau.

Pour afficher des indicateurs XBCML sur le bureau de l'utilisateur, on utilise le client SAP Web Dynpro Flex. Le client SAP Web Dynpro Flex est un moteur d'affichage basé sur Adobe Flex, qui est utilisé pour afficher des indicateurs. Pour en savoir plus sur la configuration des applications Web Dynpro, voir la rubrique *Pour activer les indicateurs sur les composants du serveur d'applications SAP NetWeaver* du *Guide de l'utilisateur d'indicateurs pour SAP BusinessObjects*.

#### Remarque

La prise en charge des indicateurs XBCML par le client SAP Web Dynpro Flex commence avec la version 7.0 EhP2 SP3. La prise en charge d'attente du client Flex est réservée aux problèmes du client Flex rencontrés dans les indicateurs XBCML dans ces versions spécifiées.

Grâce aux indicateurs, vous recherchez ou parcourez le contenu existant, comme les documents Web Intelligence, les modèles Dashboards et les applications Web Dynpro, puis collez les informations sur votre bureau afin qu'elles soient accessibles en cas de besoin.

En tant qu'indicateur, le contenu bénéficie des fonctionnalités suivantes du cadre d'application des indicateurs :

- Taille et positionnement contrôlés par l'utilisateur
- Actualisation automatique
- Paramètre facultatif, tel que la fenêtre d'application supérieure
- Sécurité totale de la plateforme de BI (parties de rapport Web Intelligence et modèles Dashboards uniquement)
- Affichage enregistré
- Etat de contexte des données enregistrées (parties de rapport Web Intelligence uniquement)
- Liens OpenDocument Web Intelligence vers des rapports détaillés (documents Web Intelligence uniquement)
- Vues avec onglets (modèles Dashboards uniquement)

## 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.

#### **i** 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**

L'outil de gestion de mise à niveau (anciennement une fonction de l'Assistant d'importation) est installé dans le cadre de la plateforme de BI et guide les administrateurs tout au long du processus d'importation des utilisateurs, groupes et dossiers depuis les versions précédentes de la plateforme de BI. Il permet également l'importation et la mise à niveau des événements, groupes de serveurs, objets de référentiel et calendriers.

Pour en savoir plus sur la mise à niveau à partir d'une version antérieure de la plateforme de BI, voir le *Guide de mise à niveau de la plateforme de Business Intelligence*.

### **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 BusinessObjects Dashboards

SAP BusinessObjects Dashboards (anciennement Xcelsius) désigne un outil conçu pour visualiser les données et créer des tableaux de bord dynamiques et interactifs. Les données et les formules sont importées ou directement saisies dans une feuille de calcul Excel incorporée. Une interface flash fournit une zone de dessin permettant d'afficher différents tableaux de bord et analyses.

Les données peuvent être mises à jour dynamiquement depuis la plateforme de BI et exportées vers différents formats qui peuvent être affichés par les utilisateurs de données dans des formats standard tels que PowerPoint, PDF ou Flash.

### 3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer est une application de détection des données qui utilise une puissante fonctionnalité de recherche afin d'extraire des réponses aux questions professionnelles à partir de données, d'une façon directe et rapide.

Lorsque vous installez SAP BusinessObjects Explorer, les serveurs suivants sont ajoutés au CCM (Central Configuration Manager) et à la CMC (Central Management Console) de la plateforme de BI :

- Serveur de base Explorer : gère tous les serveurs Explorer.
- Serveur d'indexation Explorer : assure et gère l'indexation des données et des métadonnées de l'espace d'informations.

- Serveur de recherche Explorer : traite les requêtes de recherche et renvoie les résultats.
- Serveur d'exploration Explorer : assure et gère les fonctionnalités d'exploration et d'analyse de l'espace d'informations, notamment la recherche sur les données, le filtrage et l'agrégation.

### 3.3.3.5 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. Les utilisateurs de SAP Lumira Desktop peuvent publier des documents Lumira (.lums) sur le CMS à l'aide de l'option [Publier vers SAP BI](#) de l'onglet [Partager](#). Ces documents Lumira sont accessibles dans la zone de lancement BI. Néanmoins, pour visualiser ces documents Lumira, vous devez avoir installé SAP Lumira Desktop. Reportez-vous au dernier guide des nouveautés de SAP Lumira pour savoir quelle version de SAP Lumira Desktop prend en charge l'intégration de SAP Lumira avec la fonctionnalité de la plateforme de BI.

#### 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

La zone de lancement BI (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 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 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 (précédemment connus sous le nom Dashboard Builder) 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

#### **i** Remarque

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

#### **i** Remarque

Les espaces de travail BI font partie intégrante de l'application de zone de lancement BI. Dès lors, pour utiliser les fonctionnalités des espaces de travail BI, vous devez acheter une licence de plateforme SAP BusinessObjects Business Intelligence dont le contrat inclut la zone de lancement BI.

### **3.3.4.4 Visualiseurs de rapports**

Chaque visualiseur de rapports prend en charge une plateforme et un navigateur différents. Les préférences peuvent être définies dans la zone de lancement BI et la CMC (Central Management Console). Il existe deux catégories de visualiseurs :

- Visualiseurs de rapports zéro client (visualiseur DHTML)  
Les visualiseurs de rapports zéro client résident sur le serveur d'applications Web. Lorsqu'un utilisateur demande un rapport, le serveur d'applications Web récupère les pages du rapport sur la plateforme de BI et crée des pages DHTML qui s'affichent dans le navigateur Web. Pour choisir le visualiseur de rapports zéro client (DHTML), sélectionnez ► [Préférences](#) ► [Crystal Reports](#) ► [Web \(aucun téléchargement requis\)](#) ►.
- Visualiseurs de rapports côté client (visualiseur Active X, visualiseur Java)  
Les visualiseurs de rapports côté client sont téléchargés et installés dans le navigateur de l'utilisateur. Lorsqu'un utilisateur demande un rapport, le serveur d'applications traite la requête, puis récupère les pages de rapport sur la plateforme de BI. Le serveur d'applications Web transmet ensuite les pages du rapport au visualiseur côté client qui les traite et les affiche dans le navigateur Web. Pour choisir un visualiseur de rapports côté client, sélectionnez ► [Préférences](#) ► [Crystal Reports](#) ► [Web ActiveX \(ActiveX requis\)](#) ► ou [Web Java \(Java requis\)](#).

Tous les visualiseurs de rapports traitent les requêtes de rapport et présentent les pages du rapport qui s'affichent dans le navigateur Web.

#### **i** Remarque

Pour accéder en ligne aux rapports Crystal par le biais de la CMC (Central Management Console), il est recommandé d'utiliser le visualiseur Web DHTML par défaut. Evitez d'utiliser le visualiseur Java hérité, il ne fournit pas les mêmes fonctionnalités que le visualiseur DHTML.

Pour en savoir plus sur les fonctionnalités spécifiques ou les plateformes prises en charge par chaque visualiseur de rapport, voir le *Guide de l'utilisateur de la zone de lancement BI*, le *Report Application Server .NET SDK Developer Guide* ou le *Guide du développeur pour Viewers Java SDK*.

### **3.3.4.5 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.

### 3.3.4.6 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.

### 3.3.4.7 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.

#### **i** 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.

#### **i** 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.

#### **i** 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.

**i 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 2013 et SAP Crystal Reports pour Enterprise.

**i 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 2013 non mise en cache

Ce workflow décrit le processus d'un utilisateur demandant une page d'un rapport SAP Crystal Reports 2013 (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 2013 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 2013.
8. Le serveur de traitement Crystal Reports 2013 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 2013.

#### 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 2013 ouvre l'instance de rapport et vérifie si le rapport contient des données.  
Le serveur de traitement Crystal Reports 2013 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 2013 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 2013 à la demande

Ce workflow décrit le processus d'un utilisateur demandant une page de rapport SAP Crystal Reports 2013 à la demande pour voir les dernières données, par exemple depuis le visualiseur de rapport de la zone de lancement BI.

#### **i** Remarque

Ce workflow requiert que le CMS, le Crystal Reports Cache Server, le serveur de traitement Crystal Reports 2013 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 2013 pour générer la page.
7. Le serveur de traitement Crystal Reports 2013 demande l'objet rapport à l'Input File Repository Server (FRS). L'Input FRS transmet une copie de l'objet au serveur de traitement Crystal Reports 2013.

#### **i** 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 2013 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 2013 se connecte donc à la source de données pour récupérer les données et générer le rapport.
9. Le serveur de traitement Crystal Reports 2013 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 2013 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 2013 s'exécute

Ce workflow décrit le processus d'un rapport SAP Crystal Reports 2013 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. A l'heure du travail planifié, le CMS recherche un service de planification Crystal Reports 2013 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 2013.
3. Le service de planification Crystal Reports 2013 communique avec l'Input File Repository Server (FRS) pour obtenir un exemple de rapport conforme à l'ID du rapport demandé.

#### Remarque

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

4. Le service de planification Crystal Reports 2013 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 2013.
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 2013 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 2013, il peut être exporté dans un autre format, par exemple PDF (Portable Document Format). `crxpdf.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.

#### **i 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 2013 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.

#### **i 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 Adaptive 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.

**i 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.

**i 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.

**i 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.

## 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

démarrant 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.

### **i** 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](#).

### **i** 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.

### **i** 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.

### **i** 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.

### **i** 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.

### **i** 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.

### **i** 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 relancez 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 ?.

#### i 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 \[page 95\]](#)

## 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 \[page 95\]](#)

### 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.

### **i** Remarque

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

### **i** Remarque

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

### **i** 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 \[page 99\]](#)

[Pour ajouter une clé de licence \[page 99\]](#)

[Pour visualiser l'activité du compte actuel \[page 100\]](#)

#### 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 \[page 99\]](#)

[Pour visualiser l'activité du compte actuel \[page 100\]](#)

#### 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.

### **i** 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.

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 \[page 99\]](#)

[Pour visualiser l'activité du compte actuel \[page 100\]](#)

### **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 \[page 99\]](#)

[Pour afficher les informations de licence \[page 99\]](#)



## 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 ».

Table 8 : Comptes d'utilisateur par défaut

Nom du compte	Description
<i>Administrateur</i>	Cet utilisateur appartient aux groupes <i>Administrateurs</i> et <i>Tout le monde</i> . 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).
<i>Guest</i>	Cet utilisateur appartient au groupe <i>Tout le monde</i> . 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.
<i>SMAAdmin</i>	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.

Table 9 : Comptes de groupe par défaut

Nom du compte	Description
<i>Administrateurs</i>	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 <i>Administrateurs</i> contient uniquement l'utilisateur Administrator.
<i>Tout le monde</i>	Chaque utilisateur appartient au groupe <i>Tout le monde</i> .
<i>Concepteur de groupe QaaWS</i>	Les membres de ce groupe ont accès à Query as a Web Service.
<i>Utilisateurs de l'outil de conversion de rapports</i>	Les membres de ce groupe ont accès à l'application Outil de conversion de rapports.
<i>Traducteurs</i>	Les membres de ce groupe ont accès à l'application Gestionnaire de traduction.
<i>Utilisateurs de Universe Designer</i>	Les utilisateurs qui appartiennent à ce groupe disposent des droits d'accès aux dossiers <i>Universe Designer</i> et <i>Connexions</i> . 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 \[page 125\]](#)

[Octroi d'un droit d'accès à des utilisateurs et à des groupes \[page 113\]](#)

## 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.

Table 10 : 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. Définissez les informations concernant le mot de passe et les paramètres
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.
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.

### i 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](#).

### i 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 \[page 122\]](#)

### 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 apparaît.

4. Cliquez sur [OK](#).  
Le compte d'utilisateur est supprimé.

## Informations associées

[Pour modifier un compte d'utilisateur \[page 105\]](#)

[Pour désactiver un alias \[page 123\]](#)

### 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 \[page 108\]](#)

### 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 \[page 108\]](#)

## 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* ►.

### i 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**+**cl** ou **CTRL**+**cl** 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 affiche 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**+**cl** ou **CTRL**+**cl** 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 modifier le mot de passe](#)
5. Cliquez sur [Enregistrer & Fermer](#).

### 6.2.13.2 Pour modifier les paramètres généraux de mot de passe

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.

Table 11 : Paramètres de mot de passe

Paramètre de mot de passe	Valeur minimale	Valeur maximale recommandée
<i>Doit comprendre N caractères au minimum</i>	0 caractère	64 caractères
<i>Doit changer de mot de passe tous les N jours</i>	1 jour	100 jours
<i>Les N derniers mots de passe ne peuvent être réutilisés</i>	1 mot de passe	100 mots de passe
<i>Le mot de passe peut être modifié après N minute(s)</i>	0 minute	100 minutes
<i>Désactiver le compte après N échecs de connexion</i>	1 échec	100 échecs
<i>Réinitialiser le nombre d'échecs de connexion après N minute(s)</i>	1 minute	100 minutes
<i>Réactiver le compte après N minute(s)</i>	0 minute	100 minutes

4. Cliquez sur [Mettre à jour](#).

Les comptes utilisateur inactifs ne seront pas désactivés automatiquement.

## 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 135]

---

## 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 \[page 134\]](#)

## 6.2.16 Configuration des options de la zone de lancement BI

Dans la CMC, les administrateurs peuvent configurer les préférences de la zone de lancement BI pour des groupes d'utilisateurs. En configurant les propriétés dans le fichier `BOE.war`, vous pouvez spécifier quelles informations s'affichent dans l'écran de connexion de la zone de lancement BI d'un utilisateur.

### Remarque

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

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

Par défaut, l'écran de connexion à la zone de lancement BI 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 pour le fichier `BOE.war`.

#### 6.2.16.1.1 Pour configurer l'écran de connexion à la zone de lancement BI

Pour modifier les paramètres par défaut de la zone de lancement BI, vous devez définir des propriétés de la zone de lancement BI 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 :

**BIlaunchpad.properties**

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

```
authentication.visible=true
```

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

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

Remplacez <authentication> par l'une des options suivantes :

Type d'authentification	valeur d'<authentication>
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, 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 pour les groupes d'utilisateurs dans la CMC

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

Les administrateurs peuvent spécifier des valeurs par défaut pour les préférences suivantes de la zone de lancement BI dans la CMC :

- Onglet [Accueil](#)
- Emplacement de stockage des documents
- Dossiers

- Catégories
- Nombre d'objets par page
- Colonnes affichées dans l'onglet [Document](#)
- Si affichage des documents dans la zone de lancement BI dans un onglet ou dans une nouvelle fenêtre

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 de BI affiche les préférences configurées pour un seul groupe.

Les utilisateurs peuvent configurer leurs propres préférences de la zone de lancement de BI, et les valeurs de leurs préférences ont la priorité sur les valeurs par défaut. (Les utilisateurs peuvent revenir aux préférences par défaut à tout moment.) Toutefois, si l'administrateur modifie les préférences par défaut de la zone de lancement BI 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 de BI pour un groupe d'utilisateurs

Les préférences de la zone de lancement de BI configurées dans la CMC sont les préférences par défaut pour tous les utilisateurs d'un groupe d'utilisateurs.

#### **i** Remarque

Si un utilisateur appartient à deux ou plusieurs groupes d'utilisateurs, la zone de lancement de BI affiche les préférences par défaut configurées pour un seul groupe.

Les utilisateurs peuvent définir leurs propres préférences de la zone de lancement de BI, s'ils disposent des droits appropriés. Si vous ne souhaitez pas que les utilisateurs puissent modifier les préférences, ne leur accordez pas le droit de les définir.

1. Accédez à la zone de gestion [Utilisateurs et groupes](#) de la CMC.
2. Sous [Liste des groupes](#), sélectionnez le groupe d'utilisateurs pour lesquels définir les préférences de la zone de lancement de BI.
3. Sélectionnez ► [Actions](#) ► [Préférences de la zone de lancement BI](#) ►  
La boîte de dialogue [Préférences de la zone de lancement BI](#) s'affiche.
4. Décochez la case [Aucune préférence définie](#).
5. Sélectionnez l'onglet [Accueil](#) ou [Documents](#) pour choisir la page de démarrage par défaut de la zone de lancement de BI.
6. Si vous avez sélectionné l'onglet [Accueil](#), effectuez l'une des actions suivantes pour choisir la page d'accueil dans l'onglet :
  - Pour afficher l'onglet [Accueil](#) par défaut, sélectionnez [Onglet Accueil par défaut](#).
  - Pour afficher un site web spécifique en tant qu'onglet [Accueil](#), cliquez sur [Sélectionnez l'onglet Accueil](#), cliquez sur [Parcourir l'onglet Accueil](#), choisissez un objet dans le référentiel de BI, puis cliquez sur [Ouvrir](#).
7. Si vous avez sélectionné l'onglet [Documents](#), effectuez l'une des actions suivantes :
  - Sélectionnez [Mes Documents](#) pour afficher votre tiroir de documents, puis sélectionnez le noeud par défaut à afficher :
    - [Mes favoris](#)



- [Catégories personnelles](#)
  - [Ma boîte de réception](#)
  - Sélectionnez [Dossiers](#) pour afficher votre tiroir de dossiers, puis sélectionnez le dossier par défaut à afficher :
    - Pour choisir tous les dossiers publics, sélectionnez [Dossiers publics](#).
    - Pour choisir un dossier en particulier, sélectionnez [Sélection du dossier public](#), cliquez sur [Rechercher un dossier](#), sélectionnez-le et cliquez sur [Ouvrir](#).
  - Sélectionnez [Catégories](#) pour afficher votre tiroir de catégories, puis sélectionnez la catégorie par défaut à afficher :
    - Pour choisir toutes les catégories publiques, sélectionnez [Catégories d'entreprise](#).
    - Pour choisir un dossier en particulier, sélectionnez [Sélection d'une catégorie d'entreprise](#), cliquez sur [Rechercher une catégorie](#), sélectionnez-la et cliquez sur [Ouvrir](#).
8. Sous [Sélectionner les colonnes affichées dans l'onglet Documents](#), cochez la case pour chaque colonne à afficher pour chaque objet du panneau [Liste](#) :
- [Type](#)
  - [Dernière exécution](#)
  - [Instances](#)
  - [Description](#)
  - [Créé par](#)
  - [Création le](#)
  - [Emplacement \(catégories\)](#)
  - [Reçu le \(boîte de réception\)](#)
  - [De \(boîte de réception\)](#)
9. Sous [Définissez l'emplacement de visualisation de document](#), choisissez la façon dont vous voulez que les utilisateurs visualisent les documents :
- Sélectionnez [Sur le portail de la zone de lancement BI en tant qu'onglets](#) pour afficher les documents dans des onglets individuels de la zone de lancement de BI.
  - Sélectionnez [Dans plusieurs fenêtres de navigateur en plein écran, une fenêtre par document](#) (In multiple full screen browser windows, one window for each document) pour afficher les documents dans des fenêtres individuelles
10. Dans la zone [Définissez le nombre maximal d'éléments par page](#) saisissez le nombre maximal d'objets à afficher par page lors de la visualisation des listes d'objets.
11. Cliquez sur [Enregistrer et fermer](#).

## 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.

### i 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 Entreprise 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 \[page 244\]](#)

[Pour importer des rôles SAP \[page 312\]](#)

## 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 plug-ins 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_[Nomconvivial]`. 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 Pour modifier les 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.

### i 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 Entreprise ou d'un alias pour un outil d'authentification tiers.

### i 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 Entreprise.

### i 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** + **clac** ou **CTRL** + **clac**.

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.

### i 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.

### i 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 \[page 123\]](#)



## 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'acquiescent 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 \[page 129\]](#)

#### 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 \[page 139\]](#)




### 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.

Table 12 : Options des droits d'accès

Icône	Option	Description
	<a href="#">Accordé</a>	Le droit est accordé à un utilisateur ou groupe principal.
	<a href="#">Refusé</a>	Le droit est refusé à un utilisateur ou groupe principal.
	<a href="#">Non spécifié</a>	Le droit n'est pas spécifié pour un utilisateur ou groupe principal. Par défaut, les droits définis sur <a href="#">Non spécifié</a> sont refusés.

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

## Informations associées

[Droits spécifiques au type \[page 132\]](#)

### 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.

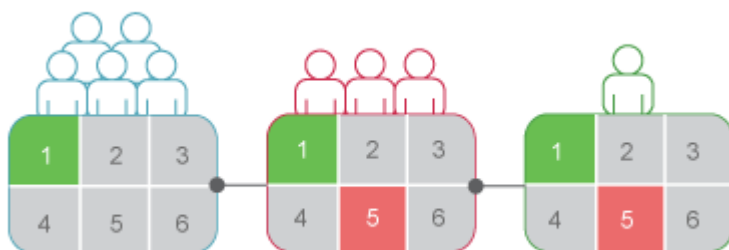


Figure 1 : Héritage de groupe - exemple 1

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.

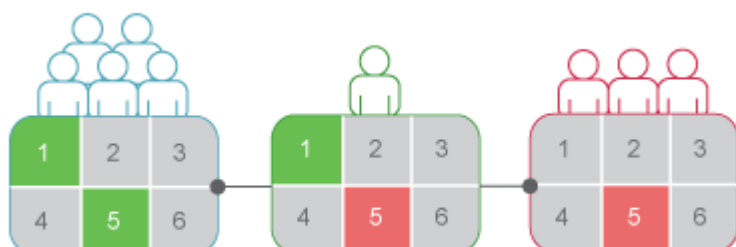


Figure 2 : Héritage de groupe - exemple 2

## Informations associées

[Remplacement des droits \[page 129\]](#)

### 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.

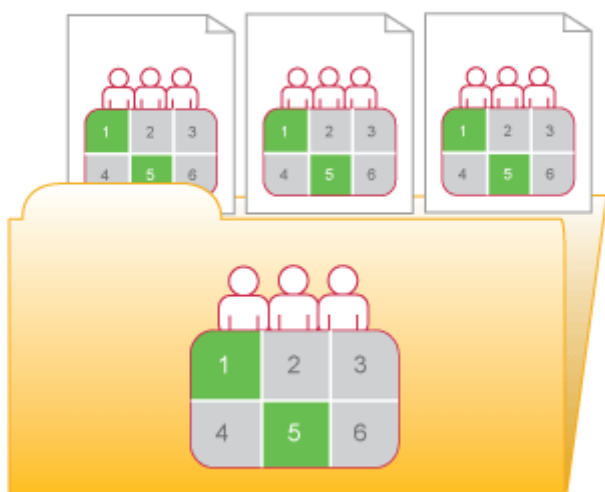


Figure 3 : Exemple d'héritage de dossier

## Informations associées

[Remplacement des droits \[page 129\]](#)

### 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.

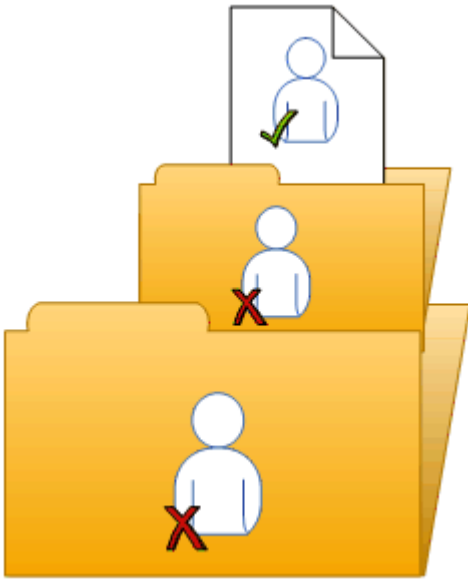


Figure 4 : Remplacement des droits - Exemple 1

« 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.

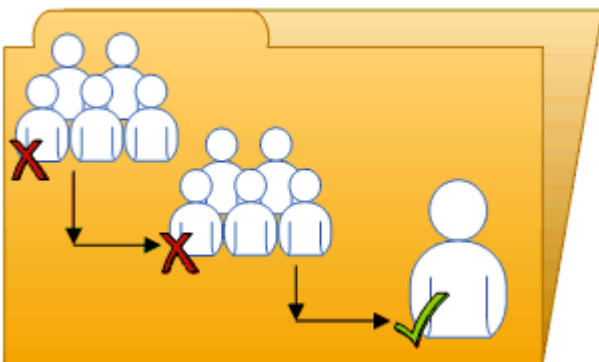


Figure 5 : Remplacement des droits - Exemple 2

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.

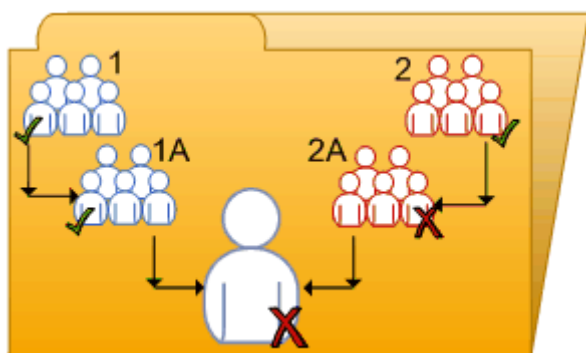


Figure 6 : Remplacement des droits complexe

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.

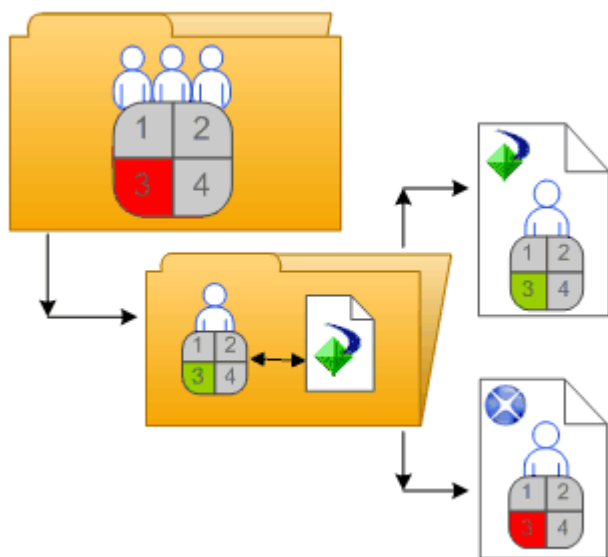


Figure 7 : Droits spécifiques au type : exemple

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.

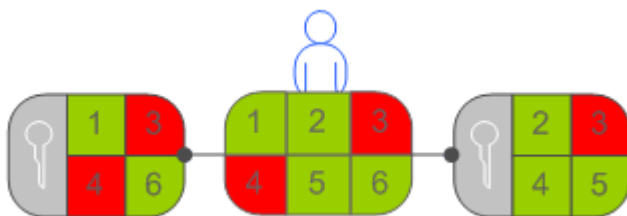


Figure 8 : Plusieurs niveaux d'accès

- 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
  - droits 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 :
  - ensemble
  - 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/groupe principaux](#).  
La boîte de dialogue [Ajouter des utilisateurs/groupe 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 \[page 135\]](#)

## 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 \[page 135\]](#)

## 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.

### i 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 \[page 135\]](#)

[Pour modifier les droits d'un utilisateur ou groupe principal sur un objet \[page 135\]](#)

## 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](#) ►.

**Créer une requête de sécurité: Nina**

**Requête d'utilisateur/groupe principal**

Cette requête va rechercher les objets de l'utilisateur/groupe principal suivant :

Nina

**Requête d'autorisation**

Cette requête recherchera les objets dans lesquels l'utilisateur/groupe principal ci-dessus dispose de toutes les autorisations suivantes :

☐ Ne pas formuler de requêtes d'autorisation

Ensemble	Type	Nom du droit		
Général	Général	Afficher les instances de document appartenant à l'utilisateur	<input checked="" type="checkbox"/>	<input type="button" value="X"/>
Général	Général	Afficher les instances du document	<input checked="" type="checkbox"/>	<input type="button" value="X"/>

**Contexte de la requête**

Cette requête va rechercher les objets dans les sections suivantes de la CMC uniquement :

☒ Dossiers  (Tout) ☒ Sous-objet de requête

☐ Dossiers

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

- 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*.

- 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.

- 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.

Table 13 : Niveaux d'accès prédéfinis

Niveau d'accès	Description	Droits impliqués
<i>Visualiser</i>	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.	<ul style="list-style-type: none"> <li>• Visualiser les objets</li> <li>• Afficher les instances du document</li> </ul>
<i>Planifier</i>	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 <i>Visualiser</i> , plus : <ul style="list-style-type: none"> <li>• Planifier l'exécution du document</li> <li>• Définir les groupes de serveurs pour traiter les tâches</li> <li>• Copier les objets dans un autre dossier</li> <li>• Planifier vers des destinations</li> <li>• Imprimer les données du rapport</li> <li>• Exporter les données du rapport</li> <li>• Modifier les objets appartenant à l'utilisateur</li> <li>• Supprimer les instances appartenant à l'utilisateur</li> <li>• Suspendre et reprendre les instances de document appartenant à l'utilisateur</li> </ul>
<i>Visualiser à la demande</i>	Un utilisateur ou groupe principal peut actualiser les données à la demande par rapport à une source de données.	Droits du niveau d'accès <i>Planifier</i> , plus : <ul style="list-style-type: none"> <li>• Actualiser les données du rapport</li> </ul>
<i>Contrôle total</i>	Un utilisateur ou groupe principal a le contrôle administratif total de l'objet.	Tous les droits disponibles, notamment : <ul style="list-style-type: none"> <li>• Ajouter les objets au dossier</li> <li>• Modifier les objets</li> <li>• Modifier les droits des utilisateurs sur les objets</li> <li>• Supprimer les objets</li> <li>• Supprimer les instances</li> </ul>

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 <i>Ajouter</i> sur le dossier racine des <i>niveaux d'accès</i>
Visualisation de droits granulaires dans un niveau d'accès	Droit <i>Visualiser</i> sur le niveau d'accès
Attribution d'un niveau d'accès à un utilisateur ou groupe principal sur un objet	Droit <i>Visualiser</i> sur le niveau d'accès Droit <i>Utiliser le niveau d'accès pour affecter la sécurité</i> sur le niveau d'accès



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

### 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 attribuer 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* ►.

### i Remarque

Vous ne pouvez pas supprimer de niveaux d'accès prédéfinis.

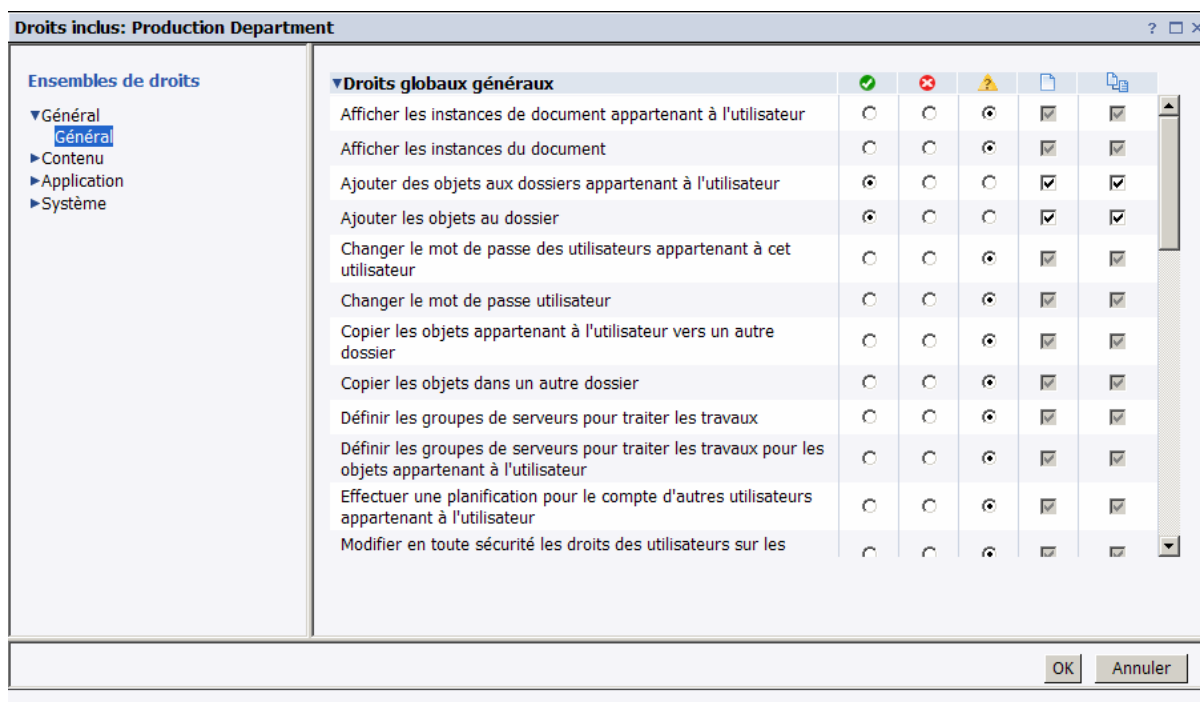
Une boîte de dialogue contenant des informations sur les objets auxquels ce niveau d'accès s'applique s'affiche. Si vous ne souhaitez pas supprimer ce niveau d'accès, cliquez sur *Annuler* pour fermer la boîte de dialogue.

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.

- 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.
- 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.
- 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.

#### **i** Remarque

Pour visualiser la liste des objets affectés, vous devez posséder les droits [Visualiser](#) sur ces objets.

#### **i** 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.

#### **i** 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.

#### **i** 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

### i 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 \[page 756\]](#)

[Suivi de la relation entre niveaux d'accès et objets \[page 144\]](#)

## 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 souhaitez 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.

### i 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.

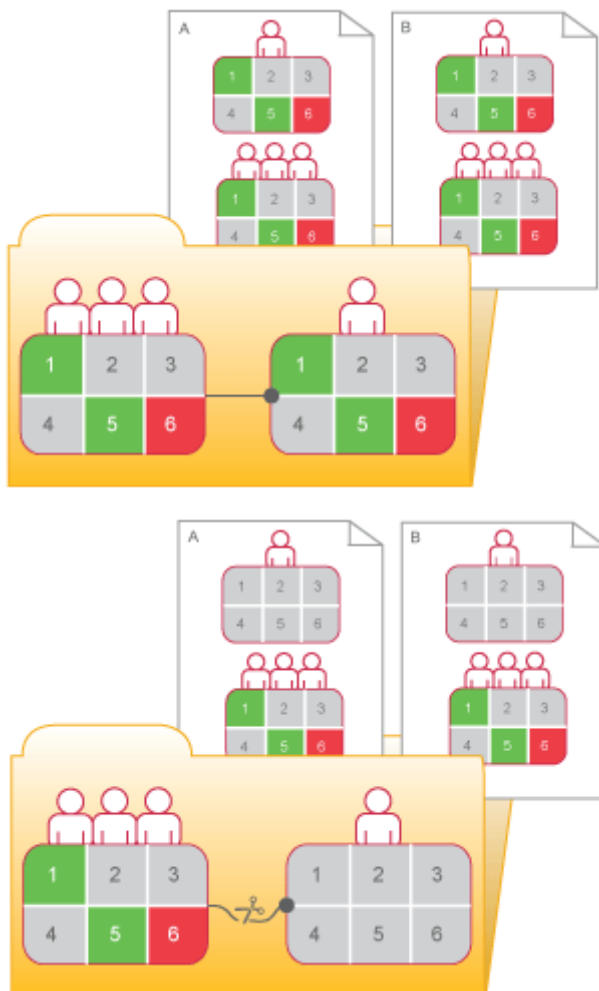


Figure 9 : Rupture de l'héritage

## 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.

### i 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.

Table 14 : Droits des administrateurs délégués

Action de l'administrateur délégué	Droits requis par l'administrateur délégué
Créer des utilisateurs	Droit <i>Ajouter</i> sur le dossier <i>Utilisateurs</i> de niveau supérieur
Créer des groupes	Droit <i>Ajouter</i> sur le dossier <i>Groupes d'utilisateurs</i> de niveau supérieur
Supprimer les groupes contrôlés, ainsi que les utilisateurs individuels appartenant à ces groupes	Droit <i>Supprimer</i> sur les groupes concernés
Supprimer uniquement les utilisateurs créés par l'administrateur délégué	Droit <i>Supprimer par le propriétaire</i> sur le dossier <i>Utilisateurs</i> de niveau supérieur
Supprimer uniquement les utilisateurs et les groupes créés par l'administrateur délégué	Droit <i>Supprimer par le propriétaire</i> sur le dossier <i>Groupes d'utilisateurs</i> 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 <i>Modifier par le propriétaire</i> et <i>Modifier en toute sécurité les droits par le propriétaire</i> sur le dossier <i>Utilisateurs</i> de niveau supérieur
Manipuler uniquement les groupes créés par l'administrateur délégué (y compris l'ajout de ces utilisateurs à ces groupes)	Droits <i>Modifier par le propriétaire</i> et <i>Modifier en toute sécurité les droits par le propriétaire</i> sur le dossier de niveau supérieur <i>Groupes d'utilisateurs</i>
Modifier les mots de passe des utilisateurs dans leurs groupes contrôlés	Droit <i>Modifier le mot de passe</i> sur les groupes concernés
Modifier les mots de passe des utilisateurs ou groupes principaux créés par l'administrateur délégué uniquement	Droit <i>Modifier le mot de passe par le propriétaire</i> sur le dossier <i>Utilisateurs</i> de niveau supérieur ou sur les groupes concernés  <div> <i>i</i> Remarque            La définition du droit <i>Modifier le mot de passe par le propriétaire</i> sur un groupe ne prend effet sur un utilisateur que lorsque vous ajoutez l'utilisateur au groupe concerné.         </div>
Modifier les noms d'utilisateur, les descriptions et les autres attributs, et réaffecter les utilisateurs à d'autres groupes	Droit <i>Modifier</i> 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 <i>Modifier le mot de passe par le propriétaire</i> sur le dossier <i>Utilisateurs</i> de niveau supérieur ou sur les groupes concernés  <div> <i>i</i> Remarque            La définition du droit <i>Modifier par le propriétaire</i> sur les groupes concernés ne prend effet sur un utilisateur que lorsque vous ajoutez l'utilisateur au groupe concerné.         </div>

### 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 souhaitez 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 souhaitez 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.
- Évitez 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 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.

#### 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.

## 8.3 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\win32_x86\config`.
  2. Changez la valeur de ce paramètre en `False` : `WebiParamDetailedDbErrorsEnabled = False`.

## Informations associées

[Configuration du protocole SSL \[page 177\]](#)

[Restrictions relatives aux mots de passe \[page 159\]](#)

[Configuration de la sécurité pour les serveurs tiers fournis \[page 154\]](#)

## 8.4 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 d'accéder à la documentation concernant les composants fournis suivants et de la consulter :

- Sybase SQL Anywhere : pour en savoir plus sur la sécurisation de cette base de données système, voir <http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/da-part-securing.html>.
- Apache Tomcat : pour en savoir plus sur la sécurité de ce serveur d'applications Web, voir <http://tomcat.apache.org/>.

## 8.5 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.

## 8.5.1 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.

## 8.5.2 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.

## 8.6 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.

### i 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.

### 8.6.1 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.



## 8.6.2 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.

### 8.6.2.1 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.

### 8.6.2.2 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** + **clique** 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.

### **i** Remarque

Vous ne pouvez pas mettre fin à votre session d'administrateur actuelle.

## **8.7 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.

### **8.7.1 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.

### **i** 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.

### **8.7.2 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 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.

## 8.9 Audit de l'activité Web

La plateforme de BI vous permet de maîtriser votre système en enregistrant l'activité Web et en vous permettant d'en examiner les détails et de les contrôler. Le serveur d'applications Web permet de sélectionner les attributs Web tels que l'heure, la date, l'adresse IP, le numéro de port, etc. à enregistrer. Les données d'audit sont consignées sur disque et stockées dans des fichiers texte séparés par des virgules, de manière à pouvoir vous y reporter facilement ou les importer dans d'autres applications.

### 8.9.1 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.

### 8.9.2 Restrictions relatives aux mots de passe

Les restrictions relatives au mot de passe incitent les utilisateurs appliquant l'authentification Enterprise par défaut à créer des mots de passe relativement complexes. Vous pouvez activer les options suivantes :

1. Respecter la casse dans les mots de passe

Cette option permet de s'assurer que les mots de passe contiennent au moins deux classes de caractères parmi les suivantes : majuscules, minuscules ou ponctuation.

2. Appliquer les chiffres dans les mots de passe

Cette option permet de vérifier que les mots de passe contiennent des chiffres

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.

### **i** Remarque

Les options 1 et 2 sont cochées par défaut. Au besoin, cela peut être modifié par l'administrateur.

## **8.9.3 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)

## **8.9.4 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.

## 8.9.5 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.

## 8.10 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 Présentation de la 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.

## 8.11.1 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.

### 8.11.1.1 Activation du mode compatible FIPS sous Windows

Par défaut, le mode compatible FIPS est désactivé lorsque la plateforme de BI est installée. Vous pouvez néanmoins activer la compatibilité FIPS pour tous les nœuds dans votre déploiement.

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.

### 8.11.1.2 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.

### 8.11.1.3 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 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.



## 8.12.1 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	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/aix_rs6000_64/</code>
Solaris	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/solaris_sparcv9/</code>
Linux	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/linux_x64/</code>

### 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.

### 8.12.1.1 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.

## 8.12.1.2 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 à huit caractères et appuyez sur la touche *Entrée*.

#### Remarque

Sur les plateformes UNIX, une clé de cluster valide contient une combinaison de huit caractères sans restrictions.

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.

## 8.12.2 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.

### i 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.

### 8.12.2.1 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.

### i 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.

### 8.12.2.2 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 \[page 170\]](#)

### 8.12.3 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 \[page 169\]](#)

[Création d'une clé de cryptage \[page 170\]](#)

[Suppression d'une clé de cryptage du système \[page 172\]](#)

[Blocage d'une clé de cryptage \[page 171\]](#)

[Affichage des objets associés à une clé de cryptage \[page 170\]](#)

[Définition des clés de cryptage sur le statut Compromis \[page 170\]](#)

## 8.12.3.1 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 <i>Actif</i> 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 <i>Actif</i> devient <i>Désactivé</i> . Une clé active ne peut pas être supprimée du système.
Désactivé	Une clé définie sur le statut <i>Désactivé</i> 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 <i>Désactivé</i> ne peut pas être supprimée du système. Vous devez définir le statut de la clé sur <i>Bloqué</i> 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 <i>Bloqué</i> .
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 <i>Désactivé</i> prend le statut Compromis, vous avez le choix entre ne rien faire ou bloquer la clé. Une fois qu'une clé définie sur le statut Compromis est bloquée, elle peut être supprimée.

## 8.12.3.2 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.

## 8.12.3.3 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.

## 8.12.3.4 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.

### i Remarque

Vous pouvez également définir une clé sur le statut Compromis après l'avoir bloquée.

1. Accédez à la zone de gestion des [clés de cryptage](#) de la CMC.
2. Sélectionnez la clé de cryptage à définir sur le statut Compromis.
3. Cliquez sur ► [Actions](#) ► [Marquer comme compromis](#) ►.  
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 compromis](#) 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 \[page 171\]](#)

[Statut des clés de cryptage \[page 169\]](#)

[Affichage des objets associés à une clé de cryptage \[page 170\]](#)

### 8.12.3.5 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.

### 8.12.3.6 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.

#### **i** 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 \[page 171\]](#)

[Statut des clés de cryptage \[page 169\]](#)

## 8.13 Configuration des serveurs pour SSL

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.

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.
- Sinon, configurez SSL pour les certificats gérés par une autorité de certification.

#### **i** Remarque

Si vous utilisez des clients lourds, tels que Crystal Reports, vous devez également les configurer pour SSL si vous voulez vous connecter au CMS à partir de ces clients lourds. 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.



## 8.13.1 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 SSLC.

### Remarque

Vous devez créer des certificats et des clés 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.

### Remarque

Les certificats créés pour des versions antérieures de la plateforme de BI ne fonctionneront pas avec la plateforme SAP BI 4.0. Ces certificats devront être recréés.

### 8.13.1.1 Pour créer un fichier de clé et un fichier de certificat pour un ordinateur

1. Exécutez l'outil de ligne de commande `sslc`.

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.`)

2. Saisissez la commande suivante :

```
sslc req -config sslc.cnf -new -out cacert.req
```

Cette commande crée deux fichiers : une demande de certificat auprès d'une autorité de certification (`cacert.req`) et une clé privée (`privkey.pem`).

3. Pour décrypter la clé privée, saisissez la commande suivante :

```
sslc rsa -in privkey.pem -out cakey.pem
```

Cette commande crée la clé décryptée `cakey.pem`.

4. Pour signer le certificat émis par l'autorité de certification, saisissez la commande suivante :

```
sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

Cette commande crée un certificat auto-signé, `cacert.pem`, qui expire au bout de 365 jours. Choisissez le nombre de jours le mieux adapté à vos besoins en terme de sécurité.

5. Dans un éditeur de texte, ouvrez le fichier `ssl.cnf` qui se trouve dans le même dossier que l'outil de ligne de commande SSLC.

### **i** Remarque

Vous devez utiliser un éditeur de texte pour Windows car Windows Explorer est susceptible de ne pas reconnaître ou afficher les fichiers ayant une extension `.cnf`.

6. Effectuez les actions suivantes basées sur les paramètres du fichier `ssl.cnf` :

- a. Placez les fichiers `cakey.pem` et `cacert.pem` dans les répertoires spécifiés par les options `certificate` et `private_key` du fichier `ssl.cnf`. Par défaut, les paramètres dans le fichier `ssl.cnf` sont les suivants :

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- b. Créez un fichier portant le nom spécifié par le paramètre `database` du fichier `ssl.cnf`.

### **i** Remarque

Par défaut, le fichier est nommé `$dir/index.txt` et doit être vide.

- c. Créez un fichier portant le nom spécifié par le paramètre `serial` du fichier `ssl.cnf`.

Le fichier doit fournir un numéro de série en chaîne octet (au format hexadécimal).

### **i** Remarque

Pour être sûr de pouvoir créer et signer d'autres certificats, choisissez un grand nombre hexadécimal comportant un nombre pair de chiffres, tel que `11111111111111111111111111111111`.

- d. Créez le répertoire spécifié par le paramètre `new_certs_dir` du fichier `ssl.cnf`.

7. Pour créer une demande de certificat et une clé privée, saisissez la commande suivante :

```
ssl req -config ssl.cnf -new -out servercert.req
```

Le certificat et les fichiers de clés générés sont placés dans le dossier de travail en cours.

8. Pour décrypter la clé du fichier `privkey.pem`, saisissez les commandes suivantes :

```
ssl rsa -in privkey.pem -out server.key
```

9. Pour signer le certificat validé par l'autorité de certification, saisissez la commande suivante :

```
ssl ca -config ssl.cnf -days 365 -out servercert.pem -in servercert.req
```

Cette commande crée le fichier `servercert.pem` qui contient le certificat signé.

10. Tapez les commandes suivantes pour convertir les certificats en certificats codés DER :

```
ssl x509 -in cacert.pem -out cacert.der -outform DER
```

```
ssl x509 -in servercert.pem -out servercert.der -outform DER
```

### **i** Remarque

Le certificat émis par l'autorité de certification (`cacert.der`) et la clé privée correspondante (`cakey.pem`) ne doivent être générés qu'une seule fois par déploiement. Tous les ordinateurs du même déploiement partagent les mêmes certificats. Tous les autres certificats doivent être signés par la clé privée d'un certificat émis par une autorité de certification.

11. Créez un fichier texte `passphrase.txt` pour stocker la phrase de passe en texte brut utilisée pour décrypter la clé privée générée.

12. Stockez les fichiers de clé et de certificat suivants dans un emplacement sécurisé (sous le même répertoire) accessible aux ordinateurs de votre déploiement de plateforme de BI :

- Fichier du certificat approuvé (`cacert.der`)
- Fichier du certificat serveur généré (`servercert.der`)
- Fichier de la clé serveur (`server.key`)
- Fichier de la phrase de passe (`passphrase.txt`)

Cet emplacement sera utilisé pour configurer le protocole SSL pour le CCM et votre serveur d'applications Web.

## 8.13.2 Configuration de SSL lorsque le certificat est géré par une autorité de certification

Lors de la configuration de SSL pour la communication des serveurs, suivez cette procédure si le certificat est géré par une autorité de certification.

1. Exportez le certificat voulu avec sa clé privée au format PKCS #12 (.PFX).  
Il sera utilisé comme certificat pour l'autorité de certification.
2. A l'aide d'OpenSSL, exécutez les commandes suivantes :
  1. Exportez le fichier de clé privée à partir du fichier .pfx :  
`openssl pkcs12 -in filename.pfx -nocerts -out privkey.pem`
  2. Exportez le fichier de certificat à partir du fichier .pfx :  
`openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cacert.pem`
  3. Supprimez la phrase de passe de la clé privée :  
`openssl rsa -in privkey.pem -out cakey.pem`
3. Configurez certains fichiers requis :
  - Copiez `cakey.pem` à l'emplacement `C:\SSL\private\cakey.pem`.
  - Copiez `cacert.pem` à l'emplacement `C:\SSL\cacert.pem`.
  - Créez un fichier texte vide (un fichier d'index de base de données) nommé `index.txt` dans le dossier `C:\SSL`.
  - Créez un autre fichier texte : `C:\SSL\serial`.
  - Ouvrez le fichier `C:\SSL\serial` dans un éditeur de texte, saisissez la valeur suivante et enregistrez le fichier : `11111111111111111111`
4. Dans un éditeur de texte, ouvrez le fichier `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslc.cnf`.  
Choisissez une de ces options :
  - Changez la valeur de la variable `policy` en `policy_anything`. Cette modification permet de créer un certificat de serveur n'ayant pas les mêmes stratégies que le certificat de votre autorité de certification.
  - Sinon, laissez la valeur de la variable `policy` inchangée, par exemple `policy_match`. Cela force le certificat du serveur à avoir les mêmes stratégies que le certificat de votre autorité de certification. Dans ce cas, vous devez modifier les propriétés de `req_distinguished_name` en conséquence.
5. Créez une demande de certificat et une clé privée.  
Dans une invite de commande, exécutez la commande suivante :  
  
`sslc req -config sslc.cnf -new -out servercert.req`

### i Remarque

Pour la Phrase de passe PEM, saisissez un mot de passe quelconque d'au moins quatre caractères.

### i Remarque

Pour le **Nom courant**, saisissez le nom de domaine complet de l'ordinateur sur lequel les serveurs de la plateforme de BI sont exécutés.

### i Remarque

Le fichier servercert.req est créé à l'emplacement C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32\_x86.

### i Remarque

Les fichiers `.rnd` et `privkey.pem` sont modifiés.

6. Décryptez la clé privée.

```
sslc rsa -in privkey.pem -out server.key
```

7. Signez le certificat.

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

**i** Remarque

Le fichier servercert.pem est créé à l'emplacement C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32\_x86.

**i** Remarque

Le fichier 11111111111111111111.pem est créé dans C:\SSL\newcerts.

### i Remarque

Une sauvegarde du fichier `serial` est créée, elle est nommée `serial.old`.

**i** Remarque

La valeur de `serial` est incrémentée de 111111111111111111 à 111111111111111112.

8. Convertissez les certificats au codage DER.

Exécutez ces commandes :

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

### **i** Remarque

Le fichier `servercert.der` est créé à l'emplacement `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

### **i** Remarque

Le fichier `cacert.der` est créé à l'emplacement `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

9. Créez un fichier texte nommé `passphrase.txt`.

Le contenu du fichier doit être la phrase de passe PEM utilisée auparavant.

10. Stockez les fichiers suivants dans un emplacement sécurisé, par exemple `C:\SSLCerts`.

- le fichier du certificat approuvé `cacert.der`
- le fichier du certificat serveur généré `servercert.der`
- le fichier de la clé serveur `server.key`
- le fichier de la phrase de passe `passphrase.txt`

## 8.13.3 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.

### 8.13.3.1 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 : <code>d:\ssl</code>
Fichier du certificat SSL du serveur	Nom du fichier utilisé pour stocker le certificat SSL du serveur. Par défaut, <code>servercert.der</code>
Fichier des certificats SSL approuvés	Nom du fichier contenant les certificats SSL approuvés. Le nom par défaut est : <code>cacert.der</code>

Champ	Description
Fichier de la clé privée SSL	Nom du fichier de clé privée SSL utilisé pour accéder au certificat. Le nom par défaut est : <code>server.key</code>
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 : <code>passphrase.txt</code>

#### Remarque

Vérifiez que le répertoire mentionné se trouve sur l'ordinateur sur lequel s'exécute le serveur.

## 8.13.3.2 Configuration du protocole SSL sous UNIX

Vous devez utiliser 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 .
4. Spécifiez le SIA cible et appuyez sur .
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.

## 8.13.3.3 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 :

Table 15 :

Exemple	Description
<code>&lt;DcertDir&gt;=d:\ssl</code>	Répertoire de stockage des certificats et des clés.
<code>&lt;DtrustedCert&gt;=cacert.der</code>	Fichier de certificat approuvé. Si vous en spécifiez plusieurs, séparez-les par des points-virgules.
<code>&lt;DsslCert&gt;=clientcert.der</code>	Certificat utilisé par le SDK.
<code>&lt;DsslKey&gt;=client.key</code>	Clé privée du certificat SDK.
<code>&lt;Dpassphrase&gt;=passphrase.txt</code>	Fichier de stockage de la phrase de passe de la clé privée.

- 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.

### 8.13.3.4 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	<code>d:\ssl</code>
Nom du fichier du certificat SSL du serveur	<code>servercert.der</code>
Certificat approuvé SSL ou nom du fichier de certificat racine	<code>cacert.der</code>
Nom du fichier de la clé privée SSL	<code>server.key</code>
Fichier contenant la phrase de passe pour accéder au fichier de la clé privée SSL	<code>passphrase.txt</code>

Une fois les ressources ci-dessus créées, observez les instructions suivantes pour configurer les applications client lourd telles que le Central Configuration Manager (CCM) ou l'outil de gestion de la mise à niveau.

- Assurez-vous que l'application client lourd n'est pas en cours d'opération.

#### **i** Remarque

Vérifiez que le répertoire mentionné se trouve sur l'ordinateur sur lequel s'exécute le serveur.

- Exécutez l'outil de ligne de commande `sslconfig.exe`.

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 -protocol ssl
```

4. Relancez l'application client lourd.

## Informations associées

[Pour créer un fichier de clé et un fichier de certificat pour un ordinateur \[page 173\]](#)

### 8.13.3.4.1 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.

### 8.13.3.4.2 Pour configurer SSL pour l'outil de conversion de rapports

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. En outre, l'outil de conversion de rapports doit être installé dans le cadre de votre déploiement de la plateforme de BI.

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



Ressource SSL	
Certificat approuvé SSL ou nom du fichier de certificat racine	<code>cacert.der</code>
Nom du fichier de la clé privée SSL	<code>server.key</code>
Fichier contenant la phrase de passe pour accéder au fichier de la clé privée SSL	<code>passphrase.txt</code>

Une fois les ressources ci-dessus créées, observez les instructions suivantes pour configurer SSL afin d'utiliser l'outil de conversion de rapports.

1. Créez une variable d'environnement Windows `<BOBJ_MIGRATION>` sur l'ordinateur hébergeant l'outil de conversion de rapport.

#### ➔ Conseil

La variable peut être définie sur une valeur quelconque.

2. A l'aide d'un éditeur de texte, ouvrez le fichier `migration.bat` dans le répertoire suivant :  
`<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.`
3. Recherchez la ligne suivante :

```
start "" "%JRE%\bin\javaw" -cp migration.jar;* -Xmx512m -Xss10m
com.bo.migration.MigrationTool
```

4. Ajoutez ceci après le paramètre `-Xss10m` :

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=d:\ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

#### i Remarque

Vérifiez qu'il existe un espace entre chaque paramètre et aucun espace à la fin des lignes.

5. Enregistrez le fichier et fermez l'éditeur de texte.

Les utilisateurs peuvent à présent utiliser SSL pour accéder à l'outil de conversion de rapports.

## Informations associées

[Pour créer un fichier de clé et un fichier de certificat pour un ordinateur \[page 173\]](#)

---

## 8.14 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 \[page 194\]](#)

[Exemples de scénarios classiques de pare-feu \[page 199\]](#)

### 8.14.1 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.

#### 8.14.1.1 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.

### 8.14.1.2 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.

### 8.14.1.3 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™.

### 8.14.1.4 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 \[page 184\]](#)

## 8.14.1.5 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.

## 8.14.1.6 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 \[page 893\]](#)

## 8.14.2 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.

### 8.14.2.1 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 \[page 186\]](#)

## 8.14.2.2 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.

### 8.14.2.2.1 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.

Table 16 :

Produit	Application client	Serveurs associés	Spécifications requises pour le port du serveur
Crystal Reports	Concepteur SAP Crystal Reports 2013	CMS Input FRS Output FRS Report Application Server (RAS) de Crystal Reports 2013 Serveur de traitement Crystal Reports 2013 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 2013  Port de requêtes du serveur de traitement Crystal Reports 2013  Port de requêtes du Crystal Reports Cache Server
Crystal Reports	Concepteur SAP Crystal Reports pour Enterprise	CMS Input FRS Output FRS Crystal Reports Processing Server 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 serveur de traitement Crystal Reports  Port de requêtes du Crystal Reports Cache Server

Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
Tableaux de bord	SAP BusinessObjects Dashboards	CMS Input FRS Output FRS Application de fournisseur de services Web (dswsboobje.war) hébergeant les services Web Dashboards, Live Office et QaaWS requis pour certaines connexions de sources de données	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 HTTP (80 par défaut)
Live Office	Client Live Office	Application de fournisseur de services Web (dswsboobje.war) hébergeant le service Web Live Office	Port HTTP (80 par défaut)
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	<p>Les ports suivants doivent être ouverts pour permettre au CCM de gérer des serveurs de la plateforme de BI distants :</p> <p>Port de serveur de noms du CMS (6400 par défaut)</p> <p>Port de requêtes du CMS</p> <p>Les ports suivants doivent être ouverts pour permettre au CCM de gérer des processus SIA distants :</p> <p>Microsoft Directory Services (port TCP 445)</p> <p>NetBIOS Session Service (port TCP 139)</p> <p>NetBIOS Datagram Service (port UDP 138)</p> <p>NetBIOS Name Service (port UDP 137)</p> <p>DNS (port TCP/UDP 53)</p> <p>(Notez que certains ports mentionnés ci-dessus peuvent ne pas être requis. Consultez votre administrateur Windows).</p>
Plateforme de BI	Server Intelligence Agent (SIA)	Tous les serveurs de la plateforme de BI y compris le CMS	<p>Port de requêtes du Server Intelligence Agent (6410 par défaut)</p> <p>Port de serveur de noms du CMS (6400 par défaut)</p> <p>Port de requêtes du CMS</p>
Plateforme de BI	Outil de conversion de rapport	CMS Input FRS	<p>Port de serveur de noms du CMS (6400 par défaut)</p> <p>Port de requêtes du CMS</p> <p>Port de requêtes de l'Input FRS</p>
Plateforme de BI	Repository Diagnostic Tool	CMS Input FRS Output FRS	<p>Port de serveur de noms du CMS (6400 par défaut)</p> <p>Port de requêtes du CMS</p> <p>Port de requêtes de l'Input FRS</p> <p>Port de requêtes de l'Output FRS</p>



Produit	Application cliente	Serveurs associés	Spécifications requises pour le port du serveur
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 2013 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 2013
Plateforme de BI	Fournisseur de services Web (dswsboj.e.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

## 8.14.2.2.2 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.

Table 17 :

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.
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 ( <a href="#">send to FTP</a> ).

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)	<p>Les Job Servers utilisent les ports SFTP pour autoriser <i>l'envoi vers SFTP</i>.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> <p>L'Administrateur/L'utilisateur doit configurer l'empreinte SHA-1 pour activer SFTP. Il peut se reporter à la documentation produit de l'implémentation de serveur SSH/SFTP pour générer une empreinte SHA-1.</p> </div> <div> <p><b>Exemple</b></p> <p>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-1, 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 :</p> <pre>ssh-rsa &lt;base64 encoded key&gt;, exécutez le script suivant :</pre> <pre>cut -d ' ' -f 2 &lt; RSAKey.pub   base64 -d   openssl dgst -c -sha1.</pre> <p>qui génère, par exemple,</p> <pre>(stdin)= 00:93:1e:cc:bd:cc: 43:05:41:89:5f:</pre> </div>

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
			<p>5c:c7:91:1d:11:a0:1e:58:e8, où la série de 20 chiffres dépend de la valeur de la clé publique codée 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.</p> <p>➔ <b>Recommandation</b></p> <p>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.</p>

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 25)	<p>Les Job Servers utilisent les ports SMTP pour autoriser l'envoi vers la messagerie (<a href="#">send to email</a>).</p> <p><b>Configuration SMTP sur SSL :</b></p> <p>Pour configurer SMTP sur SSL, le serveur et les systèmes client doivent comporter le même certificat.</p> <p>Pour configurer SMTP sur SSL, suivez les étapes mentionnées ci-dessous :</p> <ol style="list-style-type: none"> <li>1. Sur la plateforme Windows, accédez à &lt;rép_install&gt;\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64. De plus, pour les clients connectés à la plateforme de BI, accédez à &lt;install_dir&gt;\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86.</li> </ol> <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <p><b>i Remarque</b></p> <p>Pour toutes les autres plateformes prises en charge, accédez aux dossiers respectifs.</p> </div> <ol style="list-style-type: none"> <li>2. Nommez le certificat "certificat.crt". Par exemple, lors de la connexion au serveur SMTP, le serveur enverra les informations relatives au certificat. Les informations du certificat doivent être copiées dans un fichier texte brut et celui-ci doit être renommé "certificat.crt". Il doit être placé dans le dossier win64_x64 pour la plateforme Windows et dans le dossier win32_x86 pour les clients.</li> </ol> <p>La configuration SMTP sur SSL est terminée.</p>

Application tierce	Composant SAP BusinessObjects utilisant le produit tiers	Spécifications de port requises pour l'application tierce	Description
			<p><b>i Remarque</b></p> <ul style="list-style-type: none"> <li>En cochant la case <a href="#">Activer SSL</a>, l'utilisateur active un canal sécurisé. Cela permet de sécuriser la transmission SMTP sur SSL.</li> <li>SMTP ne prend pas en charge SSL via le workflow Événements (lorsque l'utilisateur tente d'envoyer une notification d'alerte par courrier électronique).</li> </ul>
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 ( <a href="#">send to disk</a> ).
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.

## 8.15 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.

### 8.15.1 Pour configurer le système pour des pare-feu

- Déterminez quels composants de la plateforme de BI doivent communiquer via un pare-feu.
- 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 \[page 184\]](#)

[Configuration des numéros de port \[page 402\]](#)

[Présentation des lignes de commande \[page 893\]](#)

[Spécification des règles de pare-feu \[page 195\]](#)

[Configurer le fichier hosts pour les pare-feu qui utilisent NAT \[page 196\]](#)

### 8.15.1.1 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.

#### **i** 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.

#### **i** 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.

Table 18 :

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
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 \[page 184\]](#)

### 8.15.1.2 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.

### 8.15.1.2.1 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`.

### 8.15.1.2.2 Configuration du fichier hosts sous UNIX

#### **i** Remarque

Votre système d'exploitation UNIX doit être configuré de façon à consulter d'abord 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`.

## 8.15.2 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
```

### 8.15.2.1 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 [Ecouté 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 \[page 402\]](#)

## 8.16 Exemples de scénarios classiques de pare-feu

Cette section fournit des exemples de scénarios de déploiement de pare-feu classiques.

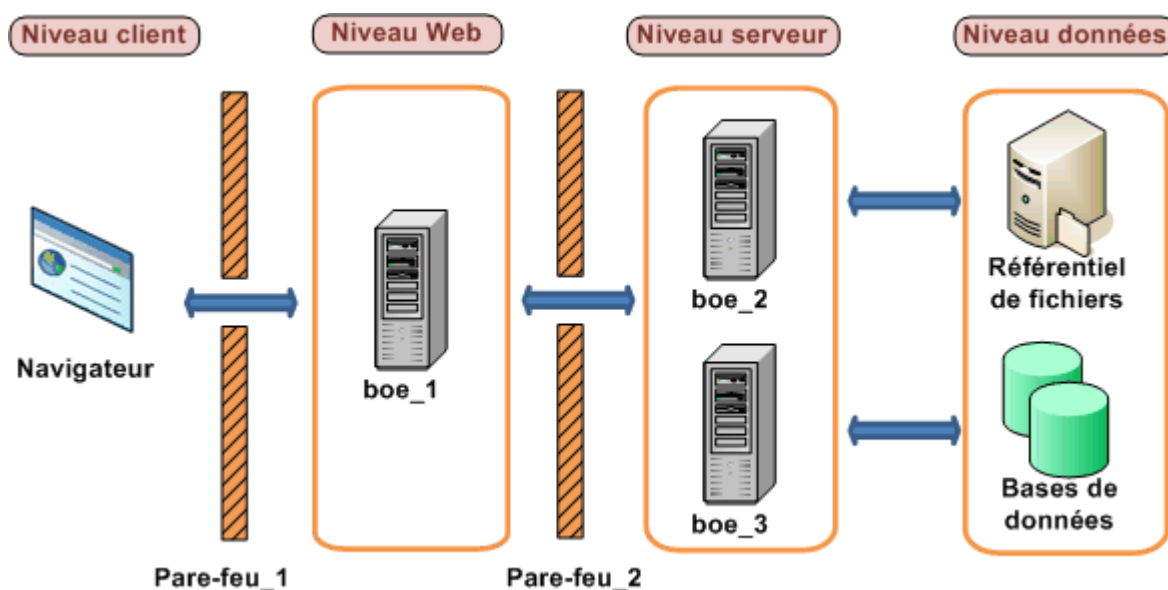
### 8.16.1 Exemple - Niveau application déployé sur un réseau distinct

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.

Figure 10 : Niveau application déployé sur un réseau distinct



### 8.16.1.1 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.

Table 19 :

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

Serveur	Numéro de port
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.

Table 20 : Configuration de Pare-feu\_1

Port	Ordinateur de destination	Port	Action
N'importe lequel	boe_1	8080	Autoriser

Table 21 : 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
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 \[page 402\]](#)

[Description de la communication entre les composants de la plateforme de BI \[page 182\]](#)

## 8.16.2 Exemple : Client lourd et niveau base de données séparés des serveurs de la plateforme de BI par un pare-feu

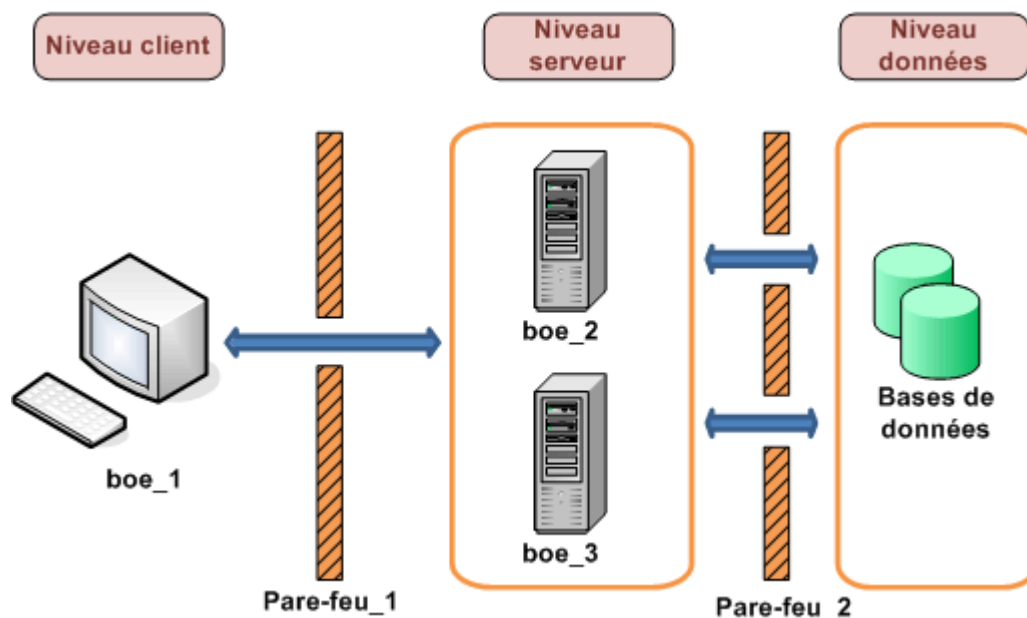
Cet exemple montre comment configurer un pare-feu et la plateforme de BI afin qu'ils puissent fonctionner ensemble dans un scénario de déploiement dans lequel :

- 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.

Figure 11 : Rich Client et niveau base de données déployés sur des réseaux distincts



## 8.16.2.1 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.

Table 22 :

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.

Table 23 :

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.

Table 24 :

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 \[page 182\]](#)

[Configuration de la plateforme de BI pour les pare-feu \[page 194\]](#)

## 8.17 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 :



Table 25 :

Spécifications requises pour le port du serveur
<ul style="list-style-type: none"><li>• Port du serveur de noms du Central Management Server</li><li>• Port de requêtes du Central Management Server</li><li>• Port de requêtes de l'Input FRS</li><li>• Port de requêtes de l'Output FRS</li><li>• Port de requêtes du Report Application Server</li><li>• Port de requêtes du Crystal Reports Cache Server</li><li>• Port de requêtes du Page Server Crystal Reports</li><li>• Port de requêtes du serveur de traitement Crystal Reports</li></ul>

## 8.17.1 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.

### **i** 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 \[page 807\]](#)

## 8.17.1.1 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 (ABAP). 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 lequel	Serveur d'applications Web de la plateforme de BI	Port HTTP/HTTPS du service Web	Autoriser
SAP	N'importe lequel	CMS	Port du serveur de noms du CMS	Autoriser
SAP	N'importe lequel	CMS	Port du CMS requis	Autoriser
Serveur d'applications Web	N'importe lequel	SAP	Port du service de passerelle du système SAP	Autoriser
Central Management Server (CMS)	N'importe lequel	SAP	Port du service de passerelle du système SAP	Autoriser
Crystal Reports™	N'importe lequel	SAP	Port du service de passerelle du système SAP et port du répartiteur du système SAP	Autoriser

## 8.17.2 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

Table 26 :

Produit	Spécifications requises pour le port du serveur
plateforme SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> <li>• Port du serveur de connexion de la plateforme de BI</li> </ul>

## Exigences en matière de ports pour JD Edwards EnterpriseOne

Table 27 :

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.

Table 28 : 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 lequel	JD Edwards EnterpriseOne	N'importe lequel	Autoriser
Serveurs de la plateforme de BI avec connectivité des données pour JD Edwards EnterpriseOne	N'importe lequel	JD Edwards EnterpriseOne	N'importe lequel	Autoriser

Ordinateur source	Port	Ordinateur de destination	Port	Action
Crystal Reports avec connectivité des données côté client pour JD Edwards EnterpriseOne	N'importe lequel	JD Edwards EnterpriseOne	N'importe lequel	Autoriser
Serveur d'applications Web	N'importe lequel	JD Edwards EnterpriseOne	N'importe lequel	Autoriser

## 8.17.3 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.

### 8.17.3.1 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 :

Table 29 :

Ordinateur source	Port	Ordinateur de destination	Port	Action
Serveur d'applications Web	N'importe lequel	Oracle EBS	Port de base de données Oracle	Autoriser
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

## 8.17.4 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

Table 30 :

Produit	Spécifications requises pour le port du serveur
Plateforme SAP BI	<ul style="list-style-type: none"><li>• Port du serveur de connexion de la plateforme de BI</li></ul>

### Configuration de port requise pour PeopleSoft

Table 31 :

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 procéder à une configuration supplémentaire.

Table 32 : 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

## 8.17.5 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.

Table 33 : Ports requis pour les serveurs de la plateforme de BI

Produit	Spécifications requises pour le port du serveur
Plateforme SAP BI	<ul style="list-style-type: none"><li>Port du serveur de connexion de la plateforme de BI</li></ul>

Table 34 : 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.

Table 35 :

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

## 8.18 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.

## 8.18.1 Serveurs proxy inverses pris en charge

La plateforme de BI prend en charge les serveurs proxy inverses suivants :

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

## 8.18.2 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
- `dswsboobje` : 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.

## 8.19 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.



## 8.19.1 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.

## 8.19.2 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.

## 8.19.3 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. 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/
```

## 8.19.4 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
```

## 8.19.5 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*.

i 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 réseauxISA 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**

#### **i** 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.

## **8.20 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.

### **8.20.1 Activation du proxy inverse pour les services Web**

Cette section décrit les procédures requises pour activer les proxys inverses pour les services Web.

#### **8.20.1.1 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` :

```
<!-- 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"
      proxyPort="80" disableUploadTimeout="true" />
-->
```

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.

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 respectivement remplacés par le nom du serveur proxy inverse et son port d'écoute.

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.

## 8.20.1.2 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.

## 8.20.2 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.

## 8.20.2.1 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.

## 8.20.2.2 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.

### 8.20.2.3 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.

### 8.20.2.4 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.

## 8.20.3 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.

### **i** 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.

### 8.20.3.1 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.

##### **i** Remarque

Par défaut, le mot de passe défini par l'utilisateur doit comporter au moins six caractères, avec un mélange de majuscules, minuscules et chiffres. En outre, l'utilisateur peut imposer des caractères spéciaux dans le mot de passe.

- 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 EnterpriseOne 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.

#### **i** 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, ce qui est le cas 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

Mode d'authentification	Serveur CMS	Options	Remarques
			et la CMC est 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.

- [Connexion unique à la plateforme de BI \[page 225\]](#)
- [Connexion unique à la base de données \[page 227\]](#)
- [Connexion unique de bout en bout \[page 228\]](#)

### 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.

#### **i** 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 pour la plateforme de BI, elle est automatiquement activée lorsque vous installez le système pour la première fois, et 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
<i>Restrictions relatives aux mots de passe</i>	<i>Appliquer des mots de passe à casse mixte</i>	Cette option permet de s'assurer que les mots de passe contiennent au moins deux classes de caractères parmi les



Paramètres	Options	Description
		<p>suivantes : majuscules, minuscules ou ponctuation.</p> <div> <i>i</i> <b>Remarque</b>  Par défaut, cette option est cochée. Au besoin, elle peut être décochée par l'administrateur. </div>
	<i>Appliquer les chiffres dans les mots de passe</i>	<p>Cette option permet de vérifier que les mots de passe comportent au moins un caractère numérique.</p> <div> <i>i</i> <b>Remarque</b>  Par défaut, cette option est cochée. Au besoin, elle peut être décochée par l'administrateur. </div>
	<i>Appliquer les caractères spéciaux dans les mots de passe</i>	Cette option permet de vérifier que les mots de passe comportent au moins un caractère spécial.
<i>Restrictions relatives aux utilisateurs</i>	<i>Doit changer de mot de passe tous les N jours</i>	Cette option permet que les mots de passe ne deviennent pas un problème et qu'ils soient actualisés régulièrement.
	<i>Les N derniers mots de passe ne peuvent pas être réutilisés</i>	Cette option permet que les mots de passe ne soient pas répétés par habitude.
	<i>Le mot de passe peut être modifié après N minute(s)</i>	Cette option permet que les nouveaux mots de passe ne puissent pas être modifiés immédiatement après leur saisie dans le système.
<i>Restrictions relatives aux connexions</i>	<i>Désactiver le compte après N échecs de connexion</i>	Cette option de sécurité spécifie le nombre de tentatives de connexion autorisées pour un utilisateur avant que son compte ne soit désactivé.
	<i>Réinitialiser le nombre d'échecs de connexion après N minute(s)</i>	Cette option spécifie un intervalle de temps avant la réinitialisation du compteur de tentatives de connexion.
	<i>Réactiver le compte après N minute(s)</i>	Cette option spécifie la durée pour laquelle un compte est suspendu après N échecs de tentative de connexion.
<i>Synchroniser les références de connexion à la source de données lors de la connexion</i>	<i>Activer et mettre à jour les références de connexion à la source de données de l'utilisateur au moment de la connexion</i>	Cette option active les références de connexion aux sources de données après que l'utilisateur se soit connecté.
<i>Authentification sécurisée</i>	<i>L'authentification sécurisée est activée</i>	Fournit les paramètres de configuration de l'authentification sécurisée.

## 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

#### i 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.

Table 36 :

Paramètre de mot de passe	Valeur minimale	Valeur maximale recommandée
<i>Doit comprendre N caractères au minimum</i>	0 caractère	64 caractères
<i>Doit changer de mot de passe tous les N jours</i>	1 jour	100 jours
<i>Les N derniers mots de passe ne peuvent être réutilisés</i>	1 mot de passe	100 mots de passe
<i>Le mot de passe peut être modifié après N minute(s)</i>	0 minute	100 minutes

Paramètre de mot de passe	Valeur minimale	Valeur maximale recommandée
<i>Désactiver le compte après N échecs de connexion</i>	1 échec	100 échecs
<i>Réinitialiser le nombre d'échecs de connexion après N minute(s)</i>	1 minute	100 minutes
<i>Réactiver le compte après N minute(s)</i>	0 minute	100 minutes

4. Cliquez sur *Mettre à jour*.

#### Remarque

Les comptes inactifs Enterprise ne sont pas automatiquement désactivés. Les administrateurs système doivent supprimer manuellement les comptes qui ne sont plus actifs.

## 9.2.4 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 allez utiliser pour établir la connexion à la plateforme de BI.
- L'URL de connexion unique pour la zone de lancement BI est `http://server:port/BOE/BI`.

## Informations associées

Pour configurer le serveur de manière à utiliser l'authentification sécurisée [page 232]

Pour configurer l'authentification sécurisée pour l'application Web [page 236]

### 9.2.4.1 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.

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. Vous devez 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 :
    - `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
    - `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
5. Cliquez sur *Mettre à jour* pour activer le secret partagé.

#### 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.

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.

## 9.2.5 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`.

### 9.2.5.1 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.

### **i** Remarque

Les utilisateurs doivent être importés sur la plateforme de BI ou disposer de comptes Enterprise.

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.

### **i** Remarque

Une propriété spécifique pour le fichier war BOE (`trusted.auth.user.namespace.enabled`) doit être activée pour que ce mécanisme fonctionne.

## 9.2.5.2 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`.

Propriété	Valeur par défaut	Description
<code>sso.enabled=true</code>	<code>sso.enabled=false</code>	Active et désactive la connexion unique (SSO) à la plateforme de BI. Définissez sur <code>true</code> pour activer l'authentification sécurisée.
<code>trusted.auth.shared.secret</code>	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.
<code>trusted.auth.user.param</code>	Aucune	Spécifie la variable utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée.
<code>trusted.auth.user.retrieval</code>	Aucune	Spécifie la méthode utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée : <ul style="list-style-type: none"><li>• <code>REMOTE_USER</code></li><li>• <code>HTTP_HEADER</code></li><li>• <code>COOKIE</code></li><li>• <code>QUERY_STRING</code></li><li>• <code>WEB_SESSION</code></li><li>• <code>USER_PRINCIPAL</code></li></ul> Ne définissez aucune valeur pour désactiver l'authentification sécurisée.
<code>trusted.auth.user.namespace.enabled</code>	Aucun	Active et désactive la liaison dynamique des alias aux comptes utilisateur existants. Si le paramètre est défini sur <code>true</code> , l'authentification sécurisée utilise la liaison d'alias pour authentifier les utilisateurs sur 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.

Propriété	Valeur par défaut	Description
		Si le paramètre est vide, l'authentification sécurisée utilisera la correspondance de noms lors de l'authentification des utilisateurs.

### 9.2.5.3 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 :

Table 37 :

Plateforme	Emplacement du fichier <code>TrustedPrincipal.conf</code>
Windows, installation par défaut	<ul style="list-style-type: none"> <li><code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86\</code></li> <li><code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\</code></li> </ul>
AIX	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/ aix_rs6000/</code>
Solaris	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/ solaris_sparc/</code>
Linux	<code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/linux_x86</code>

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/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.

#### **i** 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=<Méthode d'extraction de l'ID utilisateur>
trusted.auth.user.param=<Variable>
trusted.auth.shared.secret=<WEB_SESSION>
```

Pour la propriété `trusted.auth.shared.secret`, sélectionnez l'une des options suivantes pour l'extraction du nom d'utilisateur :

Table 38 :

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 <code>trusted.auth.user.param</code> .
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 <code>trusted.auth.user.param</code> .
COOKIE	Le nom d'utilisateur est extrait d'un cookie défini. Vous spécifiez le cookie à utiliser dans la propriété <code>trusted.auth.user.param</code> .
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 <code>trusted.auth.user.param</code> du fichier <code>global.properties</code> .
REMOTE_USER	Le nom d'utilisateur est extrait d'un appel à <code>HttpServletRequest.getRemoteUser()</code> .
USER_PRINCIPAL	Le nom d'utilisateur est extrait d'un appel à <code>getUserPrincipal().getName()</code> sur l'objet <code>HttpServletRequest</code> pour la requête en cours dans un servlet ou un fichier JSP.

### 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*.

## 9.2.5.3.1 Exemples de configuration

### 9.2.5.3.1.1 Pour transmettre le secret partagé par le biais du fichier `TrustedPrincipal.conf`

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 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\win32_x86`. 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=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

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. Apportez les modifications suivantes au fichier `custom.jsp` dans le fichier `com.businessobjects.webpath.InfoView.jar` :

```
<!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("MyUser", "JohnDoe");
%>
<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>
```

6. Créez un fichier `myScript.js` dans le dossier `web\noCacheCustomResources` 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`.
7. Ajoutez au fichier `myScript.js` les valeurs suivantes :

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```

8. Redémarrez le serveur d'applications Web.
9. 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. Le lien suivant doit apparaître : Cliquez sur ce lien pour accéder à la page de connexion de la zone de lancement BI.

### 9.2.5.3.1.2 Pour transmettre le secret partagé par le biais de la variable de session Web

L'exemple de configuration suivant suppose qu'un utilisateur `<JohnDoe>` a été créé sur la plateforme de BI.

Les informations d'utilisateur seront stockées et transmises par le biais de la session Web, tandis que le secret partagé sera transmis par le biais de la variable de session Web. Le fichier est censé se trouver dans le répertoire suivant : `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Vous devez ouvrir et consulter le contenu du fichier. Dans cet exemple de configuration, il est supposé que le secret partagé est le suivant :

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

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 :

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects  
Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web  
\custom.jsp
```

6. Modifiez le contenu du fichier pour inclure les éléments suivants :

```
<!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", "9ecb0778edcff048edae0fcddela5db8211  
2934  
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345  
285b55a0a7"  
request.getSession().setAttribute("MyUser", "JohnDoe");  
%>  
<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>
```

7. Créez le fichier myScript.js dans le répertoire suivant :

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects  
Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web  
\noCacheCustomResources
```

8. Ajoutez à myScript.js les éléments suivants :

```
function goToLogonPage() {  
    window.location = "logon.jsp";  
}
```

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*.

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. Le lien suivant devrait s'afficher :

Cliquez sur ce lien pour accéder à la page de connexion de la zone de lancement BI

### 9.2.5.3.1.3 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 le paramètre `<Realm`  
`className="org.apache.catalina.realm.UserDatabaseRealm"...` et modifiez-le pour la valeur suivante :

```
Realm className="orgapachecatalinarealmMemoryRealm"...
```

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
```

### **i** 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 Entreprise 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 \[page 244\]](#)

[Mappage des groupes LDAP \[page 254\]](#)

### 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 Entreprise pour les utilisateurs LDAP existants et attribuer des alias LDAP aux utilisateurs existants si les noms d'utilisateur correspondent aux noms d'utilisateur Entreprise. 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 \[page 248\]](#)

[Mappage de LDAP par rapport à Windows AD \[page 256\]](#)

[Configuration du plug-in LDAP pour SiteMinder \[page 252\]](#)

## 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.

#### **i** 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.

#### **i** 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.
    - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*  
Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences 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*.

### **i** 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 \[page 248\]](#)

[Configuration du plug-in LDAP pour SiteMinder \[page 252\]](#)

### **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.

### **i** Remarque

Assurez-vous d'ajouter en premier l'hôte principal, suivi des autres hôtes de basculement.

### **i** 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 \[page 244\]](#)

### 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.

## Informations associées

[Pour configurer l'hôte LDAP \[page 244\]](#)

#### 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	<p>Cette action est requise pour l'authentification serveur et mutuelle avec SSL.</p> <ol style="list-style-type: none"><li>1. Obtenez la génération d'un certificat CA par une autorité de certification.</li><li>2. Ajoutez le certificat à votre serveur LDAP.</li></ol> <p>Pour en savoir plus, voir la documentation de votre fournisseur de contenus LDAP.</p>
Certificat de serveur	<p>Cette action est requise pour l'authentification serveur et mutuelle avec SSL.</p> <ol style="list-style-type: none"><li>1. Demandez puis générez un certificat de serveur.</li><li>2. Autorisez le certificat, puis ajoutez-le au serveur LDAP.</li></ol>
cert7.db ou cert8.db, key3.db	<p>Ces fichiers sont requis pour l'authentification serveur et mutuelle avec SSL.</p>

Ressources	Effectuez les actions suivantes avant de démarrer cette tâche
	<ol style="list-style-type: none"> <li>1. Téléchargez l'application certutil qui génère un fichier cert7.db ou cert8.db (selon vos besoins) depuis l'adresse : <a href="https://developer.mozilla.org/en-US/docs/NSS/tools">https://developer.mozilla.org/en-US/docs/NSS/tools</a> .</li> <li>2. Copiez le certificat CA dans le même répertoire que l'application certutil.</li> <li>3. Utilisez la commande suivante pour générer les fichiers cert7.db ou cert8.db, key3.db et secmod.db : <pre>certutil -N -d .</pre> </li> <li>4. Utilisez la commande suivante pour ajouter le certificat CA au fichier cert7.db ou cert8.db : <pre>certutil -A -n &lt;CA_alias_name&gt; -t CT -d . -I cacert.cer</pre> </li> <li>5. Stockez les trois fichiers dans un répertoire de l'ordinateur hébergeant la plateforme de BI.</li> </ol>
cacerts	<p>Ce fichier est requis pour l'authentification serveur ou mutuelle avec SSL pour les applications Java comme la zone de lancement BI.</p> <ol style="list-style-type: none"> <li>1. Recherchez le fichier keytool dans votre répertoire bin Java.</li> <li>2. Utilisez la commande suivante pour créer le fichier cacerts : <pre>keytool -import -v -alias &lt;CA_alias_name&gt; -file &lt;CA_certificate_name&gt; -trustcacerts -keystore</pre> </li> <li>3. Stockez le fichier cacerts dans le même répertoire que les fichiers cert7.db ou cert8.db et key3.db.</li> </ol>
Certificat client	<ol style="list-style-type: none"> <li>1. Créez des demandes client distinctes pour les fichiers cert7.db ou cert8.db et .keystore : <ul style="list-style-type: none"> <li>○ Pour configurer le plug-in LDAP, utilisez l'application certutil pour générer une demande de certificat client.</li> <li>○ Utilisez la commande suivante pour générer la demande de certificat client : <pre>certutil -R -s "&lt;client_dn&gt;" -a -o &lt;certificate_request_name&gt; -d .</pre> </li> </ul> <p>&lt;client_dn&gt; inclut des informations telles que "CN=&lt;client_name&gt;, OU=&lt;org unit&gt;, O=&lt;Companyname&gt;, L=&lt;city&gt;, ST=&lt;province&gt;, and C=&lt;country&gt;".</p> </li> <li>2. Utilisez le CA pour authentifier la demande de certificat. Utilisez la commande suivante pour retrouver le</li> </ol>

Ressources	Effectuez les actions suivantes avant de démarrer cette tâche
	<p>certificat et l'insérer dans le fichier cert7.db ou cert8.db :</p> <pre>certutil -A -n &lt;client_name&gt; -t Pu -d . -I &lt;client_certificate_name&gt;</pre> <p>3. Pour faciliter l'authentification Java avec SSL :</p> <ul style="list-style-type: none"> <li>○ Utilisez l'utilitaire keytool dans le répertoire Java bin pour générer une demande de certificat client.</li> <li>○ Utilisez la commande suivante pour générer une paire clé :</li> </ul> <pre>keytool -genkey - keystore .keystore</pre> <p>4. Après avoir spécifié les informations sur votre client, utilisez la commande suivante pour générer une demande de certificat client :</p> <pre>keytool -certreq -file &lt;certificate_request_name&gt; - keystore .keystore</pre> <p>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 :</p> <pre>keytool -import -v -alias &lt;CA_alias_name&gt; -file &lt;ca_certificate_name&gt; -trustcacerts -keystore .keystore</pre> <p>6. Extrayez la demande de certificat client de l'autorité de certification (CA) et utilisez la commande suivante pour l'ajouter au fichier .keystore :</p> <pre>keytool -import -v -file &lt;client_certificate_name&gt; - trustcacerts -keystore .keystore</pre> <p>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.</p>

# 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.

#### **i** 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](#).

#### **i** 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 \[page 252\]](#)

### 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`

#### **i** 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 \[page 244\]](#)

### 9.3.2.5.1 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.

### 9.3.2.5.2 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 [Authentication](#). Si l'authentification LDAP est configurée, la zone Groupes des membres LDAP mappés affiche les groupes LDAP mappés à la plateforme de BI.

#### i 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.

#### i Remarque

Si vous avez configuré LDAP par rapport à AD, cette procédure mapperait 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 [Authentication](#) 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 existant 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.
  - [Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés](#)  
Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences 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 :

Table 39 :

Situation	Remarques
Plusieurs domaines lors du pointage vers le contrôleur de domaine de catalogue global	<p>Vous pouvez effectuer un mappage dans :</p> <ul style="list-style-type: none"> <li>○ les groupes universels d'un domaine enfant,</li> <li>○ les groupes du même domaine contenant des groupes universels d'un domaine enfant, et</li> <li>○ les groupes universels inter-domaines.</li> </ul> <p>Vous ne pouvez pas effectuer de mappage dans :</p> <ul style="list-style-type: none"> <li>○ les groupes globaux d'un domaine enfant,</li> <li>○ les groupes locaux d'un domaine enfant,</li> <li>○ les groupes du même domaine contenant un groupe global du domaine enfant, et</li> <li>○ les groupes globaux inter-domaines.</li> </ul> <p>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.</p>
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.

#### **i** 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.

Table 40 :

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.  <b>i Remarque</b> Utilisez la dernière version du client Kerberos V5. Ajoutez les dossiers <code>bin</code> et <code>lib</code> aux variables d'environnement <code>PATH</code> et <code>LD_LIBRARY_PATH</code> .
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.

### i 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
```

### i 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.

Table 41 :

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
-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 plateforme 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.

#### i 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/krb5.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 principal
08/10/11 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.

#### **i** 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)*.

#### **i** 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

Table 42 :

<code>&lt;nomsia&gt;</code>	Nom du Server Intelligence Agent
<code>&lt;service &gt;</code>	Nom du compte de service utilisé pour exécuter la plateforme de BI
<code>NOM_DOMAINE_DNS</code>	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 \[page 244\]](#)

### 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`.

#### **i** 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>";
};
```

#### **i** 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 \[page 244\]](#)

[Mappage des groupes LDAP \[page 254\]](#)

## 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.
- Bien que Windows 2008 soit une plateforme prise en charge pour l'authentification Kerberos et l'authentification NTLM, il est possible que certaines applications de la plateforme de BI n'utilisent qu'une méthode d'authentification spécifique. 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

### **i** 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.

### **i** 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 -a` 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 -a BICMS/service_account_name.domain.com serviceaccountname
setspn -a HTTP/<nomserveur> <nomservice>
setspn -a HTTP/<nomserveur.domaine.com> <nomservice>
setspn -a HTTP/<adresse ip du serveur> <nomservice>
```

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/<nomserveur>.DOMAIN.com
HTTP/<nomserveur>
<nomserveur>/<nomservice>DOMAIN.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.domain.com
HTTP/Tomcat HTTP/Tomcat.domain.com
HTTP/Load_Balancer.domain.com
```

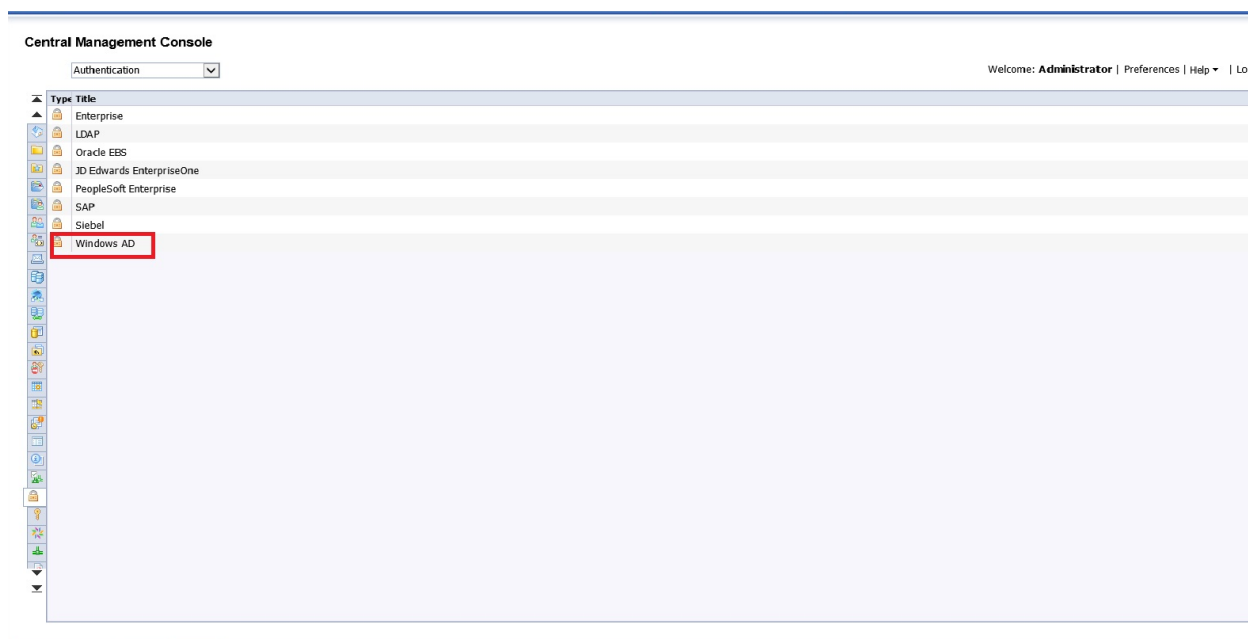
Une fois créé, des droits doivent être affectés au compte de service et celui-ci doit être ajouté au groupe Administrateurs local du serveur. Le SPN servira à importer des groupes AD dans la section suivante.

## 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 uniquement 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.
- 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.

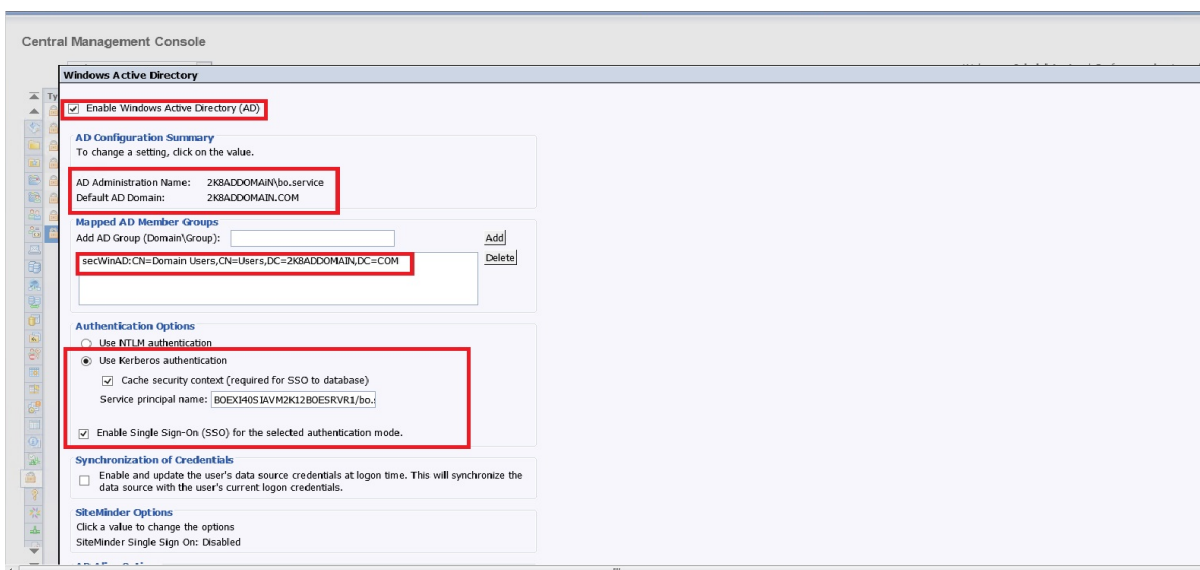
- Vous vous êtes assuré que le SPN contenant le nom de l'ordinateur sur lequel s'exécute le SIA a été ajouté au compte de service.

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=NomGroupe, ....., dc=NomDomaine, 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. Sous *Options d'authentification*, sélectionnez *Utiliser l'authentification Kerberos*.
10. 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.

11. 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.

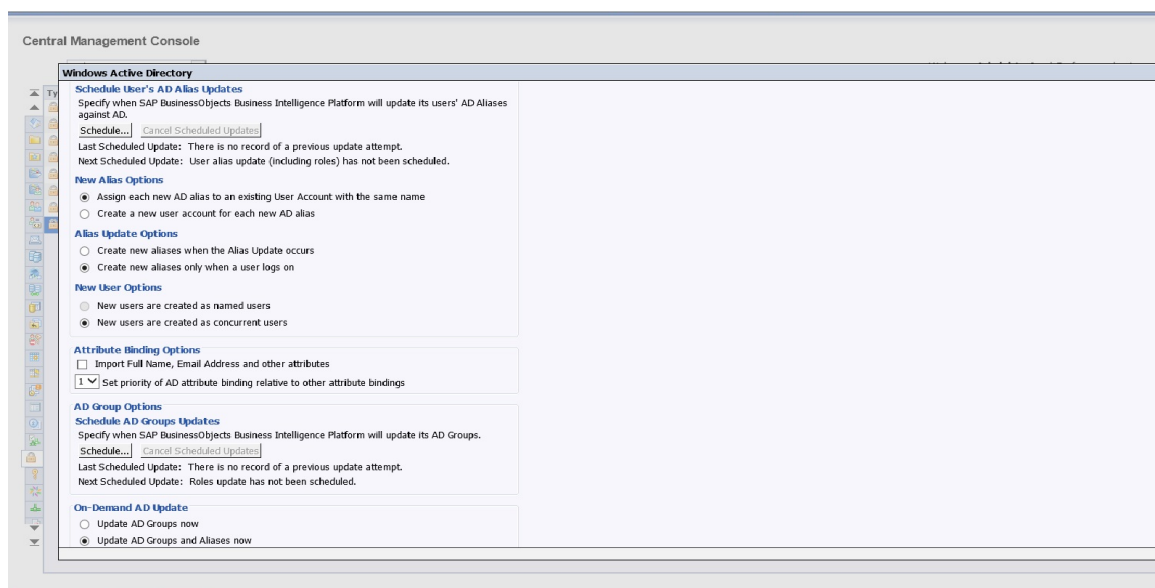
12. Si votre configuration requiert une connexion unique à la base de données, sélectionnez [Contexte de sécurité de la mémoire cache](#).

## 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.

13. 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.
14. 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.
15. 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.
- *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.

16. 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.

17. 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.

18. 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](#).

19. 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](#).

20. 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 \[page 277\]](#)

### 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.

#### **i** 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 :

Table 43 :

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

propagées sur la plateforme de BI par le plug-in AD. Les comptes créés, supprimés ou désactivés dans AD le sont aussi sur 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 : l'alias AD est mis à jour.
- 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.

#### **i** 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.

#### **i** 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.

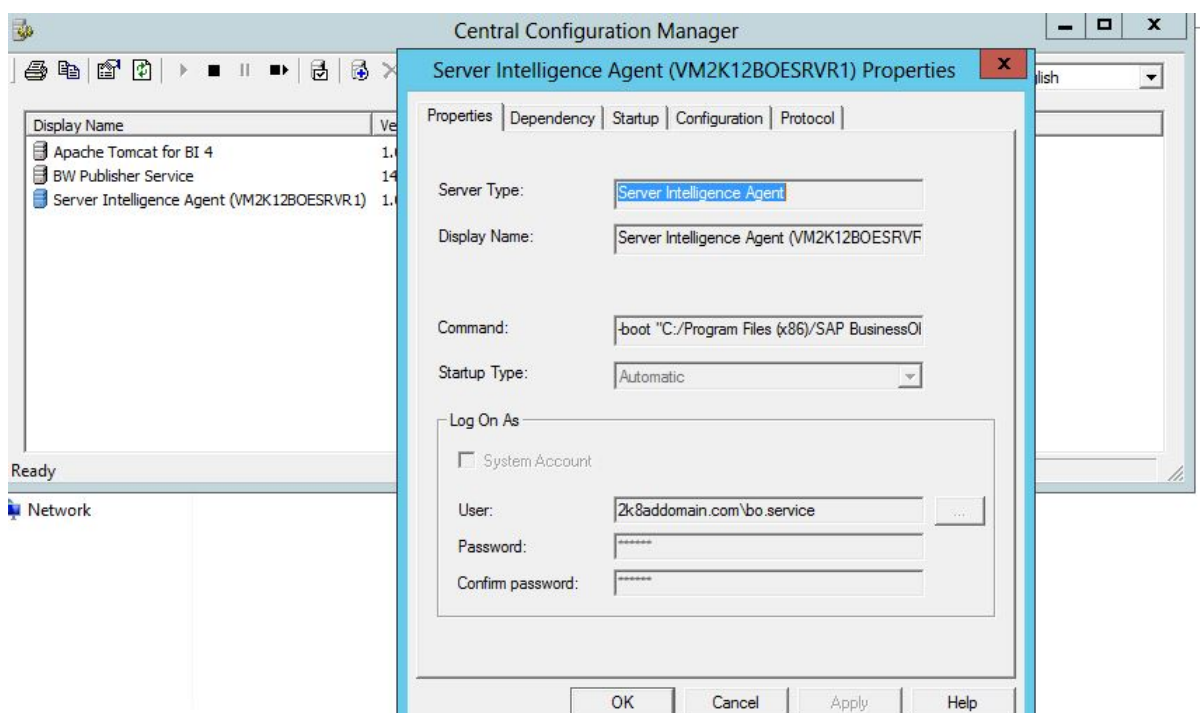
Effectuez cette tâche pour tout SIA (Server Intelligence Agent) exécutant les services utilisés par le compte de service.

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. Cliquez sur *Démarrer* > *Panneau de configuration* > *Outils d'administration* > *Stratégie de sécurité locale*.
7. Développez *Stratégies locales*, puis cliquez sur *Attribution des droits utilisateur*.
8. Cliquez deux fois sur *Agir en tant que partie du système d'exploitation*.
9. Cliquez sur *Ajouter*, saisissez le nom du compte de service créé, puis cliquez sur *OK*.
10. 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.

11. Redémarrez le SIA.
12. 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`.

#### **i** 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 autre emplacement, mais vous devrez le spécifier dans vos options Java. Pour en savoir plus sur `krb5.ini`, consultez la page <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.

Table 44 :

DOMAINE.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 correspondre à tout domaine 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	<b>Krb5LoginModule</b>
Nom de la classe	<b>com.sun.security.auth.module.Krb5LoginModule</b>

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 **Authentication** 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 Oracle Application Server

Si vous utilisez Kerberos avec Oracle Application Server, vous devez modifier les options Java pour indiquer l'emplacement du fichier de configuration Kerberos.

1. Connectez-vous à la console d'administration d'Oracle Application Server.
2. Cliquez sur le nom de l'instance OC4J qui exécute les applications de la plateforme de BI.
3. Sélectionnez [Server Properties \(propriétés du serveur\)](#).
4. Accédez à la section Multiple VM Configuration (configuration VM multiple).
5. Dans la section Command Line Options (options de ligne de commande), ajoutez le texte suivant à la fin du champ de texte [Java Options \(options Java\)](#) : `-Djava.security.krb5.conf=C:/XXXX/krb5.ini` en remplaçant XXXX par l'emplacement de stockage du fichier.
6. Redémarrez votre instance d'OC4J.

### 9.4.5.1.3.5 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.

## 9.4.5.14 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 .
  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.

## 9.4.5.15 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 pré-requises 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. Accédez à l'une des applications et sélectionnez 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 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 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

Deux 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 :

Table 45 :

Paramètre	Description
<code>-out</code>	Spécifie le nom du fichier <code>keytab</code> Kerberos à générer.

Paramètre	Description
-princ	<p>Spécifie le nom principal utilisé pour le compte de service au format SPN :&lt; <b>MYSIAMYSERVER</b>&gt;/&lt; <b>sbo.service.domain.com</b>&gt;@&lt; <b>DOMAIN</b>&gt;.COM, où &lt; <b>MYSIAMYSERVER</b>&gt; est le nom du Service Intelligence Agent spécifié dans le CCM (Central Configuration Manager).</p> <div> <p><b>i Remarque</b></p> <p>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.</p> <p><b>➔ Conseil</b></p> <p>Le SPN doit être unique dans la forêt dans laquelle il est enregistré. Pour vérifier, utilisez l'outil de support Windows <code>Ldp.exe</code> pour rechercher le SPN.</p> </div>
-pass	Indique le mot de passe utilisé par le compte de service.
-ptype	<p>Spécifie le type principal.</p> <pre>-ptype KRB5_NT_PRINCIPAL</pre>
-crypto	<p>Spécifie le type de cryptage à utiliser avec le compte de service :</p> <pre>-crypto RC4-HMAC-NT</pre>

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 \(Kerberos uniquement\)](#).



### 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*.

#### **i** 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.

1. Sauvegardez ce fichier : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\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 `<REPINSTALL>\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 `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

#### **i** 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 : `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\classes\dsweb.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>/dswebobje/services/Session`.  
Exemple : `http://BI4:8080/dswebobje/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 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.

## 9.4.6.2.7 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.

### 9.4.6.2.7.1 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.

## 9.4.6.2.7.2 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.

## 9.4.6.2.8 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.

### 9.4.6.2.9 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.

#### 9.4.6.2.9.1 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.

##### **i** 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

#### **i** 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.
  - [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.com 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.d11`) 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 droits via les 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 :

Table 46 :

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

Objet d'autorisation	Champ	Valeur
	Nom de RFC à protéger (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUN-TIME, 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)	<p>*</p> <div> <p><b>i Remarque</b></p> <p>Pour plus de sécurité, vous pouvez répertorier explicitement les groupes d'utilisateurs dont les membres doivent accéder à la plateforme de BI.</p> </div>

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.

## 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
<a href="#">Activer l'authentification SAP</a>	Décochez cette case pour désactiver l'authentification SAP.

Paramètre	Description
	<p><b>i Remarque</b></p> <p>Pour désactiver l'authentification SAP d'un système SAP spécifique, cochez la case <i>Désactivé</i> du système en question dans l'onglet <i>Système d'autorisation</i>.</p>
<i>Racine du dossier Contenu</i>	<p>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.</p> <p>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.</p>
<i>Système par défaut</i>	<p>Sélectionnez un système d'autorisation SAP pour la plateforme de BI à contacter pour authentifier les utilisateurs qui essaient de se connecter avec des références de connexion SAP mais sans indiquer de système SAP.</p> <p><b>i Remarque</b></p> <p>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.</p>
<i>Nombre maximal d'échecs d'accès au système d'autorisation</i>	<p>Saisissez le nombre de fois que la plateforme de BI doit essayer de contacter un système SAP pour satisfaire les demandes d'authentification.</p> <p>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.</p> <p><b>i Remarque</b></p> <p>Utilisez ce paramètre avec l'option <i>Laisser le système d'autorisation désactivé [secondes]</i> 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</p>



Paramètre	Description
	<p>systèmes SAP indisponibles doivent être interrompues puis reprises.</p>
<i>Laisser le système d'autorisation désactivé [secondes]</i>	<p>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.</p> <p>Par exemple, si vous saisissez la valeur 3 pour <i>Nombre maximal d'échecs d'accès au système d'autorisation</i>, la plateforme de BI ne permet que trois tentatives (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.</p>
<i>Nombre maximal de connexions simultanées par système</i>	<p>Indiquez le nombre maximal de connexions qui peuvent être ouvertes simultanément sur votre système SAP.</p> <p>Par exemple, si vous saisissez 2, la plateforme de BI garde deux connexions ouvertes sur SAP.</p>
<i>Nombre d'utilisations par connexion</i>	<p>Indiquez le nombre d'opérations que vous autorisez par connexion au système SAP.</p> <p>Par exemple, si l'option <i>Nombre maximal de connexions simultanées par système</i> est définie sur 2 et que l'option <i>Nombre d'utilisations par connexion</i> est définie sur 3, la plateforme de BI ferme et redémarre cette connexion lorsque trois sessions se trouvent sur une connexion.</p>
<i>Utilisateurs simultanés et Utilisateurs nommés</i>	<p>Indiquez si les comptes des nouveaux utilisateurs utilisent des licences Utilisateur nommé ou utilisateur simultané.</p> <p>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.</p> <p>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.</p>

Paramètre	Description
	<p><b>i Remarque</b></p> <p>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.</p>
<i>Importer le nom complet, l'adresse électronique et d'autres attributs</i>	<p>Spécifiez un niveau de priorité pour le plug-in d'authentification SAP.</p> <p>Les noms complets et les descriptions des comptes SAP sont importés et stockés avec les objets utilisateur dans la plateforme de BI.</p>
<i>Rendre la liaison d'attributs SAP prioritaire par rapport aux autres liaisons d'attributs</i>	<p>Spécifie une priorité pour la liaison des attributs utilisateur SAP (nom complet et adresse électronique).</p> <p>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.</p>

Définissez les options suivantes pour configurer le service de connexion unique SAP :

Paramètre	Description
<i>ID système</i>	Identificateur système fourni par la plateforme de BI au système SAP lors de l'exécution du service de connexion unique SAP.
<i>Parcourir</i>	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.
<i>Mot de passe du stockage de clés</i>	Fournissez le mot de passe requis pour accéder au fichier de stockage de clés.
<i>Mot de passe de la clé privée</i>	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
<i>Alias de clé privée</i>	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.

#### **i** 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 `<numéroport>` 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.

- 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 :

Table 47 :

Schéma de périodicité	Description
<i>Toutes les heures</i>	La mise à jour s'exécutera toutes les heures. Vous indiquez l'heure de début ainsi que les dates de début et de fin.
<i>Tous les jours</i>	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.
<i>Toutes les semaines</i>	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.
<i>Tous les mois</i>	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.
<i>Nième jour du mois</i>	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.
<i>1er lundi du mois</i>	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.
<i>Dernier jour du mois</i>	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.
<i>Jour X de la Nième semaine du mois</i>	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.
<i>Calendrier</i>	La mise à jour s'exécutera aux dates spécifiées dans un calendrier précédemment créé.

- 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.

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 \[page 315\]](#)

### 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. Elle est disponible pour Windows et UNIX.

Pour en savoir plus sur la bibliothèque cryptographique, 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.

## Client/serveur SNC

Dans client SNC, un identificateur de nom SNC est mappé à un (ou plusieurs) noms d'utilisateur SAP dans SU01. Lorsqu'une requête de connexion est envoyée, le nom SNC et le nom SAP sont transmis au système SAP. Toutefois, aucun mot de passe n'est envoyé. Si le nom SNC est mappé au nom SAP indiqué, la connexion est autorisée. Voici une chaîne de connexion côté client pour une connexion à l'hôte d'applications direct :

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

L'utilisateur SAP USER123 doit être mappé à p:CN=Utilisateur,O=Société,C=US dans SU01 pour que cette tentative de connexion réussisse. Sur le serveur SNC, en revanche, il n'est pas nécessaire de mapper explicitement l'identificateur de nom SNC avec le nom d'utilisateur SAP. Au lieu de cela, le nom SNC est configuré au sein de la transaction SNC0 afin de pouvoir établir une connexion de type emprunt d'identité pour « tout » utilisateur sans avoir à fournir le mot de passe de cet utilisateur. Par exemple :

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

La connexion d'identité du serveur SNC ou connexion via ID externe propose beaucoup plus de possibilités que la connexion client. Cette connexion permet d'accéder à n'importe quel compte utilisateur SAP du système. Parmi les autres options de connexion ID externe, citons Logon Tickets et les certificats client X.509.

## 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, ainsi que le type de SNC requis pour chaque domaine de responsabilités.

Serveur	Type de SNC	Domaines de responsabilités
Serveur d'applications Web	client	Liste de rôles de l'authentification SAP
Service BW Publisher	serveur	Personnalisation et listes de sélection des paramètres dynamiques de Crystal Reports



Serveur	Type de SNC	Domaines de responsabilités
CMS	client	Listes de mots de passe, de tickets, de vérification des appartenances du rôle et d'utilisateurs
Page Server	serveur	Affichage à la demande de Crystal Reports
Job Server	serveur	Planification de Crystal Reports
Web Intelligence Processing Server	serveur	Affichage et planification des rapports Web Intelligence et des invites de liste de valeurs
Service MDAS (Multi-Dimensional Analysis Service)	serveur	Analyse

#### **i** Remarque

Le serveur d'applications Web et le CMS utilisent le SNC client et requièrent par conséquent un mappage explicite du nom SNC au nom d'utilisateur SAP. Ceci est indiqué dans la transaction SU01 ou SM30 pour le tableau USRACL.

## 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.

#### **i** 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*.

- 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
<b>CN</b>	Nom usuel	Nom usuel du propriétaire du certificat.
<b>OU</b>	Unité organisationnelle	EP pour Equipe produits, par exemple.
<b>O</b>	Organisation	Nom de l'organisation pour laquelle le certificat a été émis.
<b>C</b>	Pays	Pays dans lequel se situe l'organisation.

Par exemple, pour R21 : **p:CN=R21, OU=EP, O=BOBJ, C=CA**

#### **i** 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.

- Entrez les valeurs de profil suivantes, en utilisant les valeurs correspondant à votre système SAP.

Variable de profil	Valeur
<b>ssf/name</b>	<b>SAPSECULIB</b>
<b>ssf/ssfapi_lib</b>	Chemin complet de la bibliothèque cryptographique SAP
<b>sec/libsapsecu</b>	Chemin complet de la bibliothèque cryptographique SAP
<b>snc/gssapi_lib</b>	Chemin complet de la bibliothèque cryptographique SAP
<b>snc/identity/as</b>	DN de votre système SAP

- Redémarrez l'instance SAP.
- 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.
- 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.
- Cliquez sur **OK**.
- Pour attribuer un mot de passe au PSE de la SNC, cliquez sur l'icône représentant un verrou.

#### **i** 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.

- Enregistrez les modifications.

### **i** 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
<code>snc/accept_insecure_rfc</code>	1
<code>snc/accept_insecure_r3int_rfc</code>	1
<code>snc/accept_insecure_gui</code>	1
<code>snc/accept_insecure_cplic</code>	1
<code>snc/permit_insecure_start</code>	1
<code>snc/data_protection/min</code>	1
<code>snc/data_protection/max</code>	3
<code>snc/enable</code>	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_cplic` 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 \[page 320\]](#)

[Pour générer un PSE \(environnement de sécurité personnelle\) \[page 321\]](#)

[Pour configurer les serveurs de la plateforme de Business Intelligence \[page 322\]](#)

[Pour configurer l'accès au PSE \[page 322\]](#)

[Pour configurer les paramètres SNC d'authentification SAP \[page 323\]](#)

[Utilisation de groupes de serveurs \[page 324\]](#)

### 9.5.6.3.1 Pour configurer l'environnement

La plateforme de BI comprend une bibliothèque cryptographique SAP par défaut. Si vous l'utilisez, 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 \[page 317\]](#)

### 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 -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 SNC0.

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 (ayant pour préfixe **p:**) que vous avez fourni lors de la création de votre PSE de la plateforme de BI (à l'étape 2).
- Les cases [Entrée pour RFC activée](#) et [Entrée pour ID ext. activée](#) sont cochées :

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 <MonCertSAP.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 \[page 322\]](#)

### 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
\bojsapproc.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 (3801010000001Z)
      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.

#### **i** 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.

8. Saisissez le nom SNC du système SAP sous *Paramètres d'authentification mutuelle*.

Le format de nom SNC dépend de la bibliothèque SNC. En ce qui concerne le nom distinctif, selon la bibliothèque de cryptographie SAP, il est recommandé de suivre les conventions d'appellation LDAP et d'ajouter 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 \[page 311\]](#)

### 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 [Autoriser Secure Network Communication \(SNC\)](#) 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 et le CMS doivent être sous le même type de système d'exploitation et avoir le même chemin d'accès à la bibliothèque crypto.
6. Sélectionnez un niveau de protection dans le champ [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 du 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](#).  
Lorsque plusieurs noms SNC sont configurés, laissez ce champ vide.
9. Cliquez sur [Mettre à jour](#).
10. Cliquez dans l'onglet [Systèmes d'autorisation](#) de la page [Authentification SAP](#).  
L'option [Nom SNC](#) apparaît sous l'option [Langue](#).
11. Dans le champ [Nom SNC](#), saisissez le nom SNC que vous avez configuré sur le serveur SAP BW.  
Ce nom doit être identique à celui utilisé pour configurer le système SAP afin qu'il sécurise la plateforme de BI.  
  
Si vous utilisez la structure Insight to Action pour activer l'interface Rapport-Rapport, il pourrait s'écouler une dizaine de minutes avant que SNC soit activé où que les modifications apportées à ses paramètres prennent effet. Pour déclencher une mise à jour immédiate, redémarrez le serveur de traitement adaptatif exécutant le service Insight to Action.

## Informations associées

[Connexion aux systèmes d'autorisation de SAP \[page 305\]](#)

### 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 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.

### i 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

Le programme `PKCS12Tool` permet de générer les fichiers de stockage de clés et les certificats requis pour configurer la connexion unique à la base de données SAP. Le tableau suivant répertorie les emplacements par défaut de `PKCS12Tool.jar` pour chaque plateforme prise en charge :

Plateforme	Emplacement par défaut
Windows	<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

1. Lancez une invite de commande et accédez au répertoire où se trouve le programme `PKCS12Tool`.
2. Pour générer le fichier de stockage de clés avec les paramètres par défaut, exécutez la commande suivante :

```
java -jar PKCS12Tool.jar
```

Les fichiers `cert.der` et `keystore.p12` sont générés dans le même répertoire. Les fichiers contiennent les valeurs par défaut suivantes :

Paramètre	Par défaut
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365

Paramètre	Par défaut
-cert	cert.der

### ➔ Conseil

Pour remplacer les valeurs par défaut, exécutez l'outil avec le paramètre -?. Le message suivant s'affiche :

```
Usage: PKCS12Tool <options>
       -keystore <filename(keystore.pl2)>
       -alias <key entry alias(myalias)>
       -storepass <keystore password(123456)>
       -dname <certificate subject DN(CN=CA)>
       -validity <number of days(365)>
       -cert <filename (cert.der)>
           (No certificate is generated when importing a keystore)
       -disablefips
       -importkeystore <filename>
```

Vous pouvez utiliser les paramètres pour remplacer les valeurs par défaut.

## 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.

### i 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
<a href="#">Mot de passe du stockage de clés</a>	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.
<a href="#">Mot de passe de la clé privée</a>	Fournissez le mot de passe requis pour accéder au certificat correspondant au fichier de stockage de clés. Ce

Champ	Informations requises
	mot de passe a été spécifié lors de la création du certificat du fichier de stockage de clés.
<i>Alias de clé privée</i>	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 :

Table 48 :

Pilote	Nom affiché
Pilote du magasin de données opérationnelles	<i>crdb_ods</i>
pilote Open SQL	<i>crdb_opensql</i>
Pilote InfoSet	<i>crdb_infoset</i>
pilote BW MDX Query	<i>crdb_bwmdx</i>

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 :

<b>crdb_ods</b>	Pour activer le pilote ODS
<b>crdb_opensql</b>	Pour activer le pilote Open SQL
<b>crdb_bwmdx</b>	Pour activer le pilote SAP BW MDX Query
<b>crdb_infoset</b>	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 : `"<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <serveurpeoplesoft>.cer -keystore cacerts -alias <serveurpeoplesoft>`.
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. A 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.
- *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.

#### **i** 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 :

Table 49 :

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 commencera, 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](#).

## 9.6.5 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 \[page 342\]](#).

### 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 `crpsepmsecuritybridge.sh` (sous Unix).

### i 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](#).

### i Remarque

Le SDK PeopleSoft EPM se trouve généralement sur le serveur PeopleSoft dans `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

### i 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 :

Table 50 :

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 :

Table 51 :

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](#).

**i** 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.

**i** 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](#).

**i** 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](#).

#### **i** 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.

#### **i** 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.

#### **i** 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 :

Table 52 :

Paramètre	Description
classpath	<p>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.</p> <p>Les chemins de classes requis sont pour le fichier <code>com.peoplesoft.epm.pf.jar</code> et les fichiers .jar du pilote JDBC (Java Database Connectivity).</p>

Paramètre	Description
db.driver.name	Le nom du pilote JDBC utilisé pour se connecter à la base de données PeopleSoft (par exemple, <code>com.microsoft.jdbc.sqlserver.SQLServerDriver</code> ).
db.connect.str	La chaîne de connexion JDBC utilisée pour se connecter à la base de données PeopleSoft (par exemple, <code>jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO</code> ).
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 <a href="#">Définition d'objets gérés [page 339]</a> .
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.

Paramètre	Description
peoplesoft.role.n	<p>La liste de rôles PeopleSoft gérés. Pour en savoir plus, voir <a href="#">Définition d'objets gérés [page 339]</a>.</p> <p><b>&lt;n&gt;</b> est un entier, et chaque entrée occupe une propriété avec le préfixe peoplesoft.role.</p> <div> <p><b>i Remarque</b></p> <p><b>&lt;n&gt;</b> est en base 1.</p> </div> <p>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 people-soft.role dans le fichier réponse.</p>
mapped.universe.n	<p>La liste des univers que la passerelle de sécurité doit mettre à jour. Pour en savoir plus, voir <a href="#">Définition d'objets gérés [page 339]</a>.</p> <p><b>&lt;n&gt;</b> est un entier, et chaque entrée occupe une propriété avec le préfixe mapped.universe.</p> <div> <p><b>i Remarque</b></p> <p><b>&lt;n&gt;</b> est en base 1.</p> </div> <p>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.</p>
log4j.appenders.file.File	Fichier journal enregistré par la passerelle de sécurité.

Paramètre	Description
log4j.*	<p>Propriétés log4j par défaut requises pour que log4j puisse fonctionner correctement :</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.RollingFile Appender</p> <p>log4j.appender.file.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.file.MaxFileSize=5000KB</p> <p>log4j.appender.file.MaxBackupIndex=100</p> <p>log4j.appender.file.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n</p> <p>log4j.appender.stdout=org.apache.log4j.ConsoleAppender</p> <p>log4j.appender.stdout.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.stdout.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n</p>
peoplesoft classpath	<p>Chemin de classes des fichiers .jar de l'API (Application Programming Interface) PeopleSoft EPM.</p> <p>Ce paramètre est facultatif.</p>
enterprise.classpath	<p>Le chemin de classes des fichiers .jar du SDK de la plateforme de BI.</p> <p>Ce paramètre est facultatif.</p>
db.driver.type	<p>Type de la base de données PeopleSoft. Ce paramètre peut avoir l'une des valeurs suivantes :</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>Personnalisé</p> <p>La valeur Personnalisé peut être utilisée pour spécifier des bases de données dont le type ou la version n'est pas reconnu.</p> <p>Ce paramètre est facultatif.</p>
sql.db.class.location sql.db.host sql.db.port sql.db.database	<p>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.</p> <p>Ces paramètres peuvent être utilisés uniquement si db.driver.type a pour valeur Microsoft SQL Server 2000.</p> <p>Ces paramètres sont facultatifs.</p>

Paramètre	Description
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.drivename 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 la zone [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 la zone [Domaine JD Edwards EnterpriseOne](#), saisissez le nom, l'hôte et le port utilisés pour vous connecter à votre environnement JD Edwards EnterpriseOne, saisissez un nom pour l'environnement et cliquez sur [Ajouter](#).
11. 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. A 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.
  - *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 :

Table 53 :

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](#).

## 9.8 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 "raquno") et que vous exécutez votre environnement de production avec un compte utilisateur pour Raoul Aquino (nom d'utilisateur "raquno"), 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. A 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.
  - *Les nouveaux utilisateurs sont créés en tant qu'utilisateurs simultanés*  
Les nouveaux comptes d'utilisateur sont configurés de manière à utiliser des licences 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

Si vous disposez d'un grand nombre de rôles, vous pouvez utiliser le champ *Rechercher les rôles commençant par* : pour affiner votre recherche. 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 :

Table 54 :

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 commencera, 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](#).

### **i** 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 \[page 360\]](#)

### 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. A 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.

- [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](#).

- Sélectionnez les applications que les utilisateurs peuvent utiliser dans le cadre de leur nouveau rôle dans la liste [Application](#).
- Sélectionnez les applications Oracle, les fonctions, les rapports ainsi que les programmes simultanés que les utilisateurs peuvent utiliser dans la liste [Responsabilité](#).
- Sélectionnez le groupe de sécurité auquel le nouveau rôle est affecté dans le groupe Sécurité de la liste [Groupe de sécurité](#).
- A 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 :

Table 55 :

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.
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.

#### **i** 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](#).

## 10 Administration du serveur

### 10.1 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](#).

Table 56 :

Option de l'arborescence de navigation	Description
<a href="#">Liste des serveurs</a>	Affiche la liste complète des serveurs du déploiement.
<a href="#">Liste des groupes de serveurs</a>	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.
<a href="#">Groupes de serveurs</a>	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.
<a href="#">Noeuds</a>	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
<a href="#">Catégories de service</a>	<p>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 :</p> <ul style="list-style-type: none"> <li>• <a href="#">Services de connectivité</a></li> <li>• <a href="#">Services principaux</a></li> <li>• <a href="#">Services Crystal Reports</a></li> <li>• <a href="#">Services de fédération de données</a></li> <li>• <a href="#">Services de gestion des promotions</a></li> <li>• <a href="#">Analysis Services</a></li> <li>• <a href="#">Services Web Intelligence</a></li> <li>• <a href="#">Services Dashboards</a></li> </ul> <p>Sélectionnez une catégorie de service dans la liste de navigation pour visualiser ou gérer les serveurs appartenant à cette catégorie.</p> <div> <p><b>i Remarque</b></p> <p>Un serveur peut héberger des services appartenant à plusieurs catégories de services. Par conséquent, un serveur peut apparaître dans plusieurs catégories de services.</p> </div>
<a href="#">Statut du serveur</a>	<p>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 <a href="#">Statut du serveur</a> pour déterminer rapidement si certains de vos serveurs présentent un état anormal. Les états de serveur possibles sont les suivants :</p> <ul style="list-style-type: none"> <li>• <a href="#">Arrêté</a></li> <li>• <a href="#">Démarrage en cours</a></li> <li>• <a href="#">Initialisation en cours</a></li> <li>• <a href="#">Exécution en cours</a></li> <li>• <a href="#">Arrêt en cours</a></li> <li>• <a href="#">A démarré avec des erreurs</a></li> <li>• <a href="#">Echec</a></li> <li>• <a href="#">Attente des ressources</a></li> </ul>

## 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.

Table 57 :

Colonne du volet Détails	Description
<i>Nom du serveur</i> ou <i>Nom</i>	Affiche le nom du serveur.
<i>Etat</i>	<p>Affiche le statut actuel du serveur. Vous pouvez effectuer un tri par état de serveur à l'aide de la liste <i>Statut du serveur</i> dans l'arborescence. Les états de serveur possibles sont les suivants :</p> <ul style="list-style-type: none"><li>• <i>Arrêté</i></li><li>• <i>Démarrage en cours</i></li><li>• <i>Initialisation en cours</i></li><li>• <i>Exécution en cours</i></li><li>• <i>Arrêt en cours</i></li><li>• <i>A démarré avec des erreurs</i></li><li>• <i>Echec</i></li><li>• <i>Attente des ressources</i></li></ul>
<i>Activé</i>	Indique si le serveur est activé ou désactivé.
<i>Périmé</i>	Si le serveur est marqué comme <i>Périmé</i> , un redémarrage est nécessaire. Par exemple, si vous modifiez certains paramètres du serveur dans l'écran <i>Propriétés</i> du serveur, vous devrez peut-être redémarrer le serveur pour prendre en compte les modifications.
<i>Type</i>	Affiche le type de serveur.
<i>Nom d'hôte</i>	Affiche le nom d'hôte du serveur.
<i>Santé</i>	<p>Indique la santé globale du serveur.</p> <p>Les états de serveur possibles sont les suivants :</p> <ul style="list-style-type: none"><li>• <i>Vert</i> (sain)</li><li>• <i>Orange</i> (attention)</li><li>• <i>Rouge</i> (danger)</li></ul> <p>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 la veille &lt;NOMNŒUD&gt; .CentralManagementServer.</p> <p>Vous pouvez accéder aux détails des veilles sur la page <i>Surveillance</i> dans la CMC : dans l'onglet <i>Liste de veilles</i>, sélectionnez la veille et cliquez sur <i>Modifier</i>. La <i>Règle de mise en garde</i> et la <i>Règle de danger</i> pour la veille s'affichent, qui sont mappées à l'état de santé orange et rouge, respectivement.</p>
<i>PID</i>	Affiche le numéro d'identification unique du processus.

Colonne du volet Détails	Description
<i>Description</i>	Affiche une description du serveur. Vous pouvez modifier cette description dans la page <a href="#">Etat du serveur</a> du serveur.
<i>Date de modification</i>	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.

## 10.2 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 \[page 890\]](#)

## 10.3 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 \[page 882\]](#)

## 10.4 Affichage et modification du statut d'un serveur

### 10.4.1 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 \[page 371\]](#)

[Affichage de l'état des services \[page 371\]](#)

[Démarrage, arrêt et redémarrage d'un serveur \[page 372\]](#)

[Activation et désactivation de serveurs \[page 375\]](#)

[Arrêt d'un Central Management Server \[page 374\]](#)

[Pour démarrer les serveurs automatiquement \[page 374\]](#)

### 10.4.1.1 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.

### 10.4.1.2 Affichage de l'état des services

Si un service échoue, l'état du serveur hôte est défini sur [Démarré avec erreurs](#) (c'est-à-dire qu'au moins un service a démarré correctement) ou [Echoué](#) (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 \[page 370\]](#)

### 10.4.2 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.

Table 58 :

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 \[page 375\]](#)

### 10.4.2.1 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*.

#### **i** 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*.

## 10.4.2.2 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.

## 10.4.2.3 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.

## 10.4.3 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.

#### **i** 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 \[page 405\]](#)

[Clonage des serveurs \[page 377\]](#)

[Mise en cluster de Central Management Servers \[page 379\]](#)

## 10.4.4 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.

#### **i** 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.

## 10.4.4.1 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](#).

## 10.4.4.2 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.

## 10.5 Ajout, clonage ou suppression de serveurs

### 10.5.1 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*.

#### 10.5.1.1 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 `<NOMNŒUD>.<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.

## 10.5.1.2 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. 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.

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. Par exemple, si vous clonez un CMS sur le même ordinateur, veillez à modifier les paramètres de numéro de port qui ont été copiés depuis le CMS d'origine sur le CMS cloné.

### 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.

## 10.5.1.2.1 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 clonez 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.

### 10.5.1.2.2 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.

#### **i** Remarque

Les paramètres relatifs au numéro de port sont également clonés. Bien souvent, notamment en cas de clonage d'un CMS, vous devrez modifier le numéro de port pour éviter toute confusion entre le serveur d'origine et son clone.

### 10.5.1.3 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](#).

## 10.6 Mise en cluster de Central Management Servers

### 10.6.1 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 \[page 383\]](#)

### 10.6.1.1 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.

#### i 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 \[page 382\]](#)

[Ajout d'un serveur \[page 376\]](#)

[Clonage des serveurs \[page 377\]](#)

[Présentation de la sauvegarde et de la restauration \[page 487\]](#)

## 10.6.1.2 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.

### **i** 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.

## Informations associées

[Utilisation des nœuds \[page 405\]](#)

## 10.6.1.3 Ajout de clusters aux fichiers de propriétés d'application Web

Si vous avez ajouté des CMS supplémentaires à votre déploiement et si vous utilisez un serveur d'applications Java, vous devez modifier le fichier `PlatformServices.properties` dans le répertoire `\webapps\BOE\WEB-INF\config\custom` de votre déploiement d'applications Web.

### 10.6.1.3.1 Pour définir des propriétés de cluster pour l'application Web BOE

1. Accédez au dossier "custom" du fichier `BOE.war` sur l'ordinateur hébergeant les applications Web :  
`<REINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.`

Vous devrez redéployer ultérieurement le fichier `BOE.war` modifié.

2. Créez un fichier dans un éditeur de texte.

### 3. Spécifiez les propriétés de cluster du CMS

Utilisez la propriété `cms.cluster` pour spécifier tous les clusters du déploiement. Les noms de cluster doivent être précédés de caractères @ et séparés par des virgules. Par exemple,

`cms.clusters=@samplecluster,@samplecluster2, @samplecluster3`. Utilisez la propriété `cms.clusters.<[nom du cluster]>` pour spécifier chaque CMS contenu dans le cluster. Par exemple :

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400,cmstwo
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

#### **i** Remarque

Le numéro de port est séparé du nom de CMS par le signe deux-points. Le numéro de port est supposé être 6400, sauf indication contraire.

### 4. Enregistrez le fichier sous le nom suivant .

**PlatformServices.properties**

### 5. Redémarrez le serveur d'applications.

Les nouvelles propriétés ne prennent effet que 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 de Business Intelligence*.

## 10.6.1.4 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.

#### **i** 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.

### 10.6.1.4.1 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.

## 10.6.1.4.2 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 \[page 882\]](#)

## 10.7 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.

## 10.7.1 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.

### 10.7.1.1 Pour créer un groupe de serveurs

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.

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.

## 10.7.2 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.

### 10.7.2.1 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.

## 10.7.2.2 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.
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` + `+cllc` pour sélectionner plusieurs groupes de serveurs.

5. Cliquez sur [OK](#).

## 10.7.3 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.

### 10.7.3.1 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.
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](#).

## 10.7.4 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 souhaitez 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.

### 10.7.4.1 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 \[page 125\]](#)

### 10.7.4.2 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.

## 10.8 Configuration des serveurs de traitement adaptatif (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.  
L'assistant est disponible à partir de la CMC (Central Management Console). Pour en savoir plus sur l'assistant, voir [Introduction à l'Assistant de configuration du système \[page 89\]](#). Pour en savoir plus sur les modèles de déploiement par défaut, voir le document *Modèles de déploiement de la plateforme SAP BusinessObjects BI*, disponible dans l'assistant, mais également dans <http://help.sap.com/bobip41>.
- Utilisez la CMC pour créer et configurer manuellement les APS supplémentaires. Pour en savoir plus, voir [Ajout, clonage et suppression de serveurs \[page 376\]](#).

#### ➔ 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>.

## 10.9 Évaluation des performances du système

### 10.9.1 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

[A propos de la surveillance \[page 666\]](#)

### 10.9.2 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.

#### i Remarque

Vous pouvez visualiser uniquement les métriques des serveurs en cours d'exécution.

## 10.9.2.1 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 \[page 393\]](#)

[A propos de l'annexe Métriques du serveur \[page 986\]](#)

## 10.9.3 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.

### 10.9.3.1 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](#).

## 10.9.4 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.

### **i** 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 `SYSLDGD` 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.

## 10.10 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.

### **i** 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 \[page 402\]](#)

[Pour modifier les propriétés d'un serveur \[page 393\]](#)

[Recréation de la base de données système du CMS \[page 441\]](#)

[Sélection d'une base de données CMS \(nouvelle ou existante\) \[page 439\]](#)

### 10.10.1 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](#).

#### **i** 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.

### 10.10.2 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](#).

#### **i** Remarque

Vous êtes 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.

## 10.10.3 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 \[page 394\]](#)

[Pour appliquer un modèle de configuration à un serveur \[page 395\]](#)

## 10.10.3.1 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 \[page 395\]](#)

### 10.10.3.2 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 \[page 394\]](#)

### 10.10.3.3 Pour restaurer les valeurs par défaut du système

Vous souhaitez 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.

## 10.11 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.



## 10.11.1 Options d'environnement réseau

La plateforme de BI prend en charge les trafics réseau IPv6 (Internet Protocol version 6) et IPv4 (Internet Protocol version 4). 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 IPv6 : tous les composants client et serveur s'exécutent uniquement avec le protocole IPv6.
- Réseau mixte IPv6/IPv4 : les composants client et serveur peuvent s'exécuter avec les protocoles IPv6 et IPv4.

### 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.

### 10.11.1.1 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 IPv6, 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 de nœud uniquement IPv6. 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.

## 10.11.2 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
<i>Affecter automatiquement</i>	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.

Option	Description
	<p><b>i Remarque</b></p> <p>Il est recommandé de cocher la case <i>Affecter automatiquement</i> 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 <i>Guide d'administration de la plateforme de Business Intelligence</i>.</p>
<i>Nom d'hôte</i>	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.
<i>Adresse IP</i>	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.

### **i** 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 \[page 194\]](#)

[Configuration d'un ordinateur multi-résident \[page 399\]](#)

[Pour dépanner plusieurs interfaces réseau \[page 401\]](#)

## 10.11.2.1 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
<b>Affecter automatiquement</b>	Le serveur sera lié à l'une des interfaces réseau disponibles.
<b>Nom d'hôte</b>	Saisissez le nom d'hôte de l'interface réseau sur laquelle le serveur écoute les requêtes.
<b>Adresse IP</b>	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.  <b>i Remarque</b> 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.

## 10.11.3 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 401]

### 10.11.3.1 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.

## 10.11.3.2 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 405]

## 10.11.3.3 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.

## 10.11.4 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.

Table 59 :

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). Utilisez la même interface réseau que le port du serveur de noms. Lorsque l'option <a href="#">Affecter automatiquement</a> 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 <a href="#">Affecter automatiquement</a> 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

## 10.11.4.1 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.

### **i** 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](#).

## 10.11.4.2 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 la 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.

### 10.11.4.3 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 .
4. Sélectionnez le nœud qui héberge le CMS que vous souhaitez modifier, puis appuyez sur la touche .
5. Sélectionnez **3 - Modifier un CMS local**, puis appuyez sur .
- Une liste des CMS hébergés sur le nœud s'affiche.
6. Sélectionnez le CMS à modifier, puis appuyez sur .
7. Saisissez le nouveau numéro de port du CMS et appuyez sur .
8. Spécifiez si vous voulez que le CMS démarre automatiquement en même temps que le SIA, puis appuyez sur la touche .
9. Saisissez les arguments de la ligne de commande pour le CMS ou acceptez les arguments actuels, puis appuyez sur la touche .
10. Saisissez **quit** pour fermer le script.
11. Démarrez le SIA avec le script `ccm.sh` et attendez le démarrage des serveurs.

### 10.11.4.4 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.



## 10.11.4.5 Pour changer le port utilisé par un serveur pour accepter les requêtes

### i 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.

## 10.12 Gestion des nœuds

### 10.12.1 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.

### i 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.

### i 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).

## 10.12.1.1 Variables

Variable	Description
<REPINSTALL>	Répertoire où est installée la plateforme SAP BusinessObjects Business Intelligence.  Sous Windows : C:\Program Files (x86)\SAP BusinessObjects
<REPSRIPT>	Répertoire où se trouvent les scripts de gestion des nœuds. <ul style="list-style-type: none"><li>• Sous Windows : &lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts</li><li>• Sous Unix : &lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;PLATEFORME64&gt;/scripts</li></ul>
<PLATEFORME32>	Nom de votre système d'exploitation Unix. Les valeurs acceptées sont les suivantes : <ul style="list-style-type: none"><li>• aix_rs6000</li><li>• linux_x86</li><li>• solaris_sparc</li><li>• win32_x86</li></ul>
<PLATEFORME64>	Nom de votre système d'exploitation Unix. Les valeurs acceptées sont les suivantes : <ul style="list-style-type: none"><li>• aix_rs6000_64</li><li>• linux_x64</li><li>• solaris_sparcv9</li><li>• win64_x64</li></ul>

## 10.12.1.2 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.

### **i** 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=tcipip(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 \[page 406\]](#)

## 10.12.2 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.

### 10.12.2.1 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*.

### 10.12.2.2 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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existants et nouveaux utilisent des ports différents.

5. Réviser 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.

## 10.12.2.2.1 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 \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

### 10.12.2.3 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 .
3. Tapez le nom du nouveau nœud et appuyez sur .
4. Tapez le numéro de port du nouveau SIA et appuyez sur .
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 .
  - 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 .
  - 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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existants et nouveaux utilisent des ports différents.

7. Réviser la page de confirmation et appuyez sur .
- 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.

### 10.12.2.3.1 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 abcl234
    -noservers
    -createcms
```

## Informations associées

[Variables \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

## 10.12.3 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.

## ➔ N'oubliez pas

Vous pouvez recréer un nœud uniquement sur l'ordinateur sur lequel se trouve le nœud.

### 10.12.3.1 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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.

5. Réviser 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.



### 10.12.3.1.1 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 \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

### 10.12.3.2 Recréation d'un nœud sous Unix

1. Exécutez `<REPINSTALL>/sap_bobj/serverconfig.sh`
2. Sélectionnez *Ajouter un nœud*, puis appuyez sur .
3. Tapez le nom du nouveau nœud et appuyez sur .

#### 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 .

5. Sélectionnez *Recréer un nœud*, puis appuyez sur .

- 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 .  
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 .  
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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.

7. Réviser la page de confirmation et appuyez sur .

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.

## 10.12.3.2.1 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 \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

## 10.12.4 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 \[page 411\]](#)

## 10.12.4.1 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.

### 10.12.4.1.1 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 \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

### 10.12.4.2 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 `<REFINSTALL>/sap_bobj/ccm.sh -stop <nomNœud>` pour arrêter le nœud que vous voulez supprimer.
2. Exécutez `<REFINSTALL>/sap_bobj/serverconfig.sh`
3. Sélectionnez **2 - Supprimer un nœud**, puis appuyez sur .
4. Sélectionnez le nœud que vous souhaitez supprimer, puis appuyez sur .
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.

### 10.12.4.2.1 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 \[page 406\]](#)

[Paramètres de script pour ajouter, recréer et supprimer des nœuds \[page 423\]](#)

## 10.12.5 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 \[page 407\]](#)

[Suppression d'un nœud \[page 415\]](#)

## 10.12.5.1 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 \[page 407\]](#)

[Suppression d'un nœud \[page 415\]](#)

## 10.12.5.2 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 .
3. Tapez le nom du nouveau nœud et appuyez sur .
4. Tapez le numéro de port du nouveau SIA et appuyez sur .
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 .
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 \[page 407\]](#)

[Clonage des serveurs \[page 377\]](#)

[Suppression d'un nœud \[page 415\]](#)

### 10.12.6 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.

#### 10.12.6.1 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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire.

5. Réviser 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.

## 10.12.6.1.1 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 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.

```
<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 \[page 406\]](#)

[Paramètres de script pour le déplacement de nœuds \[page 425\]](#)

## 10.12.6.2 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 .
4. Sélectionnez le nœud que vous souhaitez déplacer, puis appuyez sur .
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 . 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 . 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

Évitez d'utiliser le déploiement pendant l'exécution du CMS temporaire. Vérifiez que les CMS existant et temporaire utilisent des ports différents.

7. Réviser 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 `<REFINSTALL>/sap_bobj/ccm.sh -start <nomNœud>` pour démarrer le nœud déplacé.

## 10.12.6.2.1 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 \[page 406\]](#)

[Paramètres de script pour le déplacement de nœuds \[page 425\]](#)

## 10.12.7 Paramètres de script

### 10.12.7.1 Paramètres de script pour ajouter, recréer et supprimer des nœuds

Table 60 :

Paramètre	Description	Exemple
-adopt	Recrée le nœud s'il existe déjà dans le CMS.	<b>-adopt</b>
-cms	<p>Nom et numéro de port du CMS (Central Management Server).</p> <div> <p><b>⚠ Attention</b></p> <p>N'utilisez pas ce paramètre si vous utilisez <code>-usetempcms</code></p> </div> <div> <p><b>i Remarque</b></p> <p>Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.</p> </div>	<b>-cms mycms:6409</b>
-cmsport	<ul style="list-style-type: none"> <li>Numéro de port du CMS lors du démarrage d'un CMS temporaire.</li> </ul> <div> <p><b>⚠ Restriction</b></p> <p>Vous devez également utiliser les paramètres <code>-usetempcms</code>, <code>-dbdriver</code>, <code>-connect</code> et <code>-dbkey</code>.</p> </div> <ul style="list-style-type: none"> <li>Numéro de port du CMS lors de la création d'un CMS.</li> </ul> <div> <p><b>⚠ Restriction</b></p> <p>Vous devez également utiliser les paramètres <code>-dbdriver</code>, <code>-connect</code> et <code>-dbkey</code>.</p> </div>	<b>-cmsport 6401</b>
-connect	<p>Chaîne de connexion de la base de données système du CMS (ou du CMS temporaire).</p> <div> <p><b>i Remarque</b></p> <p>Ignorez les attributs <code>HOSTNAME</code> et <code>PORT</code> lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.</p> </div>	<b>-connect "DSN=BusinessObjects CMS 140;UID=nom_utilisateur;PWD=mot_ de_passe;HOSTNAME=base_de_donnée s;PORT=3306"</b>

Paramètre	Description	Exemple
-dbdriver	<p>Pilote de la base de données du CMS.</p> <p>Valeurs acceptées :</p> <ul style="list-style-type: none"> <li>• <code>db2databasesubsystem</code></li> <li>• <code>maxdbdatabasesubsystem</code></li> <li>• <code>mysqldatabasesubsystem</code></li> <li>• <code>oracledatabasesubsystem</code></li> <li>• <code>squidatabasesubsystem</code></li> <li>• <code>sqlserverdatabasesubsystem</code></li> <li>• <code>sybasedatabasesubsystem</code></li> <li>• <code>newdbdatabasesubsystem</code></li> </ul>	<code>-dbdriver mysqldatabasesubsystem</code>
-dbkey	Clé du cluster.	<code>-dbkey abc1234</code>
-name	Nom d'un nœud.	<code>-name mynode2</code>
-noservers	<p>Crée un nœud sans serveurs.</p> <div> <p><b>i Remarque</b></p> <p>Le paramètre supplémentaire <code>-createcms</code> crée un nœud avec un CMS, mais avec aucun autre serveur. Ignorez ces paramètres pour créer un nœud avec tous les serveurs par défaut.</p> </div>	<code>-noservers</code>
-password	Mot de passe du compte Administrateur.	<code>-password MotDePasse1</code>
-siaport	Numéro de port du Server Intelligence Agent pour le nœud.	<code>-siaport 6409</code>
-username	Nom d'utilisateur du compte Administrateur.	<code>-username Administrateur</code>
-usetempcms	<div> <p><b>⚠ Attention</b></p> <p>N'utilisez pas ce paramètre si vous utilisez <code>-cms</code></p> <p>Démarre et utilise le CMS temporaire.</p> </div> <div> <p><b>i Remarque</b></p> <p>Utilisez un CMS temporaire lorsque votre déploiement n'est pas en cours d'exécution.</p> </div>	<code>-usetempcms</code>

## Informations associées





[Ajout d'un nœud à l'aide d'un script sous Windows \[page 409\]](#)

[Ajout d'un nœud à l'aide d'un script sous Unix \[page 411\]](#)



[Recréation d'un nœud à l'aide d'un script sous Windows \[page 413\]](#)  
[Recréation d'un nœud à l'aide d'un script sous Unix \[page 414\]](#)  
[Suppression d'un nœud à l'aide d'un script sous Windows \[page 416\]](#)  
[Suppression d'un nœud à l'aide d'un script sous Unix \[page 416\]](#)

## 10.12.7.2 Paramètres de script pour le déplacement de nœuds

Table 61 :

Paramètre	Description	Exemple
-cms	<p>Nom du CMS (Central Management Server) source.</p> <div>  <b>Attention</b>            N'utilisez pas ce paramètre si vous utilisez -usetempcms         </div> <div>  <b>Remarque</b>            Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.         </div>	<b>-cms sourceMachine:6409</b>
-cmsport	<ul style="list-style-type: none"> <li>Numéro de port du CMS lors du démarrage d'un CMS temporaire.</li> </ul> <div>  <b>Restriction</b>            Vous devez également utiliser les paramètres -usetempcms, -dbdriver, -connect et -dbkey.         </div> <ul style="list-style-type: none"> <li>Numéro de port du CMS lors de la création d'un CMS.</li> </ul> <div>  <b>Restriction</b>            Vous devez également utiliser les paramètres -dbdriver, -connect et -dbkey.         </div>	<b>-cmsport 6401</b>

Paramètre	Description	Exemple
-connect	<p>Chaîne de connexion de la base de données système du CMS source (ou du CMS temporaire).</p> <div> <p><b>i Remarque</b></p> <p>Ignorez les attributs <code>HOSTNAME</code> et <code>PORT</code> lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.</p> </div>	<pre>-connect "DSN=Source BOEXI40;UID=nom_utilisateur;PWD=m ot_de_passe;HOSTNAME=base_de_donn ées;PORT=3306"</pre>
-dbdriver	<p>Pilote de la base de données du CMS source.</p> <p>Valeurs acceptées :</p> <ul style="list-style-type: none"> <li>• <code>db2databasesubsystem</code></li> <li>• <code>maxdbdatabasesubsystem</code></li> <li>• <code>mysqldatabasesubsystem</code></li> <li>• <code>oracledatabasesubsystem</code></li> <li>• <code>sqldatabasesubsystem</code></li> <li>• <code>sqlserverdatabasesubsystem</code></li> <li>• <code>sybasedatabasesubsystem</code></li> <li>• <code>newdbdatabasesubsystem</code></li> </ul>	<pre>-dbdriver mysqldatabasesubsystem</pre>
-dbkey	Clé du cluster source.	<pre>-dbkey abc1234</pre>
-destcms	<p>Nom du CMS de destination.</p> <div> <p><b>i Remarque</b></p> <p>Vous devez spécifier le numéro de port si le CMS n'est pas exécuté sur le port par défaut 6400.</p> </div>	<pre>-destcms destinationMachine:6401</pre>
-destconnect	<p>Chaîne de connexion de la base de données système du CMS de destination.</p> <div> <p><b>i Remarque</b></p> <p>Ignorez les attributs <code>HOSTNAME</code> et <code>PORT</code> lors d'une connexion à une base de données DB2, Oracle, SQL Anywhere, SQL Server ou Sybase.</p> </div>	<pre>-destconnect "DSN=Destin BOEXI40;UID=nom_utilisateur;PWD=m ot_de_passe;HOSTNAME=base_de_donn ées;PORT=3306"</pre>

Paramètre	Description	Exemple
-destdbdriver	<p>Pilote de la base de données du CMS de destination.</p> <p>Valeurs acceptées :</p> <ul style="list-style-type: none"> <li>• <b>db2databasesubsystem</b></li> <li>• <b>maxdbdatabasesubsystem</b></li> <li>• <b>mysqldatabasesubsystem</b></li> <li>• <b>oracledatabasesubsystem</b></li> <li>• <b>squidatabasesubsystem</b></li> <li>• <b>sybasedatabasesubsystem</b></li> <li>• <b>newdbdatabasesubsystem</b></li> </ul>	<b>-destdbdriver sybasedatabasesubsystem</b>
-destdbkey	Clé du cluster de destination.	<b>-destdbkey def5678</b>
-destpassword	Mot de passe du compte Administrateur sur le CMS de destination.	<b>-destpassword Password2</b>
-destusername	Nom d'utilisateur du compte Administrateur sur le CMS de destination.	<b>-destusername Administrator</b>
-password	Mot de passe du compte Administrateur sur le CMS source.	<b>-password MotDePasse1</b>
-username	Nom d'utilisateur du compte Administrateur sur le CMS source.	<b>-username Administrateur</b>
-usetempcms	<div>  <b>Attention</b>  N'utilisez pas ce paramètre si vous utilisez -cms </div> <p>Démarre et utilise le CMS temporaire.</p> <div>  <b>Remarque</b>  Utilisez un CMS temporaire lorsque votre déploiement n'est pas en cours d'exécution. </div>	<b>-usetempcms</b>

## Informations associées

[Déplacement d'un nœud à l'aide d'un script sous Windows \[page 420\]](#)

[Déplacement d'un nœud à l'aide d'un script sous Unix \[page 422\]](#)

## 10.12.8 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.

### 10.12.8.1 Ajout des dépendances de serveurs Windows

1. Utilisez le CCM (Central Configuration Manager) pour arrêter 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.

### 10.12.9 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.

### 10.12.9.1 Modification des références de connexion utilisateur pour un nœud sous Windows

1. Utilisez le CCM (Central Configuration Manager) pour arrêter 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.



## 10.13 Renommage d'un ordinateur dans un déploiement de plateforme de BI

### 10.13.1 Modification du nom des clusters

Meilleures pratiques pour renommer les clusters :



#### Attention

Ne jamais déployer plusieurs clusters ayant le même nom.

Table 62 :

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 <code>&lt;nomhôte&gt; : &lt;port&gt;</code> ). 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.	<ul style="list-style-type: none"><li>• vérifiez que le nouveau CMS s'exécute sur un port différent.</li><li>• Utilisez des mots de passe distincts pour les différents clusters afin d'empêcher les utilisateurs de se connecter à un cluster erroné.</li></ul>

### 10.13.2 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 :

Table 63 :

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 <code>localhost</code> 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 <i>Paramètres de traitement</i> de l'application sélectionnée.


Condition	Action
Vous utilisez l'URL des clients de la plateforme de BI basés sur des services Web (par exemple, Crystal Reports pour Java ou LiveOffice).	Par exemple, pour Open Document, cliquez sur l'onglet <i>Applications</i> dans la CMC, cliquez avec le bouton droit sur <i>Open Document</i> et sélectionnez <i>Paramètres de traitement</i> .
Vous utilisez OpenDocument.	

## Règles alternatives

### Remarque

Suivez ces règles uniquement si vous ne pouvez pas respecter les meilleures pratiques décrites ci-dessus.

Table 64 : 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 <i>Serveurs</i> 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.  <div>  <b>Conseil</b>            Connectez-vous à la CMC pour vérifier que la plateforme de BI est opérationnelle.         </div>

### N'oubliez pas

Redémarrez l'ordinateur après exécution d'une action.

Table 65 : 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 <i>URL du visualiseur par défaut</i> de la section <i>Paramètres de traitement</i> dans l'onglet <i>Applications</i> 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 \(nouvelle ou existante\) \[page 439\]](#)

### 10.13.3 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 :

Table 66 :

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.

#### 10.13.3.1 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 :

Table 67 :

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.

Condition	Action
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 <code>cms.default</code> .	<p>Mettez à jour le nom de l'ordinateur du CMS dans la propriété <code>cms.default</code> 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 <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom</code>.</p> <div> <p><b>i Remarque</b></p> <p>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 <code>cms.default</code> des fichiers de propriétés personnalisés.</p> </div>
L'ordinateur renommé héberge un CMS et SAP BusinessObjects Explorer est installé sur un des ordinateurs du cluster.	<p>Remplacez l'ancien nom d'hôte du CMS par le nouveau dans la propriété <code>default.cms.name</code> du fichier <code>default.settings.properties</code> sur tous les ordinateurs hébergeant des serveurs d'applications Web. Par défaut, sous Tomcat, le fichier <code>default.settings.properties</code> se trouve à l'emplacement <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\</code></p> <div> <p><b>➔ N'oubliez pas</b></p> <p>Redémarrez l'application Web Explorer ou le serveur d'applications après avoir exécuté l'action.</p> </div>
Vous utilisez la connexion unique avec Explorer	Mettez à jour la valeur <code>cms</code> dans <code>jsp-sso-provider.jsp</code> ainsi que les valeurs <code>sso.global.cms</code> et <code>sso.trusted.auth.x509.cms</code> dans le fichier <code>sso.properties</code> en leur donnant le nouveau nom d'hôte du CMS.
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.
<p>Votre déploiement répond à toutes les conditions suivantes :</p> <ul style="list-style-type: none"> <li>• Un cluster comporte plusieurs nœuds.</li> <li>• Tous les serveurs du CMS s'exécutent uniquement sur l'ordinateur ayant été renommé.</li> <li>• Au moins un des nœuds n'héberge pas le CMS.</li> <li>• Vous renommez un ordinateur comportant au moins un nœud.</li> <li>• L'adresse IP est modifiée durant le processus de renommage.</li> </ul>	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 \[page 411\]](#)

## 10.13.3.2 Niveau Web

Si vous renommez l'ordinateur qui héberge le serveur d'applications Web de la plateforme de BI, suivez ces instructions :

Table 68 :

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 ► <a href="#">Applications</a> ► <a href="#">CMC</a> ► <a href="#">Paramètres de traitement</a> ►.
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.

## 10.13.3.3 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 :

Table 69 :

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 <code>localhost</code> dans le DSN pour éviter une mise à jour si le nom d'hôte est modifié.

## Base de données système du CMS

Table 70 :

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

Table 71 :

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 <a href="#">Audit</a> de la CMC.

### 10.13.3.4 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.

## 10.14 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`

#### **i** 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`.

## 10.15 Gestion des espaces réservés de nœuds et de serveurs

### 10.15.1 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 \[page 1006\]](#)

### 10.15.2 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 modifications souhaitées, puis cliquez sur *Enregistrer* pour continuer.

---

## Informations associées

[Espaces réservés de nœud et de serveur \[page 1006\]](#)



# 11 Gestion des bases de données du Central Management Server (CMS)

## 11.1 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 \[page 393\]](#)

### 11.1.1 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 \[page 444\]](#)

[Sélection d'une base de données CMS \(nouvelle ou existante\) \[page 439\]](#)

### 11.1.2 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]
SERVERNODE=<HANA Server IP address>:<HANA server port #>
```

<New\_DB\_version> correspond à la version de SAP HANA ; par exemple, « NouvelleBD 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
```

- 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>/odbcrc <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, copiez `libodbcHDB.so` depuis le répertoire d'installation de SAP HANA vers l'emplacement `<REPINSTALL>/sap_bobj/enterprise_xi40/<PLATEFORME>`
  6. Arrêtez tous les nœuds du système.
  7. Exécutez l'application appropriée.
    - Sous UNIX, exécutez `./cmsdbsetup.sh`.
    - Sous Windows, démarrez le CCM (Central Configuration Manager).
  8. Copiez vos données depuis la base de données du CMS par défaut en sélectionnant SAP HANA 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 ».
  9. Sur les déploiements à plusieurs nœuds, 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 SAP HANA. Pour en savoir plus, voir le lien associé « Sélection d'une base de données du CMS (nouvelle ou existante) »
  10. 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 \[page 444\]](#)

[Sélection d'une base de données CMS \(nouvelle ou existante\) \[page 439\]](#)

## 11.2 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 permettent 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.)

### **i** 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 antérieure à 9.5 Fix Pack 5 (pour la gamme 9.5) ou 9.7 Fix Pack 1 (pour la gamme 9.7).

### **i** 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.

## **11.2.1 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.

## 11.2.2 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 \[page 882\]](#)

## 11.3 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.

#### **i** 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 \[page 494\]](#)

### 11.3.1 Pour recréer la base de données système du CMS sous Windows

1. Utilisez le CCM pour arrêter le Serveur Intelligence Agent (SIA).

#### **i** 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*.

#### **i** 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*.

#### **i** 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.

## 11.3.2 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.

### **i** 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>
```

### **i** 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 \[page 882\]](#)

### 11.4 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 recrées). Une fois les données copiées, la base de données de destination devient la base de données officielle et active du CMS.

#### Remarque

Pour importer des utilisateurs, des groupes, des dossiers et des rapports d'une précédente version principale de la plateforme de BI dans la version principale actuelle, utilisez l'outil de gestion de mise à niveau. Pour en savoir plus, voir le *Guide de mise à niveau de la plateforme SAP BI*.

#### Attention

N'essayez jamais d'utiliser une base de données du CMS depuis un autre cluster de la plateforme de BI. Avant de débiter 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.

#### 11.4.1 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.

#### **i** 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.

#### **i** 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.`

## **11.4.2 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](#).

### 11.4.3 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.

#### **i** 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 Gestion des serveurs conteneurs d'applications Web (WACS)

### 12.1 WACS

#### 12.1.1 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.

##### 12.1.1.1 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.

##### 12.1.1.2 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.

## 12.1.1.3 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.	<ul style="list-style-type: none"> <li>• <a href="#">Ajout ou suppression de serveurs WACS à votre déploiement [page 450]</a></li> <li>• <a href="#">Clonage d'un serveur WACS [page 452]</a></li> </ul>
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.	<a href="#">Ajout ou suppression de serveurs WACS à votre déploiement [page 450]</a>
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.	<a href="#">Ajout ou suppression de serveurs WACS à votre déploiement [page 450]</a>
Comment puis-je améliorer la sécurité des communications entre les clients et les serveurs WACS ?	Configurez HTTPS sur les serveurs WACS.	<ul style="list-style-type: none"> <li>• <a href="#">Configuration HTTPS/SSL [page 455]</a></li> <li>• <a href="#">Utilisation des serveurs WACS avec des pare-feu [page 480]</a></li> </ul>
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.	<ul style="list-style-type: none"> <li>• <a href="#">Configuration des serveurs pour SSL [page 172]</a></li> <li>• <a href="#">Utilisation des serveurs WACS avec des pare-feu [page 480]</a></li> </ul>
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.	<a href="#">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 480]</a>
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 équilibres de charge matériels, des serveurs proxy inverses et des pare-feu.	<ul style="list-style-type: none"> <li>• <a href="#">Utilisation d'un serveur WACS avec d'autres serveurs Web [page 478]</a></li> </ul>

Tâche	Description	Sujet
		<ul style="list-style-type: none"> <li>Utilisation des serveurs WACS avec un équilibreur de charge [page 479]</li> <li>Utilisation d'un serveur WACS avec un serveur proxy inverse [page 479]</li> <li>Utilisation des serveurs WACS avec des pare-feu [page 480]</li> </ul>
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.	<a href="#">Utilisation des serveurs WACS avec un équilibreur de charge [page 479]</a>
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.	<a href="#">Utilisation d'un serveur WACS avec un serveur proxy inverse [page 479]</a>
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.	<ul style="list-style-type: none"> <li><a href="#">Pour configurer le suivi sur un serveur WACS [page 482]</a></li> <li><a href="#">Affichage des métriques de serveur [page 482]</a></li> </ul>
Je n'obtiens aucune page à partir d'un port particulier. Quel est le problème ?	<p>Vous pouvez avoir des difficultés à vous connecter au serveur WACS pour plusieurs raisons. Vérifiez les points suivants :</p> <ul style="list-style-type: none"> <li>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 ?</li> <li>La mémoire allouée au serveur WACS est-elle suffisante ?</li> <li>Les serveurs WACS autorisent-ils suffisamment de demandes simultanées ?</li> <li>Si nécessaire, restaurez les paramètres système par défaut des serveurs WACS.</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Pour résoudre les conflits de ports HTTP [page 483]</a></li> <li><a href="#">Pour modifier les paramètres de la mémoire [page 484]</a></li> <li><a href="#">Pour modifier le nombre de demandes simultanées [page 484]</a></li> <li><a href="#">Pour restaurer les valeurs par défaut du système [page 485]</a></li> </ul>
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,	<a href="#">Configuration des propriétés d'applications Web [page 481]</a>

Tâche	Description	Sujet
	voir la section « Configuration des propriétés d'applications Web » de ce chapitre.	
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.	<a href="#">Propriétés des services principaux [page 950]</a>

## 12.1.2 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.

### i 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 une restauration si l'un de ces serveurs est incorrectement configuré.

### 12.1.2.1 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.

Les serveurs WACS sont uniquement pris en charge sur les systèmes d'exploitation Windows.

#### **i** 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.

## 12.1.2.2 Ajout d'un serveur WACS

#### **i** 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 une 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.

## 12.1.2.3 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 une 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.

#### **i** 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 \[page 483\]](#)

### 12.1.2.4 Suppression d'un serveur WACS de votre déploiement

Vous ne pouvez supprimer un serveur WACS qu'à condition de ne pas l'utiliser 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](#).

## 12.1.3 Ajout ou suppression de services aux serveurs WACS

### 12.1.3.1 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.

### 12.1.3.2 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.

## 12.1.4 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.

### **i** 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 utiliser 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 \[page 182\]](#)

[Utilisation d'un serveur WACS avec un serveur proxy inverse \[page 479\]](#)

### 12.1.4.1 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*, cliquez 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.

### 12.1.4.2 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> 🐼

### 12.1.4.3 Pour configurer HTTPS/SSL

Avant de configurer HTTPS/SSL sur votre serveur WACS, assurez-vous que vous avez déjà créé un fichier PKCS12 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 privées protégées par mot de passe afin d'empêcher tout accès non autorisé. Vous devez spécifier le mot de passe permettant d'accéder aux clés privées 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 de 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 PKCS12 ou du fichier de stockage des clés JKS contenant le fichier de la liste des certificats.

#### **i** Remarque

Le type de la liste des certificats de confiance doit être identique au type du fichier de stockage des certificats.

- 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 privées dans le fichier de la liste de certificats de confiance.

#### **i** 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.

## 12.1.5 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

## 12.1.6 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 biais 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 \[page 266\]](#)

[Pour mapper des utilisateurs et groupes Windows AD \[page 267\]](#)

[Configuration d'un compte de service pour l'authentification AD avec Kerberos \[page 265\]](#)

[Exécution du SIA sous le compte de service de la plateforme de BI \[page 274\]](#)

[Activation de l'authentification Kerberos dans le plug-in Windows AD pour le serveur WACS \[page 459\]](#)

[Création des fichiers de configuration \[page 461\]](#)

[Configuration d'un serveur WACS pour l'AD Kerberos \[page 464\]](#)

[Configuration de la connexion unique Kerberos AD \[page 466\]](#)

### 12.1.6.1 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.

## 12.1.6.1.1 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 \[page 265\]](#)
- [Exécution du SIA sous le compte de service de la plateforme de BI \[page 274\]](#)
- [Pour mapper des utilisateurs et groupes Windows AD \[page 267\]](#)

## 12.1.6.1.2 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 \[page 466\]](#)



## 12.1.6.2 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.

### i 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.

### 12.1.6.2.1 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.

### i 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 \[page 463\]](#).

### 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.

## 12.1.6.2.2 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.

## 12.1.6.2.3 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
}
```

## 12.1.6.3 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.

### 12.1.6.3.1 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.

## 12.1.6.4 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

### 12.1.6.4.1 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.

## 12.1.6.4.2 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.

## 12.1.6.4.3 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 :

### 12.1.6.4.3.1 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.

### 12.1.6.4.3.2 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.

## 12.1.7 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 \[page 152\]](#)

[Configuration d'AD Kerberos pour un serveur WACS \[page 459\]](#)

[Configuration de l'ordinateur pour la connexion unique Kerberos AD \[page 466\]](#)

[Configuration du serveur WACS pour la connexion unique Kerberos AD \[page 467\]](#)

### 12.1.7.1 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 \[page 290\]](#)
- [Configuration du compte de service pour la connexion unique Vintela \[page 287\]](#)

- [Configuration de plusieurs SPN \[page 467\]](#)
- [Pour augmenter la limite de taille d'en-tête de votre WACS \[page 467\]](#)

Les sections suivantes expliquent comment réaliser chacune de ces étapes.

### 12.1.7.1.1 Configuration de plusieurs SPN

L'utilisation de plusieurs SPN n'est pas prise en charge.

### 12.1.7.1.2 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.

### 12.1.7.2 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.

### 12.1.7.3 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 \[page 466\]](#).

#### 12.1.7.3.1 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.

### 12.1.8 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*.

## 12.1.8.1 Applications

### 12.1.8.1.1 Configuration de 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://<nom du serveur>:6405/biprws`. Remplacez `<nom du serveur>` 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](#) apparaît.
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://<nom du serveur>:<numéro de port>/biprws`. Remplacez `<nom du serveur>` et `<numéro de port>` par le nom du serveur et le port qui écoute les requêtes de services Web de type RESTful.
5. Cliquez sur [Enregistrer et fermer](#).

## 12.1.8.2 Propriétés des serveurs WACS

### 12.1.8.2.1 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 en 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](#).

## 12.1.8.2.2 Configuration des propriétés système

### 12.1.8.2.2.1 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.

## 12.1.8.2.2.2 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*.

## 12.1.8.2.2.3 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*.

## 12.1.8.2.2.4 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](#).

## 12.1.8.2.2.5 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 \[page 472\]](#)

### 12.1.8.2.3 Cross-Origin Resource Sharing

#### 12.1.8.2.3.1 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](#).

## 12.1.8.2.4 Authentification

### 12.1.8.2.4.1 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/adssso</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>

```

### **i** 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.princ` 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/adssso`).
6. Testez le jeton à l'aide d'une requête GET incluant `X-SAP-LogonToken` dans son en-tête et utilisant l'API `/infostore`.

## 12.1.8.2.4.2 Activation et configuration de l'authentification sécurisée

L'authentification sécurisée doit être activée et configurée via la CMC (Central Management Console) dans les zones incluses dans *Authentification > Entreprise* pour activer l'authentification et générer un fichier clé de secret partagé ; *Utilisateurs et groupes > Liste des utilisateurs* pour créer un compte pour un utilisateur approuvé, et *Serveurs > Liste des serveurs > WACS > Propriétés* pour sélectionner l'option *Méthode d'extraction* aux fins des requêtes de jeton de connexion à l'API de type `/logon/trusted`.

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, `<RépEntreprise>\<plateforme>`.

L'emplacement peut être par exemple :

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI
4.0\win64_x64\"
```

### i 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"
```

### i 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 [Extraction de la méthode](#) 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.

## 12.1.8.2.4.3 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"
```

#### **i** 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](#).

## 12.1.9 Configuration des serveurs WACS dans votre environnement informatique

Cette section explique comment configurer un serveur WACS dans un environnement complexe.

### 12.1.9.1 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.

#### **i** Remarque

Le transfert de demandes à partir d'IIS 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.

## 12.1.9.2 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 \[page 455\]](#)

## 12.1.9.3 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.

### 12.1.9.3.1 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](#).

### 12.1.9.3.2 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.

### 12.1.9.4 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 \[page 182\]](#)

### 12.1.9.5 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.

## 12.1.10 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*.

### i 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.

### i Remarque

Après avoir modifié les propriétés d'un WACS, vous devez toujours le redémarrer.

---

## Informations associées

Pour modifier les propriétés d'un serveur [page 393]

Fichier war BOE [page 636]

## 12.1.11 Dépannage

### 12.1.11.1 Pour configurer le suivi sur un serveur WACS

Pour configurer le suivi d'un serveur WACS, voir [Journalisation des traces de composant \[page 860\]](#)

### 12.1.11.2 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 \[page 997\]](#)

### 12.1.11.3 Pour visualiser 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 « Démarré 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.

## 12.1.11.4 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.

### 12.1.11.4.1 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.

### 12.1.11.4.2 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](#).

### 12.1.11.5 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.

### 12.1.11.6 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](#).

### 12.1.11.7 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.

### 12.1.11.8 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.

## 12.1.12 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 \[page 950\]](#)

# 13 Sauvegarde et restauration de votre système

## 13.1 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 \[page 491\]](#)

[Sauvegarde du contenu BI \[page 497\]](#)

[Pour sauvegarder les paramètres du serveur à l'aide du CCM sous Windows \[page 495\]](#)

[Pour sauvegarder des paramètres de serveur sous UNIX \[page 495\]](#)

[Présentation de la copie du système \[page 509\]](#)

## 13.2 Terminologie

Table 72 :

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.
Gestion des versions	<p>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.</p> <p>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).</p>

Terme	Définition
Sauvegarde système complète	<p>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.</p> <p>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.</p>
Sauvegarde système complète et sauvegarde d'applications	<p>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.</p> <p>Une sauvegarde d'applications sauvegarde les fichiers concernant des applications individuelles.</p> <p>La plateforme de BI prend en charge les sauvegardes système complètes, mais pas les sauvegardes d'applications.</p> <p>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.</p> <p>On appelle jeu de sauvegarde la sauvegarde système complète de la plateforme de BI.</p>
Jeu de sauvegarde	<p>Un jeu de sauvegarde comprend ces sauvegardes individuelles créées au même moment :</p> <ul style="list-style-type: none"> <li>• une copie de sauvegarde de la base de données système du CMS ;</li> <li>• 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 ;</li> <li>• 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) ;</li> <li>• 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) ;</li> <li>• une copie de sauvegarde de la base de données d'audit</li> </ul>
Sauvegarde à froid et sauvegarde à chaud	<p>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.</p> <p>La plateforme de BI prend en charge les deux types de sauvegarde, à froid et à chaud.</p> <p>La sauvegarde à chaud est parfois appelée « sauvegarde en ligne ».</p>

## 13.3 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
<p>Objectif : restaurer un système</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Un ordinateur hébergeant la plateforme de BI a été endommagé. Je dois le remplacer par un nouvel ordinateur.</li> </ol>	<ul style="list-style-type: none"> <li>• Un système cible dont le matériel est identique au système source ET</li> <li>• Des sauvegardes du système source</li> </ul>	<p>Utilisez le workflow de sauvegarde et restauration système détaillé dans ce guide. Voir la procédure <a href="#">Sauvegarde du système entier [page 491]</a>. Recréer le système cible à partir de sauvegardes du système source.</p>
<p>Objectif : restaurer des objets</p> <p>Je veux récupérer un document ou un autre objet supprimé accidentellement.</p>	<ul style="list-style-type: none"> <li>• Des sauvegardes des bases de données et fichiers du système source ET</li> <li>• Les informations système détaillées décrites dans <a href="#">Pour exporter depuis un système source [page 513]</a></li> </ul>	<p>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 <a href="#">Planification de la copie du système [page 510]</a> et suivez les instructions du reste du chapitre.</p> <div> <p><b>i Remarque</b></p> <p>Vous pouvez créer votre système cible sur un ordinateur comportant un déploiement existant de la 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 plateforme de BI.</p> </div>
<p>Objectif : restaurer des objets 2</p> <p>Je veux récupérer un document ou un autre objet supprimé accidentellement.</p>	<p>Un système où le versionnement de la Gestion des promotions est utilisé</p>	<p>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.</p>
<p>Objectif : sauvegarder des objets</p> <p>Je désire sauvegarder un petit nombre d'objets (par exemple, des documents, des dossiers, des utilisateurs).</p>	<p>Un système où le versionnement de la Gestion des promotions est utilisé</p>	<p>Utilisez l'application Gestion des promotions pour sauvegarder le contenu BI, puis l'exporter vers les fichiers Business Intelligence Archive (LCMBIAR). Si le contenu est corrompu ou manquant, vous pouvez le restaurer ultérieurement sans restaurer le système complet.</p>

Objectif	Ressources requises	Solution
		Pour en savoir plus, voir la rubrique associée sur la Gestion des promotions.

## Informations associées

[Sauvegardes \[page 490\]](#)

[Planification de la copie du système \[page 510\]](#)

[Présentation \[page 521\]](#)

## 13.4 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 \[page 491\]](#)

[Sauvegarde des paramètres du serveur \[page 494\]](#)

## 13.4.1 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.

### i 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.

### i 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.

### 13.4.1.1 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.

### i Remarque

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.

#### **i** 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).

#### **i** 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.

Les clients Crystal Reports 2013 Designer, Web Intelligence Rich Clients et outil de conception d'univers antérieurs à la version 4.0 FP3, ainsi que les applications client lourd personnalisées compilées par rapport à des SDK antérieurs à la version 4.0 FP3 peuvent ne pas prendre en charge la modification de fichier durant la sauvegarde à chaud. Si ces applications client modifient le contenu BI durant les sauvegardes, cela peut compromettre la qualité des données modifiées pendant la sauvegarde. Vous pouvez empêcher les applications client de modifier les documents pour garantir la cohérence des données sauvegardées. Mettez à niveau les applications client vers 4.0 FP3 dès que possible. Si ce n'est pas possible, vous pouvez examiner les solutions envisageables. Par exemple, vous pouvez conseiller aux utilisateurs des applications clients de supprimer les objets existants et d'enregistrer de nouvelles versions au lieu de modifier les objets.

### **13.4.1.1.1 Pour activer les 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.

#### **i** 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. Pour permettre aux applications anciennes (antérieures à 4.0 FP3) Web Intelligence Rich Client, Crystal Reports Designer, ou client lourd avec SDK personnalisé de modifier les documents sur le système, cochez la case [Activer le support des applications héritées \(Limitations de sauvegarde\)](#).

Si vous permettez à ces clients plus anciens de modifier des documents lors des opérations de sauvegarde, cela peut entraîner des incohérences dans les documents modifiés durant la sauvegarde. Pour en savoir plus sur les limitations de la sauvegarde, voir le lien associé concernant les sauvegardes à chaud.

6. 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.

### 13.4.1.2 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.
  - 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 \[page 491\]](#)

### 13.4.2 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.

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.

#### **i** 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`.

## 13.4.2.1 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.

## 13.4.2.2 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 .
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 .
  - Pour sauvegarder les paramètres de serveur d'un système qui n'est pas en cours d'exécution, sélectionnez **temporaire** et appuyez sur .
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 .
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 .
- Une page de synthèse affiche les informations fournies.
6. Vérifiez que les informations affichées sont correctes, puis appuyez sur  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 écrits dans le 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.

### 13.4.2.3 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/<plateforme64>/scripts`.

## Informations associées

[Scripts BackupCluster et RestoreCluster \[page 506\]](#)

### 13.4.3 Sauvegarde du contenu BI

Il est recommandé d'utiliser l'application de gestion des promotions pour effectuer des sauvegardes régulières de votre contenu Business Intelligence, comme vos rapports, vos utilisateurs et groupes ainsi que vos univers. 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 l'utilisation de l'outil de gestion des promotions, voir le chapitre « Gestion des promotions ».

Si vous utilisez Subversion avec l'outil de gestion des promotions, voir le chapitre « Gestion des versions ».

## 13.5 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 \[page 497\]](#)

[Restauration des paramètres de serveur \[page 503\]](#)

[Restauration du contenu BI \[page 506\]](#)

### 13.5.1 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

#### **i** Remarque

Si le reste de la plateforme de BI fonctionne normalement, mais que la base de données du CMS est défaillante, vous pouvez la restaurer sans avoir à restaurer le système complet.

- Stockage de fichiers du FRS
- Système de fichiers de l'ordinateur

#### **i** 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 \[page 498\]](#)

[Restauration de la base de données d'audit uniquement \[page 500\]](#)

[Pour restaurer le contenu de niveau Web \[page 500\]](#)

[Pour restaurer la base de données du CMS uniquement \[page 501\]](#)

### **13.5.1.1 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.

#### **i** 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

#### **i** Remarque

Veillez à valider les sauvegardes et assurez-vous que tous les fichiers répertoriés ci-dessus font partie du même jeu de sauvegardes. 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 seul 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 :
  - a. Recherchez les dernières copies de sauvegarde et les derniers journaux de transactions de la base de données d'audit.
  - b. Utilisez les outils de base de données pour restaurer la base de données d'audit.
  - c. Effectuez une restauration par progression de la base de données d'audit en relisant le journal de transactions.
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 \[page 502\]](#) 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 [NOM_DB].ADS_EVENT where Start_Time > '<[heure de panne de base de données]>' and Start_Time < '<[heure de restauration de base de données]>'`

## Informations associées

[Indexation de contenu dans le référentiel CMS \[page 741\]](#)

### 13.5.1.2 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.

#### **i** 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.

1. Recherchez les dernières copies de sauvegarde et les derniers journaux de transactions de la base de données d'audit.
2. Utilisez les outils de base de données pour restaurer la base de données d'audit.
3. Effectuez une restauration par progression de la base de données d'audit en relisant le journal de transactions.

#### Informations associées

Pour restaurer votre système entier [\[page 498\]](#)

### 13.5.1.3 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.



## 13.5.1.4 Pour restaurer la base de données du CMS uniquement

### **i** Remarque

Suivez cette procédure si seule la base de données du CMS est défaillante. 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.

### **i** 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.

1. Arrêtez tous les nœuds de la plateforme de BI à l'aide du CCM.
2. Localisez le dernier jeu de sauvegardes de la base de données du CMS.
3. A l'aide de vos outils de base de données, restaurez la base de données du CMS.
4. Recherchez le plus récent journal des transactions de la base de données du CMS, c'est-à-dire le journal qui contient les transactions effectuées après la dernière sauvegarde.
5. Relisez l'intégralité du journal de transactions de la base de données du CMS.
6. 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 \[page 741\]](#)

## 13.5.1.5 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 \[page 741\]](#)

### 13.5.1.5.1 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 [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.

## 13.5.2 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.

## 13.5.2.1 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. En cas d'échec de l'opération de restauration, consultez le fichier journal pour en déterminer le motif.
13. Cliquez sur *OK* pour fermer l'assistant.

Les paramètres de serveur du fichier BIAR sont 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 \[page 405\]](#)

### 13.5.2.2 Restauration des paramètres de serveur avec le CCM 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 .
  2. Saisissez un numéro de port pour le CMS (Central Management Server) temporaire à utiliser et appuyez sur .
  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 .
  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 .
- 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.

### 13.5.2.3 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 \[page 506\]](#)

## 13.5.3 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 ».

## 13.6 Scripts BackupCluster et RestoreCluster

Le tableau suivant décrit les paramètres de commande de ligne utilisés avec le script BackupCluster.

### i Remarque

Ce script sauvegarde uniquement les paramètres de serveur d'un cluster. Les autres données doivent être sauvegardées séparément.

Table 73 : Paramètres BackupCluster

Nom	Description	Exemple
-backup	Nom et chemin du fichier BIAR devant sauvegarder les paramètres de serveur de votre système à restaurer.	<code>-backup "C:\Users\Administrator\Desktop\my.biar"</code>
-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.	<code>-cms mycms:6400</code>
-username	Nom d'utilisateur d'un compte administrateur.	<code>-username Administrator</code>
-password	Mot de passe d'un compte administrateur.	<code>-password MotDePasse1</code>

Le tableau suivant décrit les paramètres de commande de ligne utilisés avec le script RestoreCluster.

Table 74 : Paramètres RestoreCluster

Nom	Description	Exemple
-restore	Nom et chemin du fichier BIAR contenant les paramètres de configuration de serveur à restaurer.	<code>-restore "C:\Users\Administrator\Desktop\my.biar"</code>
-username	Nom d'utilisateur d'un compte administrateur.	<code>-username Administrator</code>
-password	Mot de passe d'un compte administrateur.	<code>-password MotDePasse1</code>

Nom	Description	Exemple
-displaycontents	Affiche une liste des nœuds et serveurs que contient le fichier BIAR.	<b>-displaycontents "C:\Users\Administrator\Desktop\my.biar"</b>

### **i** 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.

Table 75 : 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.	<b>-usetempcms</b>
-cmsport	Numéro de port du CMS temporaire.	<b>-cmsport 6700</b>
-dbdriver	Pilote de la base de données système du CMS. Les valeurs acceptées sont les suivantes : <ul style="list-style-type: none"> <li>• <b>db2databasesubsystem</b></li> <li>• <b>maxdbdatabasesubsystem</b></li> <li>• <b>mysqldatabasesubsystem</b></li> <li>• <b>oracledatabasesubsystem</b></li> <li>• <b>sqlserverdatabasesubsystem</b></li> <li>• <b>sybasedatabasesubsystem</b></li> <li>• <b>sqlanywheredatabasesubsystem</b></li> <li>• <b>newdbdatabasesubsystem</b></li> </ul> <div> <b>i</b> Remarque            Le paramètre <b>newdbdatabasesubsystem</b> est destiné à être utilisé avec les bases de données SAP HANA.         </div>	<b>-dbdriver sqlserverdatabasesubsystem</b>
-connect	Chaîne de connexion de la base de données système du CMS.	<b>-connect "DSN=BusinessObjects CMS 1;UID=nom_utilisateur;PWD=mot_de_passe;HOSTNAME=base_de_donnees;PORT=3306"</b>
-dbkey	Clé du cluster.	<b>-dbkey abc1234</b>

### 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
```



# 14 Copie de votre déploiement de la plateforme de BI

## 14.1 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.

### Informations associées

[Présentation de la sauvegarde et de la restauration \[page 487\]](#)

## 14.2 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.

## 14.3 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
<p>Objectif : copie identique</p> <p>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.</p>	<ul style="list-style-type: none"> <li>• Un système cible dont le matériel est identique au système source ET</li> <li>• Sauvegardes du système source ou accès au système source pour en effectuer une sauvegarde</li> </ul>	<p>Utilisez le workflow de sauvegarde et restauration système détaillé dans ce guide. Voir la procédure <a href="#">Sauvegarde du système entier [page 491]</a>. Recréez le système cible à partir de sauvegardes du système source.</p>
<p>Objectif : copie</p> <p>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.</p>	<ul style="list-style-type: none"> <li>• Système source (en cours d'exécution ou arrêté) OU sauvegardes des bases de données et fichiers du système source source. ET</li> <li>• Les informations système détaillées décrites dans <a href="#">Pour exporter depuis un système source [page 513]</a></li> </ul>	<p>Utilisez le workflow de copie du système en commençant par <a href="#">Planification de la copie du système [page 510]</a> et suivez les instructions du reste du chapitre.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>

## Informations associées

[Sauvegardes \[page 490\]](#)

[Planification de la copie du système \[page 510\]](#)

## 14.4 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 bases 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)

## 14.5 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 <a href="http://www.sdn.sap.com/irj/sdn/systemcopy">http://www.sdn.sap.com/irj/sdn/systemcopy</a> (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	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>Si vous établissez une nouvelle base de données, les événements existants n'y sont pas copiés, seuls les nouveaux événements y seront enregistrés.</p> </div>
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 <code>.properties</code> du dossier <code>custom</code> ), 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 promotions. (contient différentes versions des rapports, analyses, autres ressources 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 \[page 36\]](#) 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 \[page 517\]](#) 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.

## 14.6 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.

### 14.6.1 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 \[page 1027\]](#)

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 <a href="#">Serveurs</a> de la CMC et développez <a href="#">nœuds</a> 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 <a href="#">Serveurs</a> de la CMC, cliquez avec le bouton droit sur le CMS et sélectionnez <a href="#">Espaces réservés</a> . 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.	Accédez à l'onglet <a href="#">Serveurs</a> de la CMC, cliquez avec le bouton droit sur le CMS et sélectionnez <a href="#">Métriques</a> .  Recherchez les métriques suivantes : <ul style="list-style-type: none"> <li>• <a href="#">Nom de la connexion à la base de données système</a></li> <li>• <a href="#">Nom du serveur de la base de données système</a></li> <li>• <a href="#">Nom de l'utilisateur de la base de données système</a></li> <li>• <a href="#">Nom de la source de données</a></li> <li>• <a href="#">Nom de connexion de la base de données d'audit</a> (facultatif)</li> <li>• <a href="#">Nom d'utilisateur de la base de données d'audit</a> (facultatif)</li> </ul>
<div> <i>i</i> Remarque </div> <p>Si vous copiez la base de données d'audit, vous aurez aussi besoin des noms et des références de connexion la concernant.</p>	
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 2013 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 <a href="#">Modifier ou supprimer des programmes</a> .  Sous Unix, vous pouvez utiliser l'utilitaire <code>modifyOrRemoveProducts.sh</code> 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 <a href="#">Serveurs</a> de la CMC, cliquez avec le bouton droit de la souris sur l'Input FRS ou l'Output FRS et sélectionnez <a href="#">Propriétés</a> . Recherchez la propriété <a href="#">Répertoire de stockage des fichiers</a> .

Propriété	Emplacement
	<p><b>i Remarque</b></p> <p>Si la valeur commence par %, c'est un espace réservé, vous devrez cliquer sur <a href="#">Espaces réservés</a> et noter le répertoire listé sous cet espace réservé.</p>
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.	<p>Le dossier par défaut de la base de données Gestion des promotions des installations Windows est <code>&lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE</code> et sous Unix <code>&lt;INSTALLDIR&gt;/sap_bobj/data/LCM/LCMOverride</code>.</p> <p>Les emplacements par défaut des fichiers Sous-version des installations Windows sont :</p> <ul style="list-style-type: none"> <li>• <code>&lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\CheckOut</code></li> <li>• <code>&lt;INSTALLDIR&gt;\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository</code></li> </ul> <p>Sous Unix, il s'agit de :</p> <ul style="list-style-type: none"> <li>• <code>&lt;INSTALLDIR&gt;/check_out</code> (Ce répertoire est créé uniquement lorsque vous avez utilisé la Sous-version pour extraire des fichiers.)</li> <li>• <code>\$HOME/LCM_Repository</code></li> </ul>
Si vous prévoyez de copier la base de données de surveillance, le dossier de celle-ci.	<p>Cela est défini dans la CMC. Accédez à la zone de gestion <a href="#">Applications</a> de la CMC, sélectionnez ► <a href="#">Application de surveillance</a> ► <a href="#">Propriétés</a> et recherchez le <a href="#">répertoire de sauvegarde de la base de données des tendances</a>.</p> <p>Le dossier par défaut des installations Windows est <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB</code> et sous Unix, <code>&lt;REPINSTALL&gt;/sap_bobj/Data/TrendingDB</code>.</p>
Chemin du dossier de la couche sémantique	Le chemin d'accès au dossier par défaut dans les installations Windows est <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer</code> 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 Gestion des promotions (facultatif) Cela peut se faire en sauvegardant les fichiers du dossier de base de données 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\LCM\LCMOVERRIDE`. Sous Unix : `<REPINSTALL>/sap_bobj/data/LCM/LCMOverride`.
- 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 :
  - `<INSTALLDIR>\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.

**i** Remarque

Pour consulter les contraintes et une description détaillée de ce workflow, voir la section [Sauvegardes à chaud \[page 491\]](#).

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 :
  - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/conf`
- `clientSDKOptions.xml` installé sous :
  - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/java/lib`
  - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
  - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
- `CRConfig.xml` installé sous :
  - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/java`
- `mdas.properties` installé sous :
  - `[REPINSTALL]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.sapappsvr73`
  - `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 :
    - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
    - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsboobje/WEB-INF/conf`
  - `clientaccesspolicy.xml` installé sous :
    - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
  - `clientSDKOptions.xml` installé sur :
    - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
    - `[REPINSTALL]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsboobje/WEB-INF/lib`
  - `crossdomain.xml` installé sous :
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
    - `[REPINSTALL]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.

## 14.6.2 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.

#### **i** 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 restaurer 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 \[page 497\]](#).

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.

#### **i** 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.

#### **i** 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 \[page 444\]](#) 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

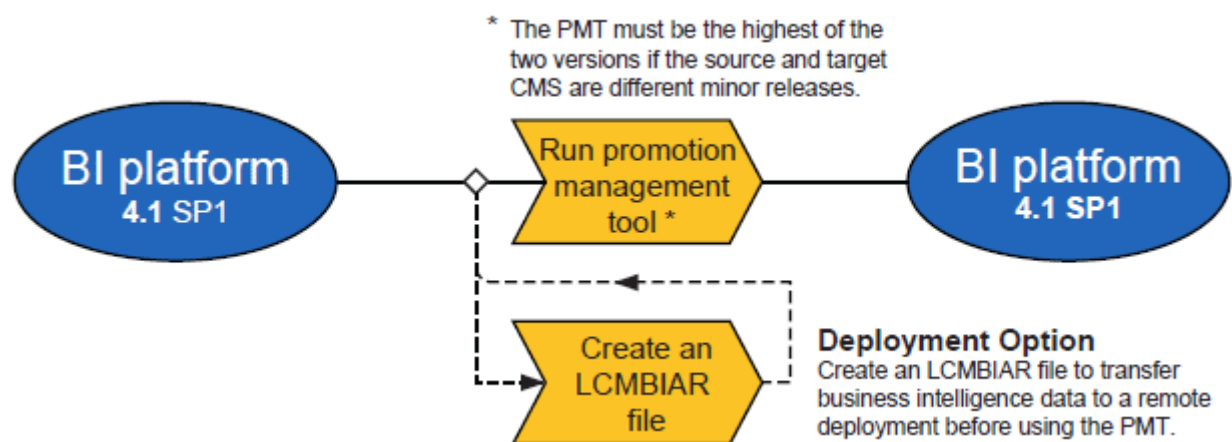
Si vous ne supprimez pas le système source (ou si vous l'utilisez en même temps que le système cible), il est recommandé de renommer le cluster sur le système cible.

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 \[page 286\]](#).
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.

## 15 Gestion des promotions

### 15.1 Bienvenue dans la gestion des promotions

#### 15.1.1 Présentation



L'outil de gestion des promotions permet de déplacer des ressources Business Intelligence (BI) d'un référentiel vers un autre, gère les dépendances des ressources et replace les ressources promues dans le système de destination, si nécessaire. Elle 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.

#### 15.1.2 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.

## 15.1.3 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).

### 15.1.4 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.

### 15.1.5 Remplacement des informations dans la plateforme de BI 4.1 SP3 et version ultérieure

A partir de la plateforme de BI 4.1 SP3, la base de données Derby est remplacée par les informations stockées dans le référentiel. Lors de la promotion de 4.0 SPx ou 4.1 SPx, une promotion automatique et silencieuse se déroule.

En cas d'échec de la promotion automatique (par exemple, si APS affiche des erreurs après la promotion), vous pouvez définir manuellement l'indicateur de migration forcée :

1. Arrêtez le serveur de traitement adaptatif (APS) exécutant la gestion des promotions.
2. Ajoutez le paramètre `-Dcom.businessobjects.lcm.migrateoverrides=true` à l'APS.
3. Démarrez l'APS et laissez la migration forcée se faire.

#### ➔ N'oubliez pas

Une fois la migration terminée, supprimez le paramètre de l'APS.

## 15.1.6 Remplacement des connexions entre le serveur d'applications et le serveur de messagerie

Vous pouvez remplacer le serveur d'applications pour vous connecter au serveur de messagerie ou remplacer le serveur de messagerie pour vous connecter au serveur d'applications en configurant les paramètres dans la boîte de dialogue [Modifier les propriétés de connexion commune](#).

### Remarque

En fonction de votre configuration système, vous pouvez également avoir besoin de mettre à jour les champs suivants communs au serveur d'applications et au serveur de messagerie : [CLIENT](#), [IDSYS](#), [NOM D'UTILISATEUR](#) et [MOT DE PASSE](#).

1. (Facultatif) Pour remplacer le serveur d'applications pour vous connecter au serveur de messagerie, vous devez définir les paramètres suivants :

<a href="#">GROUPE</a>	<GROUPE>
<a href="#">TYPE DE SERVEUR</a>	GROUPE
<a href="#">HÔTE DU SERVEUR DE MESSAGERIE</a>	<SERVEUR DE MESSAGERIE>

### Remarque

Vous pouvez également réinitialiser les champs [HÔTE DU SERVEUR D'APPLICATIONS](#) et [NUMÉRO DU SYSTÈME](#).

2. (Facultatif) Pour remplacer le serveur de messagerie pour vous connecter au serveur d'applications, vous devez définir les paramètres suivants :

<a href="#">TYPE DE SERVEUR</a>	SERVEUR
<a href="#">HÔTE DU SERVEUR D'APPLICATIONS</a>	<SERVEUR D'APPLICATIONS>
<a href="#">NUMÉRO DU SYSTÈME</a>	<NUMÉRO DU SYSTÈME>

### Remarque

Vous pouvez également réinitialiser les champs [GROUPE](#) et [HÔTE DU SERVEUR DE MESSAGERIE](#).

## 15.2 Introduction à l'outil de gestion des promotions

### 15.2.1 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.

## 15.2.2 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 :

Table 76 :

Option	Description
	permet de créer un dossier. Le nouveau dossier est créé en tant que sous-dossier dans le dossier <i>Travaux de promotion</i> .
	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	<p>permet d'annuler le travail promu sur le système de destination.</p> <div> <i>i</i> <b>Remarque</b>            Si le travail promet 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.         </div>
	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.

## 15.2.3 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.

### 15.2.3.1 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 528]

Pour utiliser l'option Paramètres du travail [page 528]

### 15.2.3.2 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 528]

### 15.2.3.3 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 l'option Paramètres du système de gestion des versions \[page 582\]](#)

### 15.2.3.4 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.

#### 15.2.3.4.1 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 \[page 527\]](#).

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. 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 des connexions uniques](#) 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. Cliquez sur [Connexion](#) pour vous connecter au système de destination à l'aide de références de connexion valides.  
Vous pouvez spécifier plusieurs systèmes de destination.
9. Cliquez sur [Promouvoir](#).  
La promotion des remplacements est terminée.

### Remarque

Si les remplacements échouent dans le système de destination pendant la promotion d'InfoObjects, le système définit le statut du travail sur Réussite partielle et définit également un statut d'avertissement Echec des remplacements sur l'objet.

10. Déconnectez-vous du système d'origine.
11. Dans l'écran [Paramètres de remplacement](#), cliquez sur [Connexion](#).  
La fenêtre Se connecter au système apparaît.
12. 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.
13. Cliquez sur la case [Sélectionner](#) des objets que vous souhaitez modifier, puis cliquez sur [Modifier](#).
14. Mettez à jour les valeurs souhaitées et cliquez sur [Terminé](#).  
Le statut des objets modifiés devient Actif.
15. Cliquez sur [Enregistrer](#).

## 15.2.3.4.2 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 \[page 527\]](#).

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.

**i 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*.

**i 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.

**i 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*.

### 15.2.3.4.3 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 \[page 527\]](#).

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](#).

### 15.2.3.5 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 \[page 570\]](#) 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.

## 15.3 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](#).

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 Echec.
- *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 est promu le travail.
- *Système de destination* : Affiche le nom du système vers lequel est promu le travail.
- *Créé par* : Affiche le nom de l'utilisateur qui a créé le travail ou dossier en question.

#### Remarque

L'outil de gestion des promotions utilise le SDK de la plateforme de BI pour toutes ses activités.


## 15.3.1 Création et suppression de dossiers

Cette section décrit comment créer et supprimer un dossier dans la page d'accueil des travaux de promotion.

### 15.3.1.1 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 \[page 535\]](#)

[Suppression d'un dossier \[page 534\]](#)

### 15.3.1.2 Suppression d'un dossier

Cette section décrit comment supprimer un dossier.

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 \[page 535\]](#)

### 15.3.2 Permet de créer un travail

Cette section décrit le mode de création d'un travail à l'aide de l'outil de gestion des promotions.

Le tableau suivant traite des éléments et champs de l'interface utilisateur que vous pouvez utiliser pour créer un travail :

Table 77 :

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 : <ul style="list-style-type: none"><li>• Enterprise</li><li>• Windows AD</li><li>• LDAP</li><li>• SAP</li></ul>

### **i** 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.

### **i** 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.

### **i** 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.

### **i** 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 \[page 529\]](#)

## 15.3.2.1 Pour se connecter à un nouveau CMS

Cette section décrit comment se connecter à un nouveau CMS.

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 \[page 535\]](#).
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 \[page 538\]](#)

[Pour ajouter un InfoObject à un travail \[page 539\]](#)

[Pour promouvoir un travail quand les référentiels sont connectés \[page 542\]](#)

[Pour planifier une promotion de travail \[page 546\]](#)

## 15.3.3 Pour créer un travail en copiant un travail existant

Cette section décrit comment créer un travail en copiant un travail existant.

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 \[page 539\]](#)

[Pour modifier un travail \[page 538\]](#)

[Pour promouvoir un travail quand les référentiels sont connectés \[page 542\]](#)

### 15.3.4 Pour rechercher un travail

La fonctionnalité de recherche de l'outil de gestion de la promotion permet de localiser un travail dans le référentiel.

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 \[page 539\]](#)

[Pour modifier un travail \[page 538\]](#)

### 15.3.5 Pour modifier un travail

Cette section décrit comment modifier un travail.

#### Remarque

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 \[page 539\]](#)

[Pour promouvoir un travail quand les référentiels sont connectés \[page 542\]](#)

[Pour planifier une promotion de travail \[page 546\]](#)

### 15.3.6 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.

#### **i** 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.

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 \[page 535\]](#) et [Pour modifier un travail \[page 538\]](#).
3. Cliquez sur [Ajouter des objets](#) en cas de modification d'un travail.

#### **i** 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 \[page 540\]](#)

[Pour promouvoir un travail quand les référentiels sont connectés \[page 542\]](#)


[Pour planifier une promotion de travail \[page 546\]](#)

## 15.3.7 Pour gérer les dépendances d'un travail

Cette section décrit comment gérer les objets dépendants d'un InfoObject.

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 \[page 535\]](#) et [Pour modifier un travail \[page 538\]](#).
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 \[page 541\]](#)

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.

#### **i** Remarque

Si vous sélectionnez un dossier pour promotion, les contenus du dossier sélectionné sont alors considérés comme ressources principales.

## **Informations associées**

[Pour promouvoir un travail quand les référentiels sont connectés \[page 542\]](#)

## **15.3.8 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.

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 \[page 540\]](#)

## 15.3.9 Pour promouvoir 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.

Le tableau suivant répertorie les types d'InfoObjects pouvant être promus au moyen de l'outil de gestion des promotions :

Table 78 :

Catégorie	Types d'objets que vous pouvez promouvoir
Rapports	Rapports Crystal Reports, Web Intelligence, Dashboards, QaaWS, Explorer
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, Événements, Profils, Lot d'objets, Lien hypertexte, Catégories, Boîte de réception, dossiers Personnel et Favoris
Univers, Espace de travail	Univers UNV, Connexions
Tableau de bord EPM	Univers, Connexions, Rapports, Tableaux de bord et Analyses
Vue d'entreprise	Fondation de données
Fédération <ul style="list-style-type: none"><li>Liste de réplique</li><li>Travaux de réplique</li></ul>	La liste de réplique promeut les objets suivants : Flash, .txt, Discussions, Dashboards, .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 réplique promeuvent les Travaux de réplique, la Connexion distante, les Publications, la Discussion, la Connexion Pioneer
Services BI	Documents Web Intelligence, Univers et Connexions
Nouveaux InfoObjects	Rapports Crystal (rpt/rptr), Pioneer, Dashboard Design, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Foundation (DFX), Webl, Explorer, Data Federator, Data Steward, Espace de travail BI, etc.

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*.

**i 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 sélectionner 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.

Vous pouvez aussi cliquer sur *Afficher la sécurité* pour visualiser les dépendances de sécurité d'InfoObjects dans le travail.

6. 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.

**i 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.

7. Cliquez sur *Planifier* si vous souhaitez que la promotion soit exécutée à un moment donné ou périodiquement.
8. 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.

## 15.3.10 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.

### i Remarque

Vous ne pouvez pas utiliser un fichier LCMBIAR créé à l'aide de l'Assistant d'importation.

## Informations associées

[Exportation d'un travail vers un fichier LCMBIAR \[page 544\]](#)

[Importation d'un travail depuis un fichier LCMBIAR \[page 545\]](#)

### 15.3.10.1 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 \[page 535\]](#)
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](#) 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](#).
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 \[page 546\]](#).

## Informations associées

[Pour ajouter un InfoObject à un travail \[page 539\]](#)

[Pour gérer les dépendances d'un travail \[page 540\]](#)


## 15.3.10.2 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.

### Remarque

Vous pouvez également importer un travail à partir d'un fichier BIAR de l'outil de gestion des mises à niveau.

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.
  - 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](#)

#### Remarque

Vous ne pouvez importer que des fichiers LCMBIAR ou des fichiers BIAR de l'outil de gestion des mises à jour.

4. Cliquez sur [Promouvoir](#).

#### Remarque

Les utilisateurs disposant du droit de modification LCMBIAR peuvent promouvoir sélectivement les objets. Si vous sélectionnez les objets à promouvoir, puis cliquez sur [Promouvoir](#), un nouveau travail est créé avec les objets sélectionnés.

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.

## Informations associées

[Pour gérer les dépendances d'un travail \[page 540\]](#)

### 15.3.11 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.

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.

#### 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 \[page 544\]](#)




### 15.3.11.1 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 \[page 548\]](#)

### 15.3.12 Pour afficher l'historique d'un travail

Cette section décrit comment visualiser l'historique d'un travail.

#### **i** Remarque

Pour visualiser l'historique d'un travail, assurez-vous que le statut du travail est l'un des suivants :

- Réussite
- Echec
- Réussite partielle

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](#).

### 15.3.13 Pour reprendre un travail

L'option Reprise permet de restaurer le système de destination à son statut précédent après la promotion d'un travail.

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.



### 15.3.13.1 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

[Pour gérer différentes versions de ressources BI \[page 580\]](#)

### 15.3.13.2 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.

#### **i** 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 \[page 550\]](#)

[Pour utiliser l'option Reprise partielle \[page 549\]](#)

## **15.3.13.2.1 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](#).

#### **i** 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 \[page 548\]](#)

[Pour utiliser l'option Reprise partielle \[page 549\]](#)

[Pour reprendre un travail après expiration du mot de passe \[page 549\]](#)

## 15.4 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. Il prend en charge les systèmes de gestion des versions SubVersion et ClearCase. 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 cliquer 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.

### 15.4.1 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](#).

## 15.4.2 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.

### 15.4.2.1 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.

### 15.4.2.2 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.

**i 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.

**i 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.

## 15.5 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.

### 15.5.1 Pour préparer les 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.

**i 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.

**i 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.

#### **i** 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.

#### **i** 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 :

Table 79 :

	Allocation d'espace tempore	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.

Par exemple, si vous évaluez que le travail contient 50 000 objets :

- Allouez 10 Go de mémoire à LCM\_CLI ( $50,000 \div 10,000 \times 2$ )
- Allouez 15 Go de mémoire au Job Server ( $50,000 \div 10,000 \times 3$ )

### 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.

## 15.5.2 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.

### **i** Remarque

La sécurité des objets est conservée puisqu'elle est héritée de la sécurité des dossiers.

## 15.6 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. Le tableau suivant répertorie les types de contenu et les paramètres 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, consultez la section « Utilisation de l'option Ligne de commande ».

### 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=<SystèmeSource>
Source_userName=Administrator
Source_password=<MotdepasseAdministrateur>
LCM_CMS=<NomduSystèmeCentral>
LCM_userName=Administrator
LCM_password=<MotdepasseAdministrateur>
Destination_CMS=<SystèmeCible>
Destination_userName=Administrator
Destination_password=<MotdepasseAdministrateur>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```



## 15.6.1 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
```

## 15.6.2 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
- Événements
- 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 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 (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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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
```

### 15.6.3 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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,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_APOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

2. Pour exécuter le travail, accédez au répertoire `<REPINSTALL>\win64x64\scripts` et exécutez la commande suivante :

```
Lcm_cli.bat -lcmproperties=primaryobjects.properties
```

#### **i** 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.

#### **i** 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 ».

## 15.6.4 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.

## 15.7 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

## 15.7.1 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>`

### **i** 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>`

## 15.7.2 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.

## 15.7.3 Paramètres d'outil de ligne de commande

Le tableau suivant décrit les paramètres et les valeurs autorisées pour l'option de ligne de commande de l'outil de gestion des promotions.

### ➔ N'oubliez pas

Ne placez pas de paramètres de ligne de commande entre guillemets.

Table 80 :

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
action	Exporter, Promouvoir Exemple : <code>action=export</code>	Cette option permet de spécifier l'opération que doit effectuer l'interface de ligne de commande (CLI). Cette opération peut réaliser n'importe laquelle des opérations suivantes : <ul style="list-style-type: none"><li>• Promouvoir des objets d'un fichier LCMBIAR ou d'un travail de gestion des promotions vers un système de la plateforme de BI.</li><li>• Exporter des objets à partir d'un système SAP de la plateforme de BI vers un fichier LCMBIAR.</li></ul>	Obligatoire

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
consolelog	true ou false	Ce paramètre est utilisé pour afficher l'intégralité du journal de la commande exécutée par l'utilisateur dans le journal de commande.	Facultatif  La valeur est false s'il n'est pas spécifié.
Destination_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3  Exemple : Destination_authentication=<authentication>	Ce paramètre indique le type d'authentification à utiliser.	Facultatif  Si le type d'authentification n'est pas spécifié, secEnterprise est utilisé
Destination_clientID	ID client  Exemple : Destination_clientID=<IDsystème>	Ce paramètre est utilisé uniquement pour l'authentification SAP.	Obligatoire pour l'authentification SAP.
Destination_CMS	Texte au format libre.  Exemple : Destination_CMS=<nomCMS: numéro du port>	Ce paramètre permet à l'utilisateur de spécifier le CMS auquel doit se connecter l'outil.	Obligatoire si action=promote
Destination_password	Texte au format libre.  Exemple : Destination_password=<mot de passe>	Ce paramètre spécifie le mot de passe associé au compte utilisateur.	Obligatoire si action=promote
Destination_systemID	ID système  Exemple : Destination_systemID=<IDsystème>	Ce paramètre est utilisé uniquement pour l'authentification SAP.	Obligatoire pour l'authentification SAP.
Destination_username	Texte au format libre.  Exemple : Destination_username=<nom utilisateur>	Ce paramètre spécifie le compte utilisateur que doit utiliser l'outil pour se connecter au CMS de la plateforme de BI.  <b>i Remarque</b>  L'administrateur délégué est pris en charge.	Obligatoire si action=promote

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
exportLocation	Texte au format libre. Extension <code>&lt;.lcmbiar&gt;</code> obligatoire  Exemple : exportLocation=C:/Backup/New.lcmbiar	Ce paramètre permet à l'utilisateur de spécifier l'emplacement du fichier LCMBIAR après l'exportation et le regroupement en lot des objets.	Obligatoire si action=export
exportDependencies	false, true  Exemple : exportDependencies=<true ou false>	Ce paramètre spécifie les dépendances d'objet que l'outil rassemble pour l'exportation. Il s'applique uniquement lorsqu'il est utilisé conjointement avec l'indicateur Source_CMS.	Facultatif, utilisé si action=promote ou export  La valeur est false s'il n'est pas spécifié.
exportQuery	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'  <b>i Remarque</b>  Vous pouvez avoir le nombre de requêtes que vous souhaitez dans un seul fichier de propriétés mais elles doivent être nommées exportQuery1, exportQuery2.	Il s'agit des requêtes que l'outil doit exécuter pour rassembler les objets à exporter.	Facultatif, utilisé si action=promote or export
exportQueriesTotal	Nombres entiers positifs exportQueriesTotal=<nombre entier>	Ce paramètre permet à l'utilisateur de 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.	Facultatif, utilisé si action=promote ou export  S'il n'est pas spécifié, la valeur par défaut est 1

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
importLocation	Texte au format libre. Extension <code>&lt;.lcmbiar&gt;</code> obligatoire  Exemple : <code>importLocation=C:/Backup/New.lcmbiar</code>	Ce paramètre permet à l'utilisateur de spécifier l'emplacement du fichier LCMBIAR qui contient les objets à promouvoir.	Facultatif si <code>action=promote</code>
includeApplicationSecurity	false, true  Exemple : <code>includeApplicationSecurity=&lt;true ou false&gt;</code>	Ce paramètre donne à l'outil l'instruction d'exporter ou d'importer la sécurité associée aux applications sélectionnées.	Facultatif, la valeur est false s'il n'est pas spécifié.  Utilisé si <code>action=promote</code> or <code>export</code>
includeSecurity	false, true  Exemple : <code>includeSecurity=&lt;true ou false&gt;</code>	Ce paramètre 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.	Facultatif, la valeur est false s'il n'est pas spécifié.  Utilisé si <code>action=promote</code> or <code>export</code>
JOB_CUID	Le CUID du travail de gestion des promotions enregistré.	Ce paramètre donne à l'outil l'instruction d'exporter tous les objets du travail vers le fichier LCMBIAR.	Facultatif, utilisé si <code>action=export</code> or <code>promote</code>
lcmbiarpassword	Texte au format libre  Exemple : <code>java -cp lcm.jar com.businessobjects.lcm.cli.LCMCLI -lcmproperty lcm.properties -lcmbiarpassword "&lt;motdepasstest&gt;"</code>	Ce paramètre permet le cryptage et le décryptage de fichiers BIAR à l'aide d'un mot de passe.	Facultatif. S'il n'est pas spécifié ou si la chaîne est vide, aucun cryptage ne sera appliqué
lcmproperty	Chemin complet de l'emplacement où le fichier de propriété a été sauvé  <code>lcm_cli.bat -lcmproperty &lt;chemin d'accès au fichier de propriété&gt;</code>	Ce paramètre fait référence aux valeurs, enregistrées dans un fichier, requises pour l'exécution d'une commande.	Obligatoire



Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
limitQueryBatchSize	false, true  Exemple : limitQueryBatchSize=<true ou false>	Ce paramètre limite le nombre d'objets renvoyés à 1 000 par défaut. Lorsque ce paramètre est défini sur faux, tous les objets demandés sont renvoyés.  <b>i Remarque</b>  Vous pouvez aussi définir explicitement la nouvelle limite pour le nombre d'objets renvoyés par la requête à l'aide de  select TOP <nombre>	Facultatif, la valeur par défaut est true s'il n'est pas spécifié
LCM_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3  Exemple : LCM_authentication=<authentication>	Ce paramètre indique le type d'authentification à utiliser.	Facultatif. Si le type d'authentification n'est pas spécifié, secEnterprise est utilisé
LCM_clientID	ID client  Exemple : LCM_clientID=<IDclient>	Ce paramètre est utilisé pour l'authentification SAP.	Obligatoire pour l'authentification SAP.
LCM_CMS	Texte au format libre.  Exemple : LCM_CMS=<nomduCMS:numéroduport>	Ce paramètre permet à l'utilisateur de spécifier le CMS de l'outil de gestion des promotions.	Obligatoire si action=promoteur ou export
LCM_password	Texte au format libre.  Exemple : LCM_password=<mot de passe>	Ce paramètre permet à l'utilisateur de spécifier le mot de passe du compte utilisateur.	Obligatoire si action=promoteur ou export
LCM_systemID	ID système  Exemple : LCM_systemID=<IDsystème>	Ce paramètre est utilisé pour l'authentification SAP.	Obligatoire pour l'authentification SAP.

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
LCM_userName	Texte au format libre.  Exemple : LCM_userName=<nom utilisateur>	Ce paramètre permet à l'utilisateur de spécifier le nom d'utilisateur du compte que doit utiliser l'outil pour se connecter au CMS de l'outil de gestion des promotions.  <b>i Remarque</b> L'administrateur délégué est pris en charge.	Obligatoire si action=promote or export
Source_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3  Exemple : Source_authentication=<authentification>	Ce paramètre indique le type d'authentification à utiliser.	Facultatif. Si le type d'authentification n'est pas spécifié, secEnterprise est utilisé
Source_clientID	ID du client SAP  Exemple : Source_clientID=<ID système>	Ce paramètre est utilisé uniquement pour l'authentification SAP.	Obligatoire pour l'authentification SAP.
Source_CMS	Texte au format libre.  Exemple : Source_CMS=<Nom du CMS: numéro du port>	Ce paramètre permet à l'utilisateur de spécifier le CMS auquel doit se connecter l'outil.	Obligatoire si action=export
Source_password	Texte au format libre.  Exemple : Source_password=<mot de passe>	Ce paramètre spécifie le mot de passe associé au compte utilisateur.	Obligatoire si action=export
Source_systemID	SAP System ID  Exemple : Source_systemID=<ID système>	Ce paramètre est utilisé uniquement pour l'authentification SAP.	Obligatoire pour l'authentification SAP.
Source_username	Texte au format libre.  Exemple : Source_username=<nom utilisateur>	Ce paramètre spécifie le compte utilisateur que doit utiliser l'outil pour se connecter au CMS de la plateforme de BI.  <b>i Remarque</b> L'administrateur délégué est pris en charge.	Obligatoire si action=export

Paramètre	Valeurs autorisées	Description	Obligatoire ou Facultatif
stacktrace	true ou false  Exemple : stacktrace=<true ou false>	Ce paramètre permet à l'utilisateur de tracer tous les appels.	Facultatif, la valeur par défaut est false s'il n'est pas spécifié

#### 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.

## 15.7.4 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>
lcmbiarpasword=<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.

## 15.8 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 \(BC-CTS\)](#)

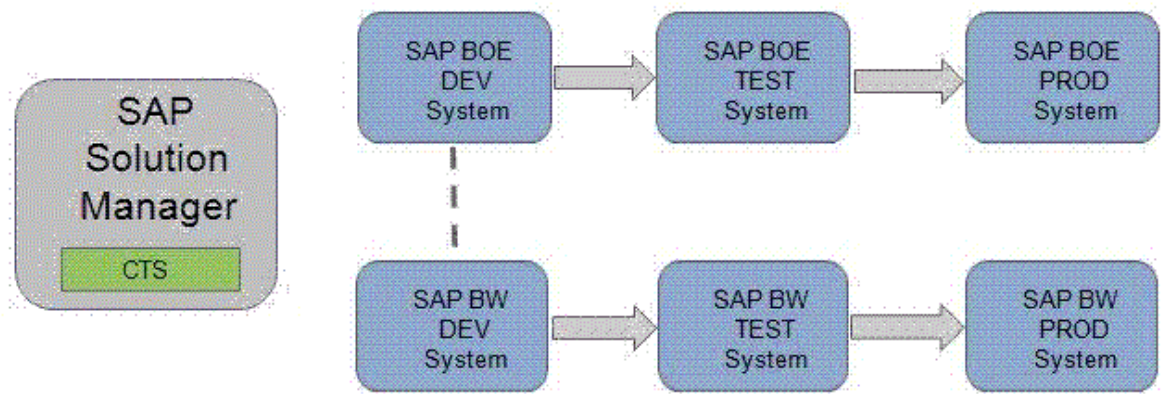
Pour en savoir plus sur le CTS+ (Enhanced Change and Transport System), voir [Transporting Non-ABAP Objects in Change and Transport System](#)

### 15.8.1 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, voir la note SAP : [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 [Note SAP 1369301](#) .
5. Le paysage de transport de SAP Business Warehouse (SAP BW) est configuré dans le CTS (Change and Transport System).
6. La [Note SAP 1692417](#)  et la [Note SAP 1860594](#)  ont été implémentées sur l'ordinateur hébergeant le service Web de déploiement CTS.

## 15.8.2 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.

### **i** 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 \[page 570\]](#)

[Pour configurer les paramètres CTS+ dans l'outil de gestion des promotions \[page 570\]](#)

[Pour configurer la plateforme de BI et l'intégration CTS+ \[page 569\]](#)

## 15.8.2.1 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.

## 15.8.2.2 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 de système 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.

### i 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](#).

## 15.8.2.3 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](#).

## 15.8.2.4 Pour exporter depuis la plateforme de BI vers CTS+ avec SSL

### 15.8.2.4.1 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](#).

### 15.8.2.4.2 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.

### 15.8.2.4.3 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)*.

### 15.8.2.4.4 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.

### 15.8.2.5 Pour importer depuis CTS+ vers la plateforme de BI avec SSL

#### 15.8.2.5.1 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 1024 -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

Un chaîne mise en forme s'affichera (par exemple, CN=John Smith, OU=Comptabilité, 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+ \[page 573\]](#)

### 15.8.2.5.2 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+ \[page 573\]](#)

### 15.8.2.5.3 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.

## 15.8.3 Pour promouvoir un travail à l'aide de CTS

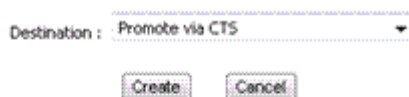
Cette section décrit le workflow pris en charge par l'outil de gestion des promotions pour promouvoir les objets du CMS (Central Management Server) de la plateforme de Business Intelligence depuis le système source jusqu'au système de destination à l'aide du CTS (Change Transport System). Pour utiliser 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](#).

**i 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 :
- Connectez-vous au contrôleur de domaine de CTS+.
  - Appelez la transaction **STMS** pour saisir le système de gestion du transport.
  - 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.
  - 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.
  - Cliquez sur [Actualiser](#).
  - 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 :
- Libérez les dépendances SAP BW vers le système de destination en procédant comme suit :
    - Connectez-vous au système SAP BW source.
    - Appelez la transaction SE09. L'écran [Transport Organizer](#) apparaît.
    - Cliquez sur [Affichage](#). La demande SAP BW s'affiche.
    - Cliquez sur la demande SAP BW et développez-la pour afficher les travaux créés pour les dépendances.
    - 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.
    - Cliquez avec le bouton droit sur la requête associée à l'objet BW principal et sélectionnez [Libérer directement](#).
    - Actualisez l'écran jusqu'à ce que les demandes soient libérées.

**i Remarque**

Vous pouvez afficher les journaux associés à une demande en cliquant deux fois dessus.

- Importez les dépendances SAP BW vers le système de destination en procédant comme suit :
  - Connectez-vous au système SAP BW de destination.
  - Appelez la transaction STMS pour saisir le système de gestion du transport.
  - Cliquez sur l'icône [Présentation de l'importation](#). L'écran [Présentation de l'importation](#) s'affiche.
  - 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.
  - 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 \[page 535\]](#)

[Pour gérer les dépendances d'un travail \[page 540\]](#)

# 16 Gestion des versions

## 16.1 Pour gérer 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.

### i Remarque

ClearCase n'est pas inclus dans l'installation de la plateforme de BI. Pour l'utiliser avec la gestion des versions, vous devez l'installer.

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](#).

### i 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 versionné 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.

## 16.2 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`.

## 16.3 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`.

## 16.4 Utilisation de l'option Paramètres du système de gestion des versions

Vous pouvez définir les paramètres du système de gestion des versions et configurer les paramètres de SubVersion et ClearCase 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`

- Sélectionnez [SVN](#), [HTTP](#) ou [HTTPS](#).

**i Remarque**

Pour en savoir plus sur la connexion à SubVersion à l'aide de HTTPS, voir la *Apache Subversion Documentation*.

- (Facultatif) Cliquez sur [Tester VMS](#) pour valider les paramètres VMS.
- Cliquez sur [Enregistrer](#).

**i 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.

## 16.4.1 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 :

Table 81 :

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
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

## 16.4.2 Configuration du système de gestion des versions ClearCase dans Windows

Pour définir le système de gestion des versions ClearCase dans Windows, procédez comme suit :

1. Dans la fenêtre *Options d'administration*, cliquez sur *Paramètres VMS*.
2. Dans la liste déroulante *Systèmes de gestion des versions*, sélectionnez *ClearCase*.
3. Saisissez les détails suivants :
  - Mappage du lecteur ClearCase : Saisissez le nom du lecteur. Par défaut, il s'agit du lecteur M. Par exemple : M:
  - Nom de l'onglet VOB : Saisissez le nom de la base d'objets versionnés (VOB). Par exemple : VBVendredi
  - Afficher le répertoire de stockage : Saisissez le chemin vers le dossier partagé. Par exemple : \\NomHôte\NomDossier

### Remarque

Le nom d'hôte ne doit pas être indiqué comme localhost.

4. Cliquez sur *Enregistrer*.
5. Pour utiliser ClearCase comme système de gestion des versions par défaut, sélectionnez *Utiliser comme VMS par défaut*.

## 16.4.3 Configuration du système de gestion des versions ClearCase dans Unix

Pour définir le système de gestion des versions ClearCase dans Unix, procédez comme suit :

1. Dans la fenêtre d'Options d'administration, cliquez sur *Paramètres VMS*.
2. Dans la liste déroulante Système de gestion des versions, sélectionnez *ClearCase*.
3. Saisissez les détails suivants :
  - Mappage du lecteur ClearCase : Saisissez le nom du dossier où est situé le MVFS. Par défaut, il s'agit de /view
  - Nom de l'onglet VOB : Saisissez le nom du dossier où est située la VOB. Par exemple : DossierVob/NomVob
  - Afficher le répertoire de stockage : Saisissez le chemin du répertoire où sont créées les vues.
4. Cliquez sur *Enregistrer*.
5. Pour utiliser ClearCase comme système de gestion des versions par défaut, sélectionnez *Utiliser comme VMS par défaut*.

## 16.5 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.

## 16.6 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 3.x.
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.

## 16.7 Configuration de Subversion pour les Job Server de traitement groupés

### 16.7.1 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.

### 16.7.2 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.

#### **i** 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://
<ORDINATEUR_SUBVERSION>:3690/svn_repository \\<PARTAGE_SUBVERSION>\CheckOut
\<NOM_ESPACEDETRAVAIL>-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.

#### **i** 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 : \\<PARTAGE\_SUBVERSION>\CheckOut
8. Arrêtez le Server Intelligence Agent (SIA) et remplacez le compte LocalSystem par l'administrateur du système d'exploitation.
9. Démarrez le SIA.

#### **i** 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.

## 16.7.3 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.

#### **i** 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.

## 16.8 Pour accéder à la même vue ClearCase depuis plusieurs serveurs de gestion des versions

1. Configurez l'ordinateur ClearCase principal.

Cet ordinateur hébergera les fichiers internes et les métadonnées utilisés par ClearCase. Les autres ordinateurs seront connectés à cet ordinateur.

2. Configurez l'ordinateur ClearCase secondaire.

Cet ordinateur se connectera et partagera les vues de l'ordinateur ClearCase principal.

### ➔ N'oubliez pas

N'installez pas de composants de serveurs (tels que le serveur de base d'objets versionnés (VOB) ou le serveur de visualisation) avec les packages Clearcase.

3. Ajoutez le nom de l'ordinateur ClearCase principal pour l'utiliser en tant que serveur de registre.
4. Ne suivez pas les étapes indiquées dans la section « Création d'un VOB ». Démarrez la vue principale localement et installez le VOB.
  - a. 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.
  - b. Affichez la vue localement en exécutant la commande suivante : `cleartool startview <NOM_VUE>`  
La vue apparaît sur l'ordinateur ClearCase secondaire.
  - c. Installez le VOB en exécutant la commande suivante : `cleartool mount \<VOB_TAG>`



# 17 Différence visuelle

## 17.1 Différence visuelle dans l'outil de gestion des promotions

La différence visuelle permet de visualiser les différences existant entre deux versions d'un type de fichier (LCMBIAR) ou d'objet (travail LCM) pris en charge, ou bien 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.

### Remarque

Pour utiliser la différence visuelle, vous devez installer Adobe Flash Viewer.

Voici les trois types de différence visuelle que vous pouvez détecter dans un fichier ou un objet :

- Supprimé - Dans un rapport, s'il manque un élément dans l'une des versions du fichier, le type de différence affiché est Supprimé. Par exemple, l'élément peut être une ligne, une instance de section, voire un bloc.
- Modifié - Dans un rapport, s'il existe une valeur différente entre la version source et la version de destination, le type de différence affiché est Modifié. Par exemple, la valeur peut être le contenu de la cellule ou une variable locale.
- Inséré - Dans un rapport, s'il existe un élément dans la version de destination qui n'est pas présent dans la version source, le type de différence affiché est Inséré.

Voici les types d'objet prenant en charge la différence visuelle :

- LCMBIAR
- Travail de gestion des promotions

Vous pouvez comparer les combinaisons suivantes :

- Un travail de gestion des promotions avec un autre travail de gestion des promotions
- Un travail de gestion des promotions avec un fichier LCMBIAR
- Un fichier LCMBIAR avec un autre fichier LCMBIAR
- Un fichier LCMBIAR avec un travail de gestion des promotions

## Préférences

Sur la page d'accueil de la fonction de différence visuelle, vous pouvez configurer des préférences telles que les paramètres régionaux du produit, les paramètres régionaux de visualisation préférés, le nombre maximum d'objets par page, le fuseau horaire et les invites relatives aux données non enregistrées.

## 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

### 17.1.1 Comparaison d'objets ou de fichiers à l'aide de la différence visuelle

L'option de différence visuelle permet de comparer les fichiers et les objets BIAR.

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, cliquez sur l'icône Dossier.

3. Cliquez sur [Nouvelle comparaison](#).  
L'écran [Différence visuelle - Comparaisons](#) s'affiche.
4. Sélectionnez le système de référence dans [Sélectionner un système](#) sous Référence.  
Vous pouvez vous connecter à l'un des systèmes de référence suivants :
  - CMS
  - VMS
  - Système de fichiers local
5. Cliquez sur [Parcourir](#) pour sélectionner l'objet ou un fichier de votre système local à comparer.
6. Sélectionnez le système cible dans [Sélectionner un système](#) sous Cible.  
Vous pouvez vous connecter à l'un des systèmes de référence suivants :
  - CMS
  - VMS
  - Système de fichiers local

#### Remarque

Si vous vous connectez au CMS ou au VMS, l'objet sélectionné du système de référence peut également être mis en correspondance automatiquement avec un objet du même nom dans le système de référence.

7. Cliquez sur [Parcourir](#) pour sélectionner l'objet ou un travail de votre système local à comparer.

8. Cliquez sur [Ajouter](#).

Les objets sélectionnés pour la comparaison sont ajoutés au panier.

Si plusieurs paires d'objets sont ajoutées au panier, une comparaison ultérieure des objets peut être planifiée. Cependant, si le panier contient une seule paire d'objets, vous pouvez les comparer.

Pour comparer les fichiers, passez à l'étape suivante. Pour planifier la comparaison, voir [Planification de la comparaison \[page 592\]](#).

9. Cliquez sur [Comparer](#) pour comparer les objets ou les dossiers.

#### **i** Remarque

La comparaison du fichier de travail LCMBIAR/gestion des promotions inclut les points suivants :

- Métadonnées LCMBIAR : comparaison des détails des travaux, tels que le nom, le créateur, la date et l'heure.
- Objets principaux : comparaison de chacun des objets explicitement sélectionnés dans le fichier LCMBIAR par rapport à un objet similaire dans le fichier LCMBIAR cible par le CUID.
- Objets dépendants : comparaison de l'objet dépendant sélectionné dans le fichier par rapport à un objet similaire dans le fichier cible par le CUID.

Si les objets autres qu'un travail LCMBIAR ou de gestion des promotions sont sélectionnés, le message d'erreur suivant est affiché : `Plugin introuvable`.

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](#).

## **17.1.2 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.

#### **i** 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. Pour planifier la comparaison, voir *Planification de la comparaison* [page 592].
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*.

### 17.1.3 Planification de la comparaison

Pour planifier la comparaison de fichiers ou d'objets, procédez comme suit :

1. Cliquez sur *Planifier*.  
La fenêtre *Planifier* s'affiche.
2. Sélectionnez la fréquence de planification de la comparaison dans la liste *Comparer*.
3. Spécifiez dans les champs appropriés le nombre de tentatives autorisé et l'intervalle entre chaque tentative.

#### Remarque

Pour spécifier un intervalle entre les tentatives, vous devez spécifier le nombre de tentatives.

4. Spécifiez le nom du rapport et cliquez sur *Parcourir* pour rechercher l'emplacement où vous souhaitez enregistrer le rapport.  
La fenêtre *Enregistrer le travail dans* apparaît.
5. Spécifiez le dossier dans lequel vous souhaitez enregistrer le rapport, puis cliquez sur *OK*.

#### Remarque

En fonction de l'option sélectionnée dans la liste *Comparer*, vous devez spécifier la date et l'heure de la comparaison.

6. Cliquez sur *Planifier*.

---

L'utilisateur peut afficher ultérieurement dans le visualiseur de différence visuelle l'objet de comparaison ou le rapport de différences. La page [Différences comparées](#) s'affiche avec la liste des dossiers et des fichiers ou des rapports de comparaison.

La page Différence comparée contient également les options suivantes :

- [Historique](#) Cette option permet d'afficher l'historique de la comparaison.
- [Réexécuter](#) Cette option permet de relancer l'exécution de la comparaison.
- [Planifier](#) Cette option permet de planifier la comparaison.

---

# 18 Gestion des applications

## 18.1 Gestion des applications via la CMC

### 18.1.1 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
- Applications Web BEx
- Zone de lancement BI
- Espaces de travail BI
- Central Management Console
- Collaboration (avec SAP Jam ou SAP StreamWork)
- Configuration de Crystal Reports
- Tableaux de bord
- Desktop Intelligence
- Discussions
- Authentification HANA
- Outil de conception d'information
- Application de surveillance
- Outil de gestion de l'architecture mutualisée
- Application Information Steward
- Open Document
- Application de recherche de plateformes
- Gestion des promotions
- Outil de conversion de rapport
- SAP BusinessObjects Mobile
- SAP Lumira
- Outil de gestion de la traduction
- Outil de conception d'univers
- Outil de gestion de mise à niveau
- Gestion des versions
- Différence visuelle

- Web Intelligence
- Service Web RESTful
- Service Web
- Indicateurs

## 18.1.2 Paramètres courants pour les applications

### 18.1.2.1 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.*

### 18.1.2.2 Pour définir le niveau du journal 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, 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](#).


Le nouveau niveau du journal de suivi prend effet après la prochaine connexion à l'application Web.

## Informations associées

[Niveaux du journal de suivi \[page 596\]](#)

## 18.1.2.2.1 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 <code>.ini</code> ).
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	<div><p>Aucun message n'est filtré. Ce niveau est recommandé pour les besoins du débogage.</p><div> <b>Attention</b> 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.</div></div>

## 18.1.3 Paramètres spécifiques aux applications

### 18.1.3.1 Gestion des paramètres de l'application CMC

#### 18.1.3.1.1 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 la 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 la 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`

## 18.1.3.1.1 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 des programmes Java*.

Si vous sélectionnez *Exécuter des 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*.

## 18.1.3.1.2 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\win32_x86\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.

#### **i** 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.

### 18.1.3.1.2.1 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.

## 18.1.3.1.2.2 Partage des extensions de traitement entre plusieurs serveurs

### i 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 traitement Crystal 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.

### i 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.

## 18.1.3.1.3 Gestion de l'accès aux onglets de la CMC

### 18.1.3.1.3.1 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 \[page 602\]](#)

[Pour gérer l'autorisation de configurer l'accès aux onglets de la CMC pour d'autres utilisateurs ou groupes d'utilisateurs \[page 604\]](#)

## 18.1.3.1.3.2 Utilisation de l'accès aux onglets de la CMC

### 18.1.3.1.3.2.1 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*
  - *Événements*
  - *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](#)
  - [Authentications](#)
  - [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).

## 18.1.3.1.3.2.1.1 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.

#### **i** 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 \[page 606\]](#)

### 18.1.3.1.3.2.1.2 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.

#### **i** 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.

### 18.1.3.1.3.2.1.3 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.

#### i 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 <a href="#">Niveaux d'accès</a> , <a href="#">Dossiers</a> , <a href="#">Boîtes de réception</a> , <a href="#">Dossiers personnels</a> , <a href="#">Catégories personnelles</a> , <a href="#">Résultats de requête</a> , <a href="#">Sessions</a> et <a href="#">Utilisateurs et groupes</a> . Définissez tous les autres onglets sur <a href="#">Hérité</a> .
Administrateurs de contenu	Accordez l'accès à <a href="#">Calendriers</a> , <a href="#">Catégories</a> , <a href="#">Événements</a> , <a href="#">Dossiers</a> , <a href="#">Gestionnaire d'instances</a> , <a href="#">Catégories personnelles</a> , <a href="#">Dossiers personnels</a> , <a href="#">Profils</a> , <a href="#">Résultats de requête</a> et <a href="#">Univers</a> . Définissez tous les autres onglets sur <a href="#">Hérité</a> .
Administrateurs de serveurs	Accordez l'accès à <a href="#">Serveurs</a> et <a href="#">Applications</a> . Définissez tous les autres onglets sur <a href="#">Hérité</a> .

### 18.1.3.1.3.2.1.4 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.

#### i 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.

**i 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 \[page 600\]](#)

[Héritage de l'accès aux onglets de la CMC \[page 603\]](#)

### 18.1.3.1.3.2.1.5 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*.

### 18.1.3.1.3.2.2 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 \[page 607\]](#)

### 18.1.3.1.3.2.3 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.

#### **i** 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'utilisateur :

- 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.

#### **i** 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 \[page 602\]](#)

[Héritage de l'accès aux onglets de la CMC \[page 603\]](#)

## 18.1.3.2 Gestion des paramètres de discussion

Dans la zone [Applications](#) de la CMC de la plateforme de BI, il est possible de spécifier des paramètres au niveau système pour les threads de discussion.

L'application [Discussions](#) permet de gérer et d'interagir avec des threads de discussion de différentes façons, notamment de :

- Rechercher des threads de discussion selon les critères de recherche spécifiés.

- Trier les résultats de la recherche de threads de discussion.
- Supprimer des threads de discussion

### **i** Remarque

Les paramètres des droits utilisateur ne sont pas disponibles pour l'application Discussions. Vous pouvez néanmoins définir des droits sur les rapports individuels.

## 18.1.3.2.1 Pour rechercher un thread de discussion

Par défaut, la page [Discussions](#) affiche les titres de tous les threads de discussion. Seuls les threads de niveau racine sont affichés.

Pour parcourir la liste des threads de discussion, utilisez les boutons Précédent et Suivant. Vous pouvez également rechercher un thread ou groupe de threads particulier.

1. Accédez à la zone [Applications](#) de la CMC, puis sélectionnez [Discussions](#).
2. Cliquez sur ► [Gérer](#) ► [Gérer les threads](#) ►.  
La boîte de dialogue [Administration des notes](#) s'ouvre.
3. Dans la liste [Nom du champ](#), sélectionnez une option.

Option	Description
<a href="#">Titre du thread</a>	Effectue la recherche en fonction du titre du thread.
<a href="#">Date de création</a>	Effectue la recherche en fonction de la date de création.
<a href="#">Date de la dernière modification</a>	Effectue la recherche en fonction de la date de la dernière modification.
<a href="#">Auteur</a>	Effectue la recherche en fonction du nom de l'auteur.

4. Affinez votre recherche dans la deuxième liste.

### **i** Remarque

Les recherches ne respectent pas la casse.

- Si vous avez sélectionné [Titre du thread](#) ou [Auteur](#), choisissez l'une des options suivantes dans le deuxième champ.

Option	Description
<a href="#">est égal à</a>	Recherche les threads de discussion dont le titre ou le nom de l'auteur correspond exactement au texte indiqué dans le troisième champ.
<a href="#">est différent de</a>	Recherche les threads de discussion dont le titre ou le nom de l'auteur ne correspond pas exactement au texte indiqué dans le troisième champ.
<a href="#">contient</a>	Recherche les threads de discussion qui contiennent la chaîne de texte recherchée dans une partie du titre du thread ou du nom de l'auteur.

Option	Description
<a href="#">ne contient pas</a>	Recherche les threads de discussion qui ne contiennent pas la chaîne de texte dans une partie du titre du thread.

- Si vous avez sélectionné [Date de création](#) ou [Date de la dernière modification](#), choisissez l'une des options suivantes, puis indiquez une date de recherche.

Option	Description
<a href="#">avant</a>	Recherche les threads de discussion qui ont été créés ou modifiés avant la date de recherche.
<a href="#">après</a>	Recherche les threads de discussion qui ont été créés ou modifiés après la date de recherche.
<a href="#">entre</a>	Recherche les threads de discussion qui ont été créés ou modifiés entre les deux dates de recherche.

- Pour affiner encore votre recherche, utilisez le troisième champ de texte.
  - Si vous avez sélectionné une recherche se basant sur du texte dans les deux premiers champs, saisissez la chaîne de texte.
  - Si vous avez sélectionné une recherche basée sur une date, saisissez la ou les dates dans les champs appropriés.
- Cliquez sur [Rechercher](#).

### 18.1.3.2.2 Pour trier les résultats de la recherche de threads de discussion

Lorsque vous recherchez des threads de discussion, vous pouvez sélectionner le mode d'affichage des résultats de la recherche. Vous pouvez par exemple les trier par ordre alphabétique croissant et choisir le nombre de résultats à afficher par page.

- Accédez à la zone [Applications](#) de la CMC, puis sélectionnez [Discussions](#).
- Cliquez sur [Gérer](#) [Gérer les threads](#).  
La boîte de dialogue [Administration des notes](#) s'ouvre.
- Dans la liste [Trier par](#), sélectionnez une option de tri.

Option	Description
<a href="#">Titre du thread</a>	Permet d'effectuer un tri en fonction du titre d'un thread de discussion.
<a href="#">Date de création</a>	Permet d'effectuer un tri en fonction de la date de création du thread de discussion.
<a href="#">Date de la dernière modification</a>	Permet d'effectuer un tri en fonction de la date de la dernière modification d'un thread de discussion.
<a href="#">Auteur</a>	Permet d'effectuer un tri en fonction de l'auteur d'un thread de discussion particulier.

- Dans la deuxième liste, choisissez entre un affichage par ordre croissant ou décroissant des enregistrements.

5. Dans le troisième champ de texte, saisissez le nombre de résultats de thread de discussion à afficher sur chaque page.  
La valeur par défaut est 10 résultats par page.
6. Cliquez sur [Rechercher](#).

### 18.1.3.2.3 Pour supprimer un thread de discussion

Vous pouvez supprimer les threads de discussion figurant dans la zone [Applications](#) de la CMC dans la plateforme de BI.

1. Accédez à la zone [Applications](#) de la CMC, puis sélectionnez [Discussions](#).
2. Cliquez sur ► [Gérer](#) ► [Gérer les threads](#) ►.  
La boîte de dialogue [Administration des notes](#) s'ouvre.
3. Dans la liste des résultats, recherchez le thread de discussion à supprimer, puis sélectionnez-le.
4. Cliquez sur [Supprimer](#).

### 18.1.3.3 Gestion des paramètres de la zone de lancement BI

Dans la zone [Applications](#) de la CMC de la plateforme de BI, sélectionnez ► [Gérer](#) ► [Propriétés](#) ► pour visualiser les options d'affichage de la zone de lancement BI.

Pour la zone de lancement BI, vous pouvez accorder aux utilisateurs ou aux groupes les fonctionnalités suivantes :

- Modifier les préférences
- Organiser les dossiers
- Rechercher
- Filtrer les listes d'objets par type d'objet
- Afficher le dossier [Favoris](#)

Par exemple, si vous avez créé les dossiers d'utilisateurs à l'aide d'une convention d'affectation de noms standard, vous pouvez empêcher les utilisateurs d'organiser leurs propres dossiers.

#### Remarque

Par défaut, tous les utilisateurs ont accès à ces fonctionnalités.

#### 18.1.3.3.1 Pour modifier les 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 discussions des utilisateurs de la zone de lancement BI, cochez la case [Activer les discussions](#).

3. 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.

4. Cliquez sur [Enregistrer et fermer](#).

## 18.1.3.4 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.

### 18.1.3.4.1 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](#) ►.
3. Définissez une des options d'affichage suivantes :

Option	Description
<a href="#">Dimensions et détails</a>	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 <a href="#">OK</a> lorsque vous avez terminé.
<a href="#">Valeurs fluctuantes (indicateurs numériques)</a>	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 <a href="#">OK</a> lorsque vous avez terminé.
<a href="#">Propriétés de l'image incorporée</a>	Saisissez la taille maximale de l'image incorporée.
<a href="#">Propriétés du mode d'affichage rapide</a>	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.
<a href="#">Paramètres d'enregistrement automatique</a>	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 enregistrez un document manuellement.
<a href="#">Actualisation automatique</a>	Active l'actualisation automatique des documents Web Intelligence quand leur propriété <a href="#">Actualisation automatique</a> est sélectionnée.  Pour en savoir plus, voir le <a href="#">Guide de l'utilisateur de SAP BusinessObjects Web Intelligence</a> .
<a href="#">Fusion automatique</a>	Active la fusion automatique des dimensions quand la propriété de document Web Intelligence <a href="#">Fusionner automatiquement les dimensions</a> est sélectionnée.  Pour en savoir plus, voir le <a href="#">Guide de l'utilisateur de SAP BusinessObjects Web Intelligence</a> .

Option	Description
<a href="#">Actualisation automatique du document à l'ouverture du paramètre du droit de sécurité</a>	Décochez cette option pour permettre à Web Intelligence d'actualiser les documents automatiquement à l'ouverture, sans activer l'option <a href="#">Actualisation à l'ouverture</a> dans les propriétés du document Web Intelligence. La sélection de cette option sélectionne le droit de sécurité <a href="#">Documents : désactiver l'actualisation automatique à l'ouverture</a> .
<a href="#">Vue intelligente</a>	Cette option détermine quelle version du document est affichée lorsque les utilisateurs ouvrent des documents dans Web Intelligence. <ul style="list-style-type: none"> <li>○ 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. Quand un utilisateur enregistre cette instance, le document d'origine est mis à jour en conséquence.</li> <li>○ 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.</li> </ul>

4. Cliquez sur [Enregistrer & Fermer](#).

#### Remarque

Pour remplacer vos sélections par les variables d'affichage par défaut, cliquez sur [Réinitialiser](#).

## 18.1.3.5 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 \[page 595\]](#)



## 18.1.3.5.1 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 \[page 595\]](#)

[Gestion des paramètres d'alerte \[page 612\]](#)

## 18.1.3.5.2 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
<a href="#">Période d'expiration</a>	Spécifie la période pendant laquelle les messages d'alerte seront conservés dans le système avant d'être supprimés.
<a href="#">Nombre maximal de messages d'alerte</a>	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 \[page 612\]](#)

## 18.1.3.6 Gestion des paramètres d'indicateur

Indicateurs de SAP BusinessObjects est une application bureau qui permet aux utilisateurs d'ajouter des mini applications sur leur bureau pour accéder facilement au contenu de Business Intelligence dans les applications de la plateforme de BI et Web Dynpro sur des serveurs d'applications SAP NetWeaver .

Dans la zone "Applications" de la CMC, vous pouvez contrôler l'accès permettant aux utilisateurs de créer et d'utiliser des indicateurs sur leur bureau et déterminer s'ils peuvent effectuer des recherches dans le référentiel de la plateforme de BI depuis l'application d'indicateurs sur leur bureau.

Vous pouvez accorder aux utilisateurs ou aux groupes le droit d'effectuer les opérations suivantes :

- Utiliser des indicateurs
- Modifier des objets créés par des indicateurs
- Modifier des droits utilisateur pour l'accès aux objets

#### Remarque

Par défaut, tous les utilisateurs généraux ont accès à ces fonctionnalités.

### 18.1.3.7 Gestion des paramètres de SAP BusinessObjects Explorer

Vous pouvez définir les fonctions accessibles aux utilisateurs pour SAP BusinessObjects Explorer en définissant leurs droits de sécurité dans la zone Applications de la CMC.

#### 18.1.3.7.1 Modification des propriétés de l'application SAP BusinessObjects Explorer

1. Accédez à la zone [Applications](#) de la CMC.
2. Cliquez sur ► [Gérer](#) ► [Propriétés](#) ►.  
La boîte de dialogue [Propriétés](#) s'affiche.
3. Définissez l'un des paramètres SAP BusinessObjects Explorer suivants :
  - Validité des signets
  - Configuration avancée
4. Cliquez sur [Enregistrer et fermer](#).

### 18.1.3.8 Gestion de l'intégration d'application de collaboration

Ce guide est destiné aux administrateurs de la plateforme de BI qui procéderont à l'intégration de l'application de collaboration SAP Jam ou SAP StreamWork 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 ou SAP StreamWork configurée, les flux sont disponibles dans la zone de lancement BI.

SAP Jam ne prend pas en charge Microsoft Internet Explorer 11.

#### 18.1.3.8.1 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 ou SAP StreamWork) doit être configurée dans la Central Management Console (CMC).
- Une application de collaboration (SAP Jam ou organisation Enterprise SAP StreamWork) doit être définie.
- Les utilisateurs de SAP Jam ou de SAP StreamWork doivent appartenir à l'organisation Enterprise.
- Un agent SAP Jam ou Enterprise SAP StreamWork est requis pour mettre en service les utilisateurs qui utilisent un service de répertoire LDAP/AD sur site.

## 18.1.3.8.2 Configuration de la plateforme de BI

### 18.1.3.8.2.1 Options de configuration de la collaboration

Les options de collaboration s'affichent dans la boîte de dialogue *Propriétés : Collaboration* de 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* ►.

Table 82 :

Option	Description
<i>Activer la collaboration</i>	Cochez cette case, puis sélectionnez <i>SAP Jam</i> ou <i>SAP StreamWork</i> .
<i>Connexion URL (URL de connexion)</i>	Saisissez l'URL de l'application de collaboration.
<i>ID du fournisseur d'identité unique</i>	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.
<i>Certificat en base 64 du fournisseur d'identité</i>	Lorsque vous cliquez sur <i>Générer</i> , 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.
<i>Clé du consommateur OAuth</i>	Saisissez la clé consommateur OAuth générée par la console d'administration de l'application de collaboration.

Option	Description
<a href="#">Connexion à l'aide du proxy</a>	<p>Cochez cette case pour activer la connexion par proxy et saisissez les informations d'hôte proxy dans les zones <a href="#">Hôte proxy HTTP</a> et <a href="#">Port</a>.</p> <p>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.</p> <p>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.</p>
<a href="#">Hôte proxy HTTP</a>	<p>Dans la configuration du proxy inverse, saisissez une adresse externe accessible à l'application de collaboration. Par exemple, utilisez <code>https://&lt;ProxyInverse&gt;/</code>, où <code>&lt;ProxyInverse&gt;</code> est le nom de domaine ou de sous-domaine du proxy inverse.</p> <p>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.</p>
<a href="#">Port</a>	<p>L'agent Enterprise de l'application de collaboration est configuré pour une écoute sur le port 8443.</p>

## 18.1.3.8.2.2 Activation et configuration de la collaboration dans la CMC

Cette tâche requiert une connexion valide à la console d'administration (SAP Jam ou SAP StreamWork) 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 ou SAP StreamWork :

- 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](#) ou [SAP StreamWork](#).
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 ou SAP StreamWork, 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](#).

## 18.1.3.8.3 Configuration de SAP Jam

### 18.1.3.8.3.1 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 Entreprise 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](#).

### 18.1.3.8.3.2 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 Entreprise 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 OAuth](#).
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.

## 18.1.3.8.4 Configuration de SAP StreamWork

### 18.1.3.8.4.1 Illustration de l'intégration à SAP StreamWork

Ce diagramme montre les composants d'agent de la plateforme de BI, SAP StreamWork et SAP StreamWork Enterprise requis pour l'intégration à SAP StreamWork.

Le workflow décrit les étapes impliquées dans l'intégration de systèmes ainsi qu'une présentation des actions que les utilisateurs peuvent effectuer après l'intégration :

- Dans l'agent Enterprise SAP StreamWork, les utilisateurs peuvent mettre en service les utilisateurs Enterprise à partir de LDAP vers SAP StreamWork.
- Dans la CMC de la plateforme de BI, les administrateurs peuvent créer des utilisateurs et les mapper aux utilisateurs Enterprise.
- Dans la zone de lancement BI, les utilisateurs peuvent créer des activités et les afficher dans un navigateur sans créer de compte ni se connecter à SAP StreamWork.
- Dans la zone de lancement BI, les utilisateurs peuvent afficher et répondre aux flux SAP StreamWork.



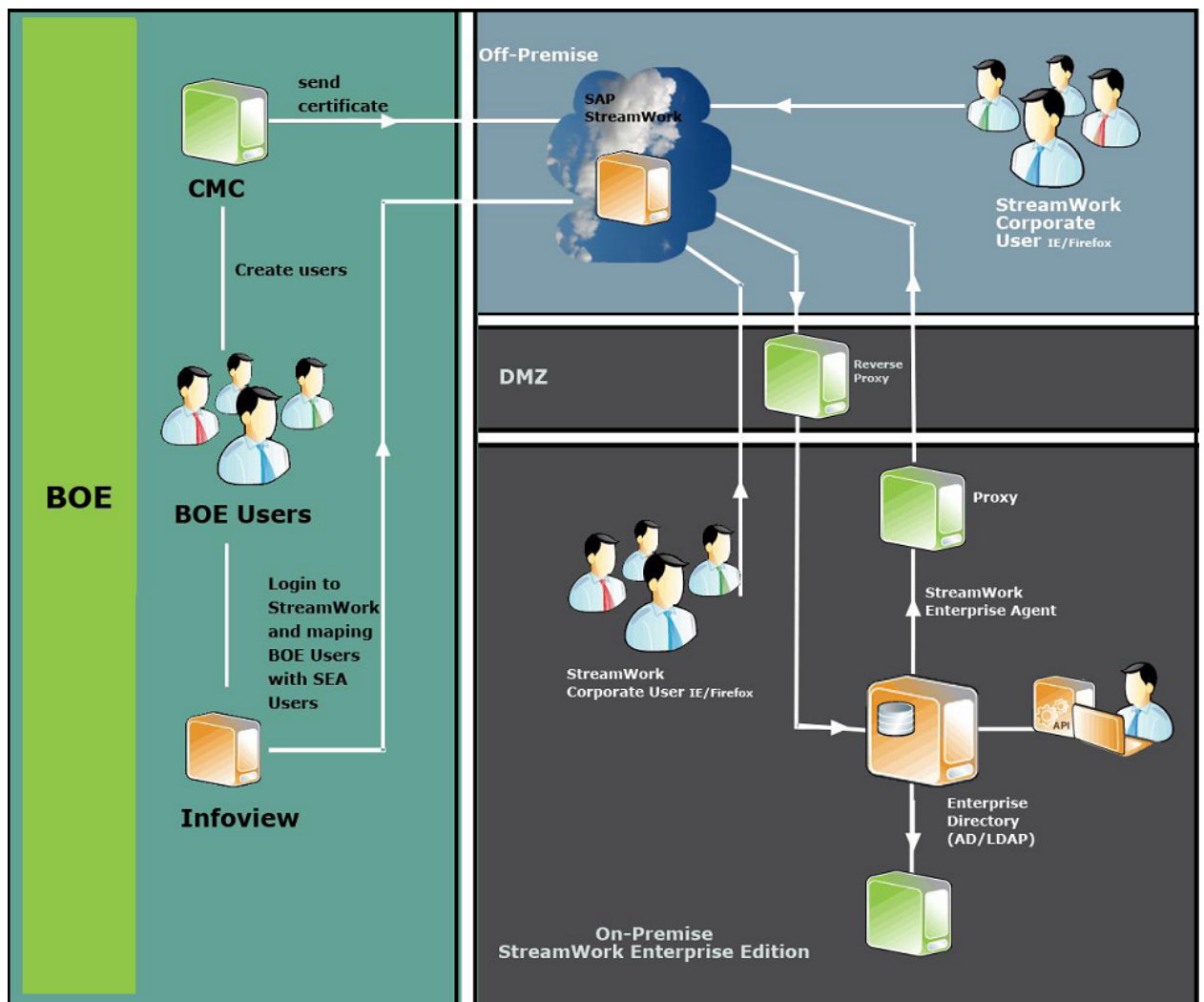


Figure 12 : Paysage système

#### 18.1.3.8.4.2 Création d'une clé du consommateur OAuth pour SAP StreamWork

Avant de pouvoir créer une clé du consommateur OAuth, vous devez disposer des droits d'administrateur pour l'organisation Enterprise SAP StreamWork.

1. Dans la console d'administration SAP StreamWork, dans l'onglet *Admin*, sélectionnez *IDP sécurisés SAML*, puis connectez-vous à SAP StreamWork avec un compte indiqué comme étant un compte d'administrateur d'organisation Enterprise.
2. Cliquez sur *Enregistrer votre fournisseur d'identité*.
3. Sélectionnez *Cliquer ici pour créer une nouvelle application administrative OAuth*, puis acceptez les Conditions d'utilisation.
4. Dans la fenêtre *Enregistrer une nouvelle application d'application OAuth*, effectuez les actions suivantes :
  - a. Dans la zone *Nom d'application*, saisissez le nom de l'instance d'application à utiliser dans l'intégration. Ces informations identifient quelle application est nécessaire pour effectuer des actions au nom d'un utilisateur (par exemple, publier un flux SAP StreamWork pour un utilisateur). Les utilisateurs doivent pouvoir reconnaître ce nom d'application.

- b. Dans la zone [URL d'intégration URL](#), saisissez l'URL de la zone de lancement BI.
- c. Dans la zone [Base64 X509 Certificate](#) (Certificat X509 (Base64)), saisissez la valeur du certificat en base 64 générée lors de la configuration de SAP StreamWork dans la CMC (Central Management Console) de la plateforme de BI.  
Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.
5. 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.
6. Cliquez sur [Retour](#) pour afficher les fournisseurs d'identité sécurisés SAML.
7. Dans la fenêtre [Enregistrer un nouveau fournisseur d'identité sécurisé SAML](#), effectuez les actions suivantes :
  - a. Dans la zone [Display Name](#) (Nom d'affichage), saisissez un nom pour le déploiement de la plateforme de BI.  
Ce nom s'affichera aux utilisateurs dans SAP StreamWork.
  - b. Dans la zone [IDP ID](#) (ID d'IDP), saisissez la valeur du fournisseur d'identité unique créé lors de la configuration de SAP StreamWork sur la plateforme de BI.  
Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.
  - c. Dans la zone [Base64 X509 Certificate](#) (Certificat X509 (Base64)), saisissez la valeur du certificat en Base64 générée lors de la configuration de SAP StreamWork sur la plateforme de BI.  
Si vous ne connaissez pas cette valeur, contactez l'administrateur de votre application externe.
8. Cliquez sur [Enregistrer](#).

### 18.1.3.8.4.3 Ajout de SAP StreamWork à un espace de travail BI

SAP StreamWork est masqué et doit être affiché manuellement dans la liste des modules de zone de lancement BI pouvant être ajoutés à un espace de travail BI.

1. Recherchez `C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\asdk-ivdm_ext.jar\conf-syst\conf-syst\home-analyticlist.xml`.

Le contenu du fichier doit débiter par le texte suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<CHOICE>
<!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$" />-->
<!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/-->
<HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$"/>
<HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$"
DESCRIPTION="$MSGHOMEAPPLICATIONSDESC$"/>
<HOMERECENTLYRUNDOS NAME="$MSG_HOMERECENTLYRUNDOS$"
DESCRIPTION="$MSG_HOMERECENTLYRUNDOSDESC$"/>
<HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$" DESCRIPTION="$MSG_HOMERECENTDOCSDESC$" />
<HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$"
DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$"/>
</CHOICE>
```

2. Supprimez les lignes `!-- from the SW_ACTIVITIES NAME=` and `SW_FEED NAME=`.

3. Redémarrez le serveur Tomcat.

*Flux SAP StreamWork* apparaît dans la liste *Modules de zone de lancement BI* de la bibliothèque de modules pour les espaces de travail BI, dans la zone de lancement BI.

## 18.1.3.9 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.

### 18.1.3.9.1 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 :

Table 83 :

Option	Description
Statistiques de recherche	La recherche de plateformes fournit les statistiques de recherche suivantes : <ul style="list-style-type: none"><li>○ Statut de l'indexation : affiche le statut du processus d'indexation.</li><li>○ Nombre de documents indexés : affiche le nombre de documents indexés.</li><li>○ Dernier horodatage indexé : affiche l'horodatage de la dernière indexation du document.</li></ul>
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 <i>Arrêter l'indexation</i> .
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	<p>Vous pouvez indexer l'ensemble du référentiel de la plateforme de BI à l'aide des options suivantes :</p> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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 <i>Planification d'un objet</i> de l'application de recherche de plateformes dans l'<i>Aide en ligne de la CMC de la plateforme SAP BusinessObjects Business Intelligence</i>.</li> </ul> <div> <p><b>i Remarque</b></p> <ul style="list-style-type: none"> <li>○ Si vous sélectionnez <i>Analyse planifiée</i> et définissez la <i>Périodicité</i> sur une option autre que <i>Maintenant</i>, l'application de recherche de plateformes affiche la date et l'horodatage de la prochaine indexation planifiée du document.</li> <li>○ Si vous sélectionnez <i>Analyse planifiée</i>, le bouton <i>Démarrer l'indexation</i> est activé et le bouton <i>Arrêter l'indexation</i> est désactivé.</li> <li>○ Une fois la planification terminée, le bouton <i>Arrêter l'indexation</i> est désactivé.</li> </ul> </div>

Option	Description
Emplacement de l'index	<p>Les index sont stockés dans des dossiers partagés aux emplacements suivants :</p> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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.</li> </ul> <p>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.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur&gt;\ContentStores.</p> <p>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 :</p> <ol style="list-style-type: none"> <li>1. {bobj.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur&gt;\ContentStores.</li> <li>2. {bobj.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur 1&gt;\ContentStores.</li> </ol> <ul style="list-style-type: none"> <li>○ 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.</li> </ul> <div> <p><b>i Remarque</b></p> <ul style="list-style-type: none"> <li>○ L'emplacement de l'index maître doit être un emplacement partagé.</li> <li>○ Vous devez cliquer sur <a href="#">Arrêter l'indexation</a> pour modifier l'emplacement de l'index.</li> <li>○ 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.</li> </ul> </div>

Option	Description
Niveau d'indexation	<p>Vous pouvez ajuster le contenu de la recherche en définissant le niveau d'indexation de l'une des façons suivantes :</p> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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.</li> <li>○ Contenu complet : cet index comprend les métadonnées de plateformes, les métadonnées de documents et les autres contenus tels que : <ul style="list-style-type: none"> <li>○ Le contenu réel du document</li> <li>○ Le contenu des invites et listes de valeurs</li> <li>○ Diagrammes, graphiques et étiquettes</li> </ul> </li> </ul> <div> <p><b>i Remarque</b></p> <p>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.</p> </div> <div> <p><b>i Remarque</b></p> <p>Lorsque vous modifiez le niveau d'indexation, l'indexation est initialisée pour l'actualisation de l'ensemble du référentiel de la plateforme de BI.</p> </div>

Option	Description
Types de contenus	<p>Vous pouvez sélectionner les types de contenu suivants pour l'indexation :</p> <ul style="list-style-type: none"> <li>○ Crystal Reports</li> <li>○ Web Intelligence</li> <li>○ Univers</li> <li>○ Espace de travail BI</li> <li>○ Analysis Office</li> <li>○ Lumira</li> <li>○ Microsoft PowerPoint</li> <li>○ Adobe Acrobat</li> <li>○ Texte enrichi</li> <li>○ Texte</li> <li>○ Microsoft Word</li> <li>○ Microsoft Excel</li> </ul> <p>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.</p> <p>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.</p>
Régénérer l'index	<p>Cette option supprime les index existants et réindexe l'ensemble du référentiel.</p> <p>Vous pouvez sélectionner l'option <a href="#">Régénérer l'index</a>, 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.</p> <p>Si vous ne souhaitez pas que l'application de recherche de plateformes réindexe les documents, désélectionner l'option <a href="#">Régénérer l'index</a> avant de cliquer sur <a href="#">Démarrer l'indexation</a>.</p>

Option	Description
Documents exclus de l'indexation	<p>L'option <i>Documents exclus de l'indexation</i> 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.</p> <p>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 <i>Documents exclus de l'indexation</i> ne puissent pas être recherchés, vous devez régénérer l'index.</p> <p>Par défaut, seul le compte Administrateur dispose du contrôle complet de l'option <i>Documents exclus de l'indexation</i>. Les autres utilisateurs disposant des droits suivants peuvent seulement ajouter des documents aux <i>Documents exclus de l'indexation</i>.</p> <ul style="list-style-type: none"> <li>○ Droits de visualisation et de modification sur la catégorie</li> <li>○ Modifier le document directement</li> </ul>

5. Cliquez sur *Enregistrer et fermer*.

#### **i** 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.

## 18.1.3.10 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 630]

Démarrage d'un serveur autonome pour les BEx Web Applications [page 630]

Configuration des paramètres de serveur [page 630]

Vérification de la connexion au système BW [page 631]

Configuration d'une connexion entre BEx Web Application Designer et la plateforme de BI [page 632]

### 18.1.3.10.1 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.

### 18.1.3.10.2 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.

### 18.1.3.10.3 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.

#### **i** 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 \[page 633\]](#)

### 18.1.3.10.4 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.

#### **i** 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.

## 18.1.3.10.5 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 \[page 633\]](#)

## 18.1.3.10.5.1 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 \[page 630\]](#)

## 18.1.3.11 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.

#### **i** 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.

### 18.1.3.11.1 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 de base de données.
  - c. Enregistrez le nom de l'ordinateur hôte et le numéro de port.  
Vous aurez besoin de ces informations au cours de l'étape 2.
2. Configurez une connexion SAP HANA sur la plateforme de 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. Entrez le nom de l'ordinateur hôte et le numéro de port enregistrés à l'étape 1.
  - d. Dans le champ [ID du fournisseur d'identité unique](#), spécifiez une valeur à utiliser pour le déploiement de la plateforme de BI.
  - e. Cliquez sur [Régénérer](#).  
Un certificat est créé dans la zone [Certificat en Base64 du fournisseur d'identité](#).
3. Configurez votre déploiement SAP HANA.
  - a. A l'aide de l'application SAP HANA Studio, cliquez avec le bouton droit de la souris sur le système SAP HANA, puis sur [Propriétés](#).
  - b. Sélectionnez [SAML Configuration](#) (Configuration de SAML).
  - c. Cliquez sur [Ajouter](#).
  - d. Dans la boîte de dialogue [Create SAML Identity Provider](#) (Créer un fournisseur d'identité SAML), sélectionnez [Read from Certificate](#) (Lire à partir du certificat).
  - e. Cliquez sur [Open File](#) (Ouvrir le fichier) pour compléter les valeurs DN.
  - f. Cliquez sur [OK](#).
  - g. Redémarrez SAP HANA.
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.

## 18.1.3.11.2 Paramètres de connexion SAP HANA

Le tableau ci-dessous résume les paramètres disponibles dans la CMC pour configurer les connexions SAP HANA.

Table 84 :

Paramètre	Description
<i>Nom d'hôte HANA</i>	Fournissez le nom de votre hôte SAP HANA.
<i>Port HANA</i>	Fournissez le numéro de port de votre hôte SAP HANA.
<i>ID du fournisseur d'identité unique</i>	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.
<i>Certificat en base 64 du fournisseur d'identité</i>	Lorsque vous cliquez sur <a href="#">Générer</a> , un certificat est créé dans le champ <i>Certificat en base 64 du fournisseur d'identité</i> . Copiez ce certificat dans le fichier <code>trust.pem</code> 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.

## 18.1.3.12 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 Gestion des applications via les propriétés du fichier BOE.war

### 18.2.1 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`.

#### **i** 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 redéploier le fichier. Pour en savoir plus, voir le *Guide de déploiement d'applications Web de la plateforme SAP BusinessObjects Business Intelligence*.

#### 18.2.1.1 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
<code>persistentcookies.enabled</code>	<code>persistentcookies.enabled=true</code>	Active ou désactive les cookies persistants de la page de connexion de l'application Web.
<code>siteminder.authentication</code>	<code>siteminder.authentication=secLDAP</code>	Spécifie quelle méthode d'authentification utiliser avec SiteMinder. Les seules options sont <code>secLDAP</code> et <code>secwinAD</code> .
<code>siteminder.enabled</code>	<code>siteminder.enabled=false</code>	Active et désactive l'authentification avec SiteMinder.
<code>sso.enabled</code>	<code>sso.enabled=false</code>	Active et désactive la connexion unique (SSO) à la plateforme de BI.
<code>sso.sap.primary</code>	<code>sso.sap.primary=false</code>	Attribuez la valeur <code>true</code> 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.
<code>max.tree.children.threshold</code>	<code>max.tree.children.threshold=200</code>	Spécifie le seuil auquel le contrôle d'arborescence n'affiche pas l'ensemble des nœuds, mais un message "Nombre d'enfants trop important".
<code>trusted.auth.shared.secret</code>	Aucune	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.
<code>trusted.auth.user.param</code>	Aucune	Spécifie la variable utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée et peut être défini sur l'une des valeurs suivantes : <ul style="list-style-type: none"> <li>• En-tête</li> <li>• Paramètre URL</li> <li>• Cookie</li> <li>• Session</li> </ul>
<code>trusted.auth.user.retrieve</code>	Aucune	Spécifie la méthode utilisée pour extraire le nom d'utilisateur pour l'authentification sécurisée et peut être défini sur l'une des valeurs suivantes : <ul style="list-style-type: none"> <li>• "REMOTE_USER"</li> <li>• "HTTP_HEADER"</li> <li>• "COOKIE"</li> <li>• "QUERY_STRING"</li> <li>• "WEB_SESSION"</li> <li>• "USER_PRINCIPAL"</li> </ul> N'attribuez aucune valeur pour désactiver l'authentification sécurisée.
<code>trusted.auth.user.namepace.enabled</code>	<code>trusted.auth.user.namepace.enabled=false</code>	Active et désactive la liaison dynamique des alias aux comptes utilisateur existants. Si la valeur <code>true</code> est attribuée à la propriété, l'authentification sécurisée utilise la liaison d'alias pour authentifier les utilisateurs à la plateforme de BI. Avec la liaison d'alias, votre serveur d'applications peut

Paramètre	Valeurs par défaut	Description
		fonctionner comme un fournisseur de service SAML, activant par conséquent l'authentification sécurisée pour fournir une connexion unique SAML au système. Si la valeur <code>false</code> est attribuée, l'authentification sécurisée utilise la correspondance de noms pour authentifier les utilisateurs.
<code>vintela.enabled</code>	<pre>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</pre>	Permet d'activer ou de désactiver les paramètres Vintela pour l'authentification Windows AD.
<code>pinger.showWarningDialog.cmc</code>	<code>pinger.showWarningDialog.cmc=true</code>	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.
<code>pinger.showWarningDialog.bilaunchpad</code>	<code>pinger.showWarningDialog.bilaunchpad=true</code>	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.
<code>pinger.warningPeriod.pingIncrementsInSeconds</code>	<code>pinger.warningPeriod.pingIncrementsInSeconds=15</code>	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.
<code>pinger.warningPeriod.lengthInMinutes</code>	<code>pinger.warningPeriod.lengthInMinutes=5</code>	Spécifie combien de temps avant l'expiration de session l'avertissement doit être affiché.
<code>logoff.on.websession.expiry</code>	<code>logoff.on.websession.expiry=true</code>	Spécifie si toutes les sessions d'application se déconnectent lorsque la session Web expire.
<code>pinger.enabled</code>	<code>pinger.enabled=true</code>	Active ou désactive le mécanisme de message d'avertissement d'expiration de session.
<code>system.com.sap.bip.jcomanager.destinations.maxsize</code>	<code>system.com.sap.bip.jcomanager.destinations.maxsize=1000</code>	Spécifie le nombre maximal de connexions Java en cache.
<code>httpproxy.username</code>	<code>httpproxy.username=monnomd'utilisateur</code>	Spécifie le nom d'utilisateur pour se connecter au serveur proxy HTTP.
<code>httpproxy.password</code>	<code>httpproxy.password=monmotdepasse</code>	Spécifie le mot de passe pour se connecter au serveur proxy HTTP.
<code>logon.embed.secret</code>	Aucune	Secret partagé entre un portail qui intègre les applications de la plateforme de BI et le serveur

Paramètre	Valeurs par défaut	Description
		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.
<code>logon.embed.timeout</code>	<code>logon.embed.timeout=300</code>	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.
<code>iview.autologoff</code>	<code>iview.autologoff=true</code>	Définissez sur <code>true</code> pour permettre une déconnexion automatique immédiate des iViews de la plateforme technologique SAP NetWeaver.
<code>pinger.showWarningDialog</code>	<code>pinger.showWarningDialog=true</code>	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.
<code>ure.request.queue.timeout.seconds</code>	<code>ure.request.queue.timeout.seconds=20</code>	<p>Nombre de seconde d'attente des demandes précédentes attendues par une demande avant l'expiration.</p> <p>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 inattendu se produit dans la requête back-end.</p>

## 18.2.1.2 Propriétés de la zone de lancement BI

Le tableau suivant répertorie les paramètres inclus dans le fichier `bilaunchpad.properties` par défaut pour le fichier 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`.

Paramètres	Description
<code>app.name</code>	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 : <code>app.name=BI launch pad</code>

Paramètres	Description																		
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_launchpad																		
app.url.name	Spécifie le nom d'URL de l'application, précédé par le caractère « / ». Par défaut : app.url.name=/BI																		
authentication.default	<p>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 :</p> <table> <tr> <th>Authentification</th><th>Valeur de paramètre</th></tr> <tr> <td>Entreprise</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> <p>Par défaut : authentication.default=secEnterprise</p>	Authentification	Valeur de paramètre	Entreprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Authentification	Valeur de paramètre																		
Entreprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	Spécifie si les utilisateurs se connectant à la zone de lancement BI ont la possibilité de visualiser et modifier la méthode d'authentification. Par défaut : authentication.visible=false																		
cms.default	Spécifie le nom de CMS par défaut. Par défaut : cms.default=[nom de l'ordinateur hôte]																		
cms.visible	Spécifie si les utilisateurs se connectant à la zone de lancement BI ont la possibilité de visualiser et 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 de 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 <i>De</i> lors de la planification d'un objet vers une destination. Par défaut : SMTPFrom=true																		

Paramètres	Description
	<p>Lorsque la valeur est définie sur <code>false</code>, le champ <i>De</i> n'est pas affiché et le système tente d'extraire la valeur de courrier électronique <i>De</i> dans l'ordre suivant :</p> <ol style="list-style-type: none"> <li>1. D'abord à partir du rapport par défaut pour un objet rapport.</li> <li>2. Ensuite, à partir de l'adresse électronique dans le profil de l'utilisateur connecté.</li> <li>3. Pour terminer, à partir du Job Server par défaut.</li> </ol>
<code>url.exit</code>	Spécifie vers quelle URL rediriger les utilisateurs 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.
<code>disable.locale.preference</code>	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 : <code>disable.locale.preference=false</code>
<code>extlogon.allow.logoff</code>	Active ou désactive automatiquement la déconnexion des sessions utilisateur une fois que les utilisateurs ont fermé leur session de zone de lancement BI. Attribuez-y la valeur <code>false</code> si vous voulez que les sessions utilisateur ne se terminent pas lorsque les utilisateurs se déconnectent de la zone de lancement BI. Par défaut : <code>extlogon.allow.logoff=true</code>
<code>logon.allowInsecureEmbedding</code>	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 : <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Spécifie une liste séparée par des virgules des types de connexion unique à activer et l'ordre dans lequel elles sont exécutées.</p> <p>Une liste vide indique que l'ordre hérité doit être utilisé.</p> <p>Si la liste est spécifiée, les options d'héritage sont ignorées.</p> <p>Options valides : <code>vinetela</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVinetela</code>, <code>trustedX509</code>, <code>sapSSO</code> et <code>siteminder</code>.</p> <p>Si vous n'en voulez aucune, spécifiez : <code>none</code></p>

## 18.2.1.3 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`.

Paramètres	Description																		
<code>app.name</code>	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 : <code>app.name=SAP BusinessObjects OpenDocument</code>																		
<code>app.name.short</code>	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 : <code>app.name.short=OpenDocument</code>																		
<code>authentication.default</code>	<p>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 :</p> <table><tr><th>Authentification</th><th>Valeur de paramètre</th></tr><tr><td>Entreprise</td><td><code>secEnterprise</code></td></tr><tr><td>LDAP</td><td><code>secLDAP</code></td></tr><tr><td>Windows AD</td><td><code>secWinAD</code></td></tr><tr><td>SAP</td><td><code>secSAPR3</code></td></tr><tr><td>PeopleSoft</td><td><code>secpsenterprise</code></td></tr><tr><td>JD Edwards</td><td><code>secPSE1</code></td></tr><tr><td>Siebel</td><td><code>secSiebel7</code></td></tr><tr><td>Oracles EBS</td><td><code>secOraApps</code></td></tr></table> <p>Par défaut : <code>authentication.default=secEnterprise</code></p>	Authentification	Valeur de paramètre	Entreprise	<code>secEnterprise</code>	LDAP	<code>secLDAP</code>	Windows AD	<code>secWinAD</code>	SAP	<code>secSAPR3</code>	PeopleSoft	<code>secpsenterprise</code>	JD Edwards	<code>secPSE1</code>	Siebel	<code>secSiebel7</code>	Oracles EBS	<code>secOraApps</code>
Authentification	Valeur de paramètre																		
Entreprise	<code>secEnterprise</code>																		
LDAP	<code>secLDAP</code>																		
Windows AD	<code>secWinAD</code>																		
SAP	<code>secSAPR3</code>																		
PeopleSoft	<code>secpsenterprise</code>																		
JD Edwards	<code>secPSE1</code>																		
Siebel	<code>secSiebel7</code>																		
Oracles EBS	<code>secOraApps</code>																		
<code>authentication.visible</code>	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>																		
<code>cms.default</code>	Spécifie le nom de CMS par défaut. Par défaut : <code>cms.default=[nom de l'ordinateur hôte]</code>																		
<code>cms.visible</code>	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>																		
<code>logontoken.enabled</code>	Spécifie si la création de jeton doit ou non être activée pour la session après la connexion d'un utilisateur à OpenDocument.																		

Paramètres	Description
	Le jeton sera stocké dans un cookie. Par défaut : <code>logontoken.enabled=false</code>
<code>extlogon.allow.logoff</code>	Active ou désactive automatiquement la déconnexion des sessions utilisateur une fois que les utilisateurs ont fermé leur session OpenDocument. Attribuez-y la valeur <code>false</code> si vous voulez que les sessions utilisateur ne se terminent pas lorsque les utilisateurs se déconnectent d'OpenDocument. Par défaut : <code>extlogon.allow.logoff=true</code>
<code>SAPLogonToken.enabled</code>	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 <code>X-SAP-LogonToken</code> dans l'en-tête de requête après une connexion réussie à l'URL de service Web RESTful. Par défaut : <code>SAPLogonToken.enabled=true</code>
<code>logon.allowInsecureEmbedding=false</code>	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 : <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Spécifie une liste séparée par des virgules des types de connexion unique à activer et l'ordre dans lequel elles sont exécutées.</p> <p>Une liste vide indique que l'ordre hérité doit être utilisé.</p> <p>Si la liste est spécifiée, les options d'héritage sont ignorées.</p> <p>Options valides : <code>serializedSession</code>, <code>sapLogonToken</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVintela</code>, <code>vintela</code>, <code>infoview</code>, <code>trustedX509</code>, <code>sapSSO</code> et <code>siteminder</code>.</p> <p>Si vous n'en voulez aucune, spécifiez : <code>none</code></p>

## 18.2.1.4 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`.

Paramètres	Description
<code>app.url.name</code>	Spécifie le nom d'URL de l'application, précédé par le caractère « / »". Par défaut : <code>app.url.name=/CMC</code>

Paramètres	Description																		
authentication.default	<p>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 :</p> <table> <tr> <th>Authentification</th><th>Valeur de paramètre</th></tr> <tr> <td>Entreprise</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> <p>Par défaut : authentication.default=secEnterprise</p>	Authentification	Valeur de paramètre	Entreprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Authentification	Valeur de paramètre																		
Entreprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	<p>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</p>																		
cms.default	<p>Spécifie le nom de CMS par défaut. Par défaut : cms.default=[nom de l'ordinateur hôte]</p>																		
cms.visible	<p>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</p>																		
dialogue.prompt.enabled	<p>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</p>																		
logontoken.enabled	<p>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</p>																		
SMTPFrom	<p>Active ou désactive le champ <b>De</b> lors de la planification d'un objet vers une destination. Par défaut : SMTPFrom=true</p> <p>Lorsque la valeur est définie sur <code>false</code>, le champ <b>De</b> n'est pas affiché et le système tente d'extraire la valeur de courrier électronique <b>De</b> dans l'ordre suivant :</p> <ol style="list-style-type: none"> <li>1. D'abord à partir du rapport par défaut pour un objet rapport.</li> </ol>																		



Paramètres	Description
	<ol style="list-style-type: none"> <li>2. Ensuite, à partir de l'adresse électronique dans le profil de l'utilisateur connecté.</li> <li>3. Pour terminer, à partir du Job Server par défaut.</li> </ol>

## 18.3 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*.

### 18.3.1 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.

Table 85 : 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

Table 86 : 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

## 18.3.2 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.

### 18.3.3 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.

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 \[page 231\]](#)

[Pour configurer l'authentification sécurisée pour l'application Web \[page 236\]](#)

## 18.4 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.

### 18.4.1 Web Intelligence

#### 18.4.1.1 Personnalisation des éléments d'interface Web Intelligence par groupe d'utilisateurs ou dossiers

Dans la CMC, vous pouvez personnaliser l'apparence des éléments d'interface Web Intelligence pour un utilisateur en fonction du groupe d'utilisateurs auquel il appartient et des dossiers contenant des documents Web Intelligence. Par exemple, la barre d'outils dans sa totalité ou certains de ses éléments ; de même que l'accès personnalisé à certains modes de document. Vous pouvez aussi personnaliser Web Intelligence en activant des extensions.

Par défaut, tous les éléments d'interface sont visibles. Pour que des éléments spécifiques ne s'affichent pas, désélectionnez-les dans la CMC. Tous les points d'extension sont désactivés par défaut. Pour les rendre disponibles pour les utilisateurs, activez-les dans la CMC.

##### Remarque

- La personnalisation et les points d'extension activés sont applicables à tous les clients d'application Web Intelligence : HTML, applet Java et Rich Client.
- Il se peut que la personnalisation et les points d'extension activés ne fonctionnent pas sur Web Intelligence Rich Client en raison de la configuration de proxy ou de DNS. Pour résoudre ce problème, connectez-vous à la CMC à l'aide de l'adresse IP du serveur au lieu du nom du serveur lorsque vous personnalisez Web Intelligence : Cette adresse IP servira de référence durant la personnalisation.

#### 18.4.1.1.1 Interface de personnalisation

La section Personnalisation contient la section et les onglets suivants :

- Section Dossiers personnalisés  
Dans cette section, vous pouvez sélectionner les dossiers contenant des documents Web Intelligence pour lesquels vous souhaitez personnaliser l'interface utilisateur et activer des extensions.
- Onglet Éléments de l'interface utilisateur  
Dans cet onglet, vous pouvez sélectionner des éléments d'interface individuels à masquer, par exemple une barre d'outils ou un onglet, ou bien leurs sous-éléments, par exemple un bouton de commande.
- Onglet Fonctionnalités  
Dans cet onglet, vous pouvez choisir de masquer tous les éléments de l'interface utilisateur liés à une fonction, par exemple Actualiser.

- Onglet Extensions  
Dans cet onglet, vous pouvez activer les extensions de l'interface utilisateur Web Intelligence que vous avez créées et déployées dans votre installation.

### 18.4.1.1.2 Section Dossiers de personnalisation

La section *Dossiers de personnalisation* contient un dossier nommé Dossiers par défaut, utilisé pour définir la personnalisation par défaut. Vous pouvez choisir les dossiers pour lesquels appliquer la personnalisation en cliquant sur le bouton *Ajouter un dossier*. Pour éviter de redéfinir la même personnalisation pour les autres dossiers, vous pouvez copier la personnalisation à partir d'un dossier dans un autre à l'aide des options *Copier la personnalisation* et *Coller la personnalisation* figurant dans la liste déroulante. Pour supprimer la personnalisation d'un dossier donné, vous devez supprimer le dossier ajouté en sélectionnant l'option *Supprimer le dossier* figurant dans la liste déroulante.

#### i Remarque



Il n'est pas possible de supprimer Dossiers par défaut de la section *Dossiers de personnalisation*.

### 18.4.1.1.3 Onglet Eléments de l'interface utilisateur

Certains des éléments d'interface que vous pouvez personnaliser sont identifiés dans les diagrammes des sous-sections suivantes. Utilisez le tableau suivant pour identifier les éléments dans les diagrammes.

Table 87 :

Eléments de l'interface utilisateur	Sous-élément	Description	Numéro dans le diagramme
Ecran de présentation		Ecran s'affichant lorsqu'un utilisateur ouvre Web Intelligence.	
Menu contextuel d'application		Menu s'affichant lorsqu'un utilisateur clique avec le bouton droit de la souris sur l'écran Web Intelligence.	1
	Mode Application	Option de changement du mode d'application dans le menu contextuel de l'application.	1a
	Barre de filtre	Option de barre de filtre dans le menu contextuel de l'application.	1b
	Plan	Option de plan dans le menu contextuel de l'application.	1c
	Barre de formule	Option de barre de formule dans le menu contextuel de l'application.	1d
	Panneau latéral	Option de panneau latéral dans le menu contextuel de l'application.	1e
	Onglets du rapport	Option d'onglets du rapport dans le menu contextuel de l'application.	1f
	Barre d'état	Option de barre d'état dans le menu contextuel de l'application.	1g
Panneau latéral		Panneau latéral en regard de l'éditeur de rapport permettant aux utilisateurs d'accéder à différents onglets d'informations.	2

Éléments de l'interface utilisateur	Sous-élément	Description	Numéro dans le diagramme
	Résumé du document	Onglet de résumé du document dans le panneau latéral.	2a
	Carte de navigation	Onglet de carte de navigation (nommée carte de rapport dans l'interface HTML) dans le panneau latéral.	2b
	Contrôles de saisie	Onglet de contrôles de saisie dans le panneau latéral.	2c
	Saisie d'invite utilisateur	Onglet de saisie d'invite utilisateur dans le panneau latéral.	2d
	Objets disponibles	Onglet d'objets disponibles dans le panneau latéral.	2e
	Filtres et structure du document	Onglet de filtres et structure du document dans le panneau latéral.	2f
	Editeur de service Web	Onglet d'éditeur de service Web dans le panneau latéral.	2g
	Données	Onglet de données dans le panneau latéral.	2h
Barre d'état		Barre d'état où l'utilisateur visualise des informations sur les états des actions du document et peut réaliser des tâches de zoom, de navigation dans les pages et d'activation de la barre de formule.	3
	SAP Marketplace	Bouton SAP Marketplace (  ) dans la barre d'état.	Non affiché
	Liste déroulante Rapports	Liste déroulante de rapports dans la barre d'état.	3a
	Icône du statut de l'impression	Liste d'icônes du statut de l'impression dans la barre d'état.	3b
	Suivi des modifications de données	Etat de suivi des modifications de données dans la barre d'état.	3c
	Navigation dans les pages	Barre de navigation dans les pages dans la barre d'état.	3d
	Mode Pagination	Boutons de mode de pagination dans la barre d'état.	3e
	Liste Zoom	Liste déroulante de pourcentages de zoom dans la barre d'état.	3f
	Curseur de zoom	Barre de curseur de zoom dans la barre d'état.	3g
	Statut de l'espace de travail	Indicateur de statut de l'espace de travail dans la barre d'état.  <b>i Remarque</b>  L'indicateur du statut de l'espace de travail (  ) s'affiche entre le Curseur de zoom et la Date de la dernière actualisation si un problème se produit dans l'espace de travail.	Non affiché
	Date de la dernière actualisation	Date d'actualisation du document dans la barre d'état.	3i
	Statut de la connexion	Statut de la connexion de Web Intelligence Rich Client dans la barre d'état.	3j

Éléments de l'interface utilisateur	Sous-élément	Description	Numéro dans le diagramme
Zone du rapport		Zone de rapport dans Web Intelligence.	4
	Onglets du rapport	Onglets du rapport dans la zone de rapport.	4a
	Défilement de page bidirectionnel	Fonction de défilement bi-directionnel de la page dans le coin inférieur de la page de zone de rapport.	4b
	Barre de formule	Barre de formule dans la partie supérieure de la zone de rapport.	4c
Barre d'outils du mode Lecture		Barres d'outils affichées en mode Lecture.	5
	Liste déroulante Web Intelligence	Liste déroulante Web Intelligence en mode Lecture.	5a
	Groupe de fichiers	Barre d'outils de groupe de fichiers en mode Lecture.	5b
	Groupe d'actions standard	Barre d'outils de groupe d'actions standard en mode Lecture.	5c
	Groupe d'analyses	La barre d'outils Groupe d'analyses en mode Lecture.	5d
Barre d'outils du mode Conception		Barres d'outils et onglets affichés en mode Conception.	6
	Onglet Fichier	Onglet de fichier en mode Lecture.	6a
	Onglet Propriétés	Onglet de propriétés en mode Lecture.	6b
	Groupe d'actions standard	Barre d'outils de groupe d'actions standard en mode Lecture.	6c
	Onglet Eléments du rapport	Onglet d'éléments du rapport en mode Lecture.	6d
	Onglet Format	Onglet de format en mode Lecture.	6e
	Onglet Accès aux données	Onglet d'accès aux données en mode Lecture.	6f
	Onglet Analyse	Onglet d'analyse en mode Lecture.	6g
	Onglet Mise en page	Onglet de mise en page en mode Lecture.	6h
Barre d'outils initiale		Barres d'outils s'affichant initialement lorsqu'un utilisateur ouvre l'application Web Intelligence.	7
	Liste déroulante Web Intelligence	Liste déroulante Web Intelligence dans la barre d'outils initiale.	7a
	Groupe de fichiers	Barre d'outils de groupe de fichiers dans la barre d'outils initiale.	7b
Barre d'outils de contrôle d'application		Barre d'outils de contrôle d'application s'affichant dans la barre d'outils supérieure de Web Intelligence.	8
	Boutons du mode Application	Boutons du mode d'application (Lecture, Conception et Données) dans la barre d'outils supérieure de Web Intelligence.	8a
	Outils	Icône d'outils dans la barre d'outils supérieure de Web Intelligence.	8b

Éléments de l'interface utilisateur	Sous-élément	Description	Numéro dans le diagramme
	Aide	Icône d'aide dans la barre d'outils supérieure de Web Intelligence.	8c
	Fermer	Icône de fermeture dans la barre d'outils supérieure de Web Intelligence.	8d
Raccourcis		Raccourcis clavier tels que <b>Ctrl</b> + <b>N</b> ou <b>Ctrl</b> + <b>S</b> .	Non affiché

## Ecran de présentation

Dans la personnalisation des utilisateurs et groupes de la CMC, vous pouvez choisir de masquer l'écran de présentation de Web Intelligence qui s'affiche. L'image suivante montre l'écran de présentation qui s'affiche par défaut à l'ouverture de Web Intelligence.



Figure 13 : Ecran de présentation (exemple en anglais)

## Menu contextuel d'application

Les diagrammes suivants montrent les éléments qui peuvent être masqués dans le menu contextuel par clic droit.



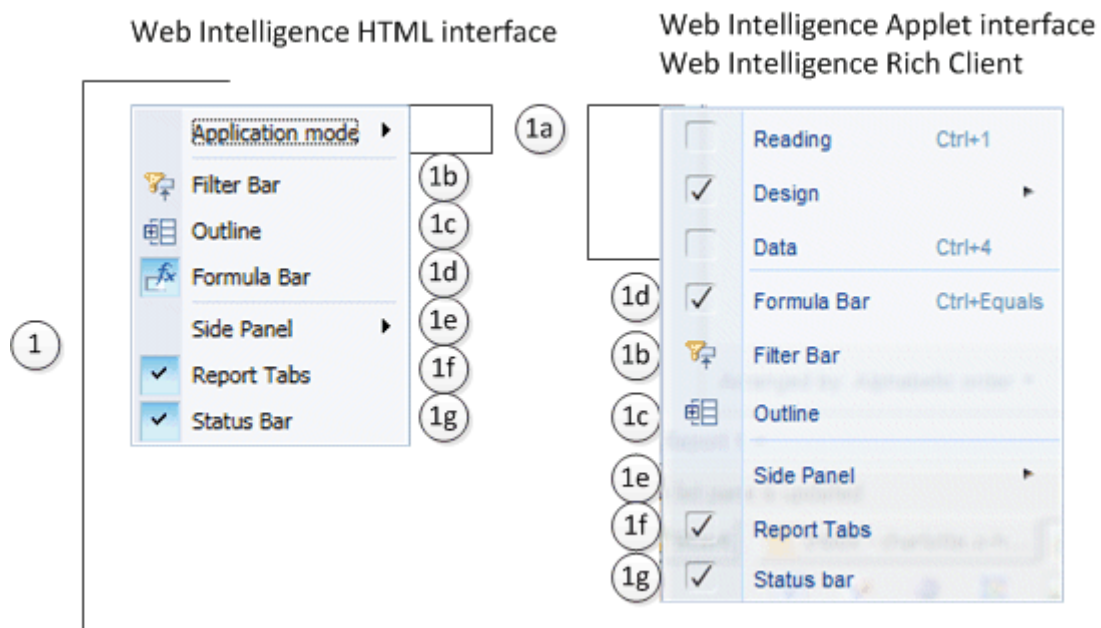
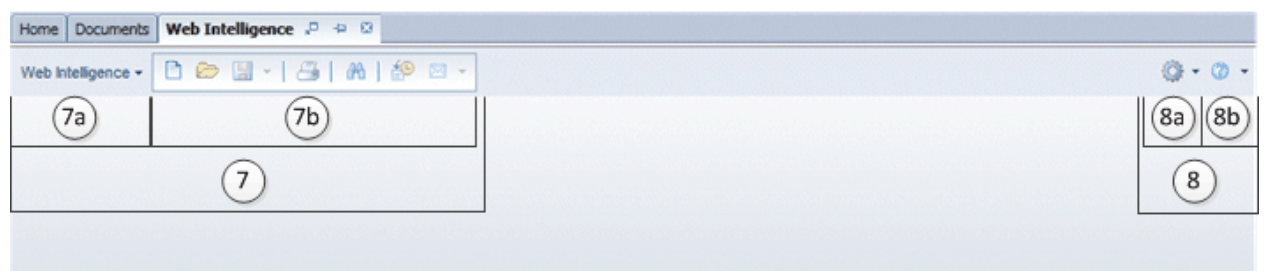


Figure 14 : Menu contextuel d'application (exemple en anglais)

## Barre d'outils initiale

Les diagrammes suivants montrent les éléments qui peuvent être masqués dans les barres d'outils qui s'affichent dans Web Intelligence quand aucun document n'est ouvert.

### Web Intelligence Applet interface Web Intelligence Rich Client



### Web Intelligence HTML interface

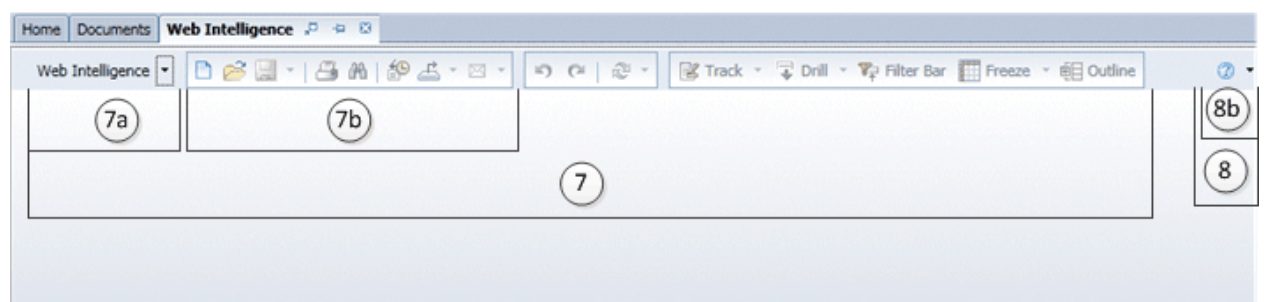
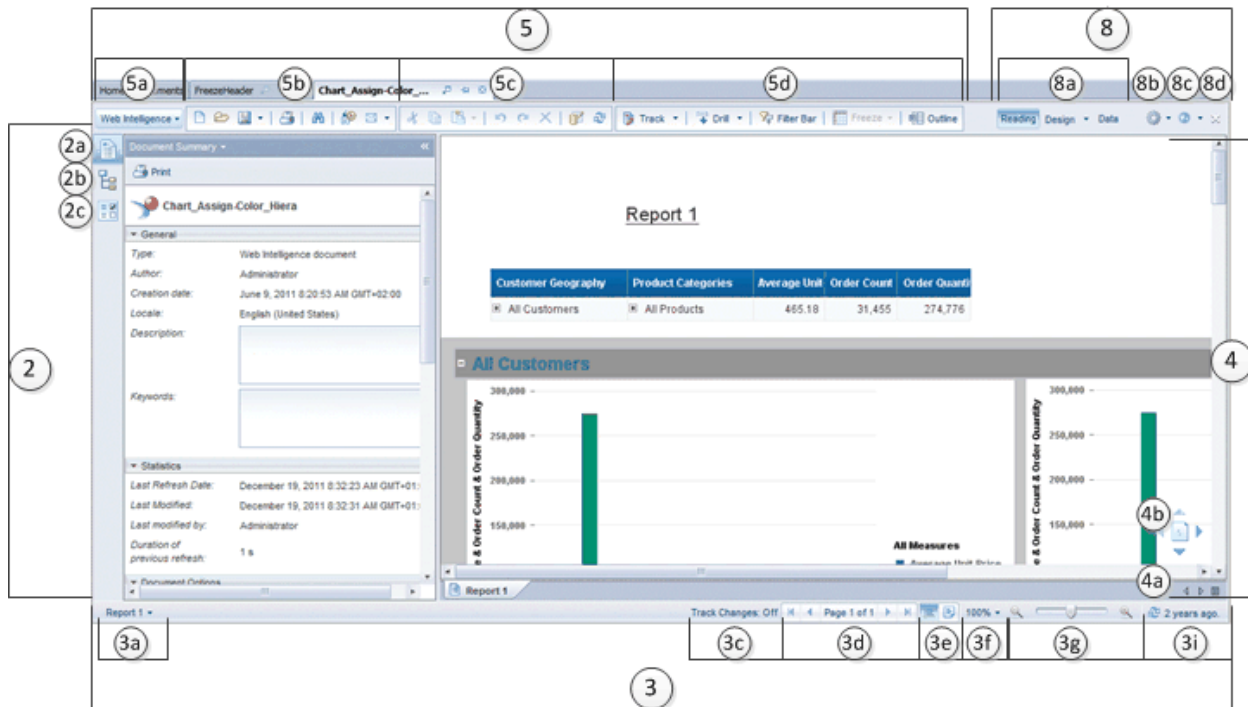


Figure 15 : Barre d'outils initiale (exemple en anglais)

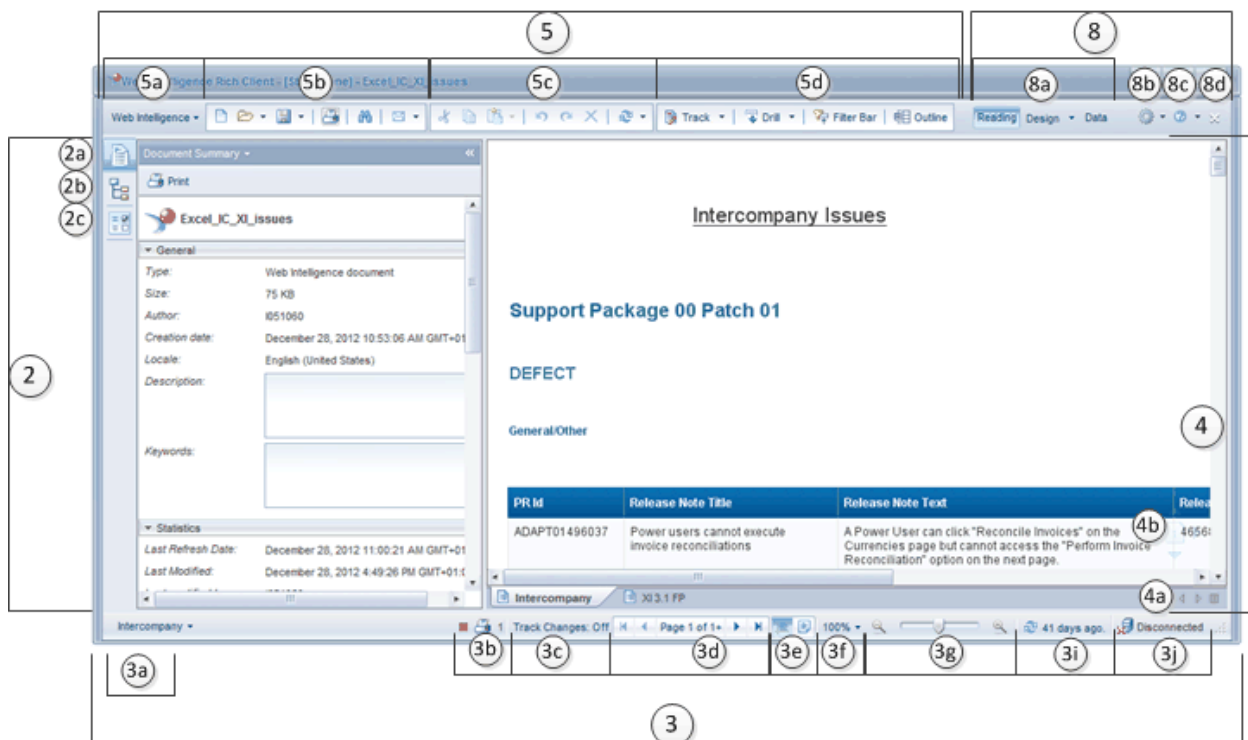
## Mode Lecture

Les diagrammes suivants montrent les éléments qui peuvent être masqués en mode Lecture de Web Intelligence.

### Web Intelligence Applet interface



### Web Intelligence Rich Client



## Web Intelligence HTML interface

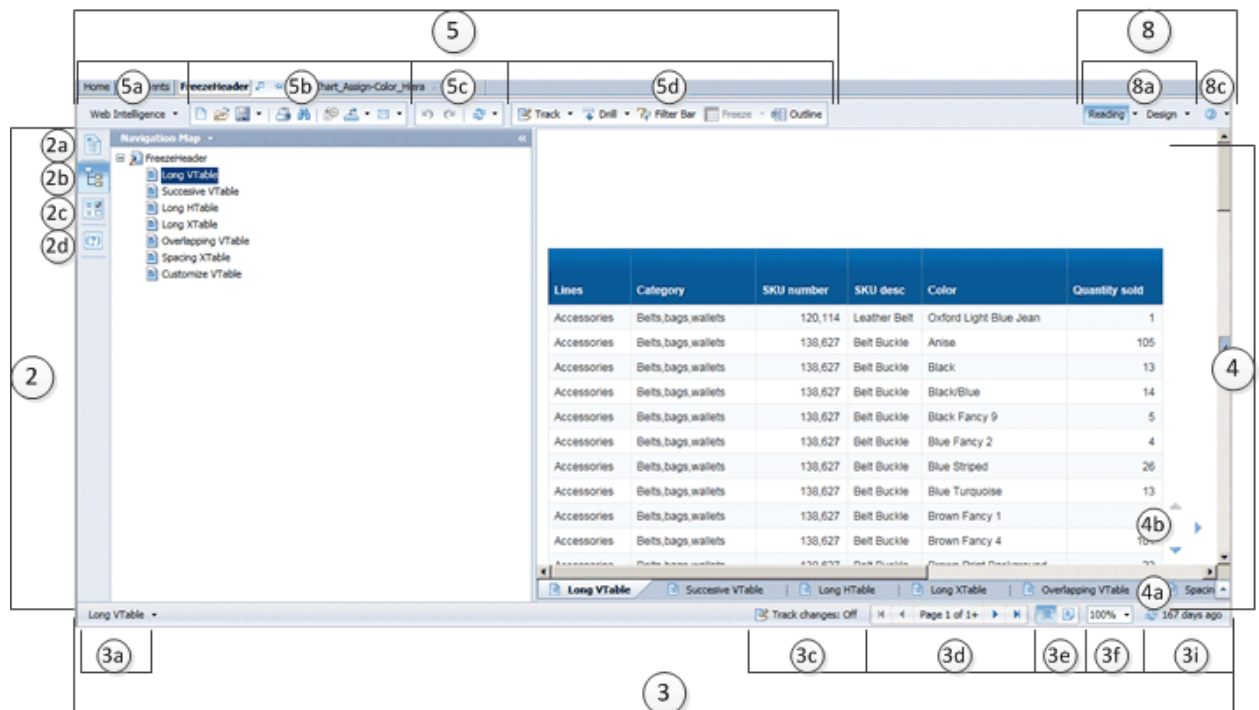
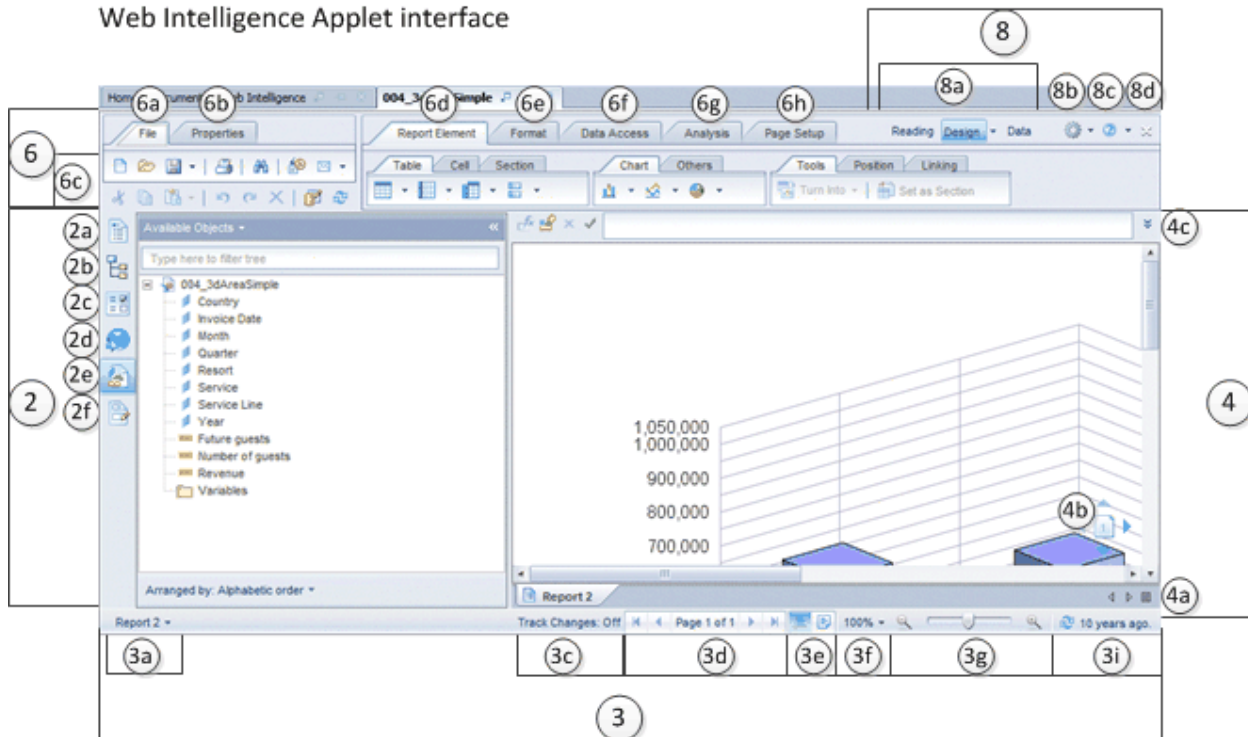


Figure 16 : Mode Lecture (exemple en anglais)

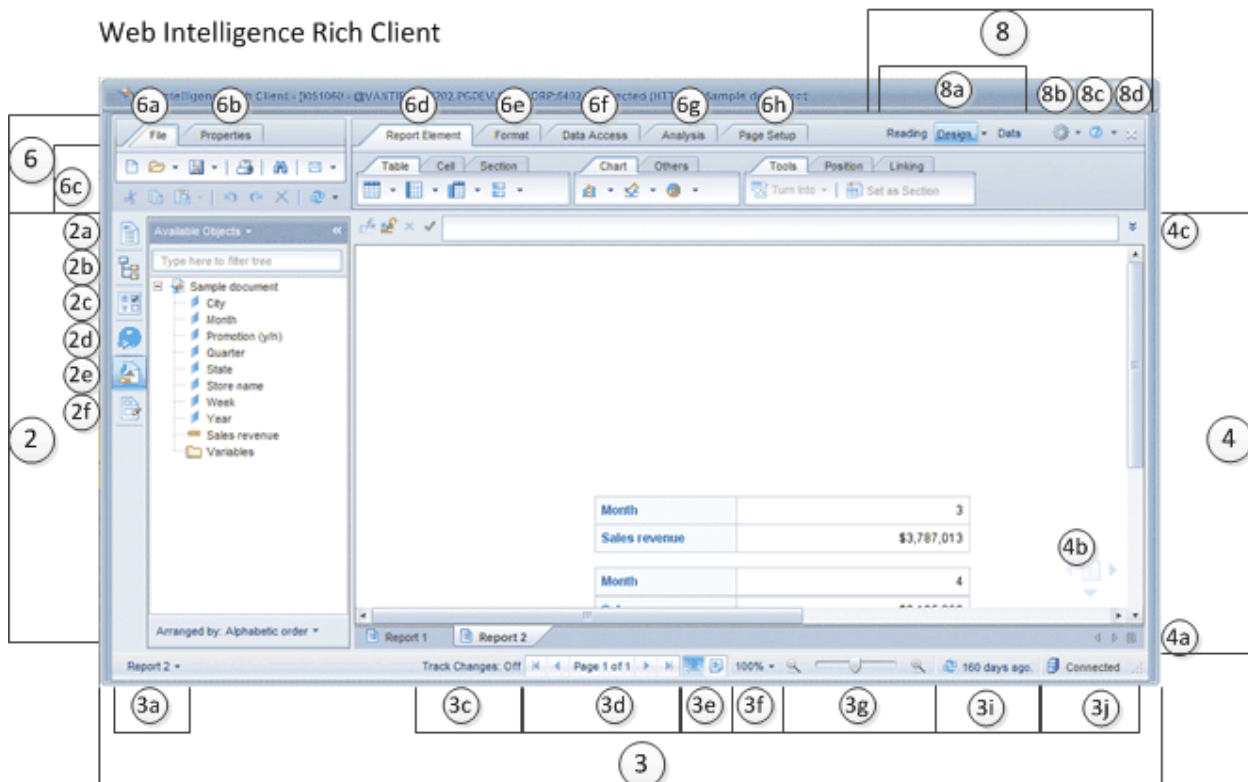
## Mode Conception

Les diagrammes suivants montrent les éléments qui peuvent être masqués en mode Conception de Web Intelligence.

## Web Intelligence Applet interface



## Web Intelligence Rich Client



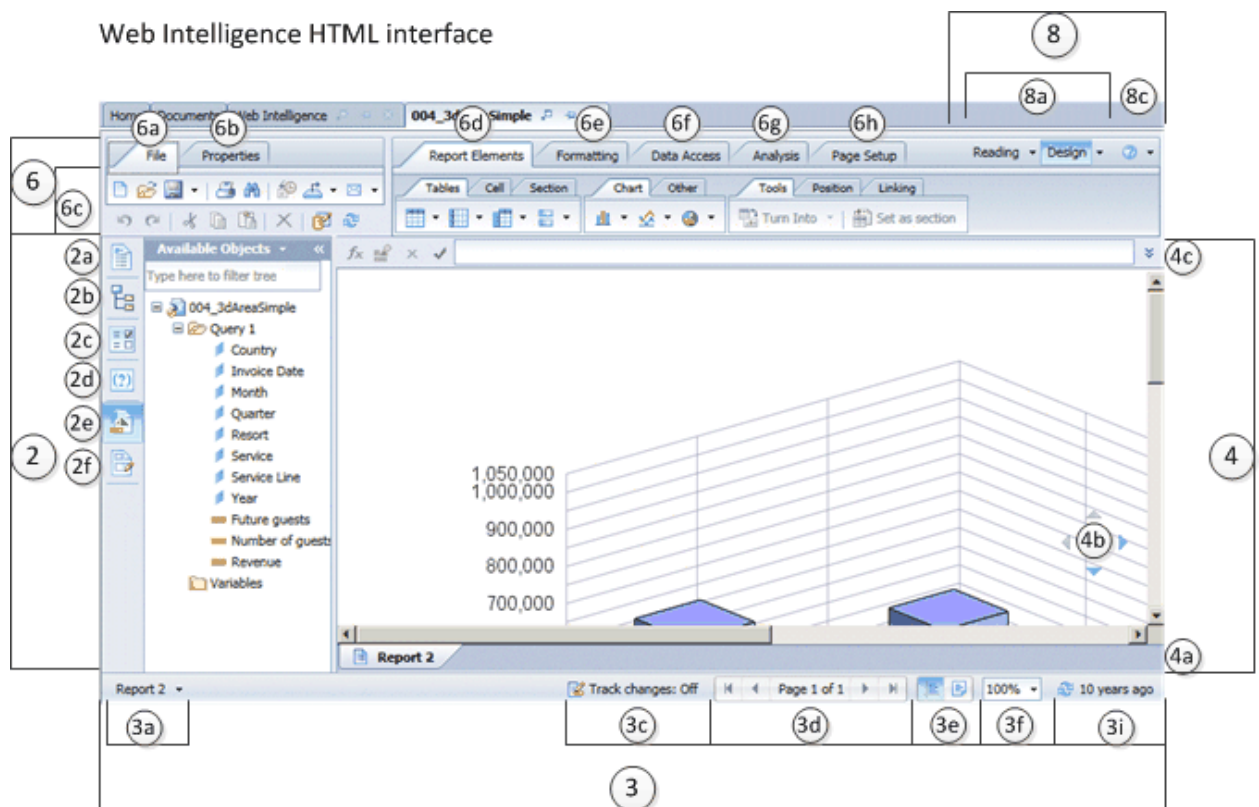


Figure 17 : Mode Conception (exemple en anglais)

## Mode Données

Les diagrammes suivants montrent les éléments qui peuvent être masqués en mode Données de Web Intelligence.



## Web Intelligence Applet interface

The screenshot shows the Web Intelligence Applet interface. The top menu bar includes Home, Documents, Web Intelligence, and a specific document '004\_3dAreaSimple'. The 'Data' menu is open, showing options like 'New data provider', 'Edit', 'Purge', 'New Variable', and 'Merge'. The 'Data' pane on the left shows a tree structure for '004\_3dAreaSimple' with a 'Query 1' folder containing various fields like Country, Invoice Date, Month, Quarter, Resort, Service, Service Line, Year, Future guests, Number of guests, Revenue, and Variables. The main pane displays 'All data providers of '004\_3dAreaSimple'' with a table showing one provider: 'Query 1' from 'Beach oracle(Bea...)' with a refresh date of 'May 29, 2003' and a status of '1'. The bottom status bar shows 'Track Changes: Off', 'Page 1 of 1', '100%', and '10 years ago'.

Annotations: 2h, 2, 3, 8, 8a, 8b, 8c, 8d, 3i.

## Web Intelligence Rich Client

The screenshot shows the Web Intelligence Rich Client interface. The top menu bar includes File, Properties, Report Element, Format, Data Access, Analysis, Page Setup, Reading, Design, and Data. The 'Data' menu is open, showing options like 'New data provider', 'Edit', 'Purge', 'New Variable', and 'Merge'. The 'Data' pane on the left shows a tree structure for 'Sample document' with a 'Query 1' folder containing various fields like City, Month, Promotion (y/n), Quarter, State, Store name, Week, Year, and Sales revenue. The main pane displays 'All data providers of 'Sample document'' with a table showing one provider: 'Query 1' from 'efashion' with a refresh date of 'Aug 13, 2012' and a status of '3' and '1992 rows'. The bottom status bar shows 'Track Changes: Off', 'Page 1 of 1', '100%', '160 days ago', and 'Connected'.

Annotations: 2h, 2, 3, 8, 8a, 8b, 8c, 8d, 3i, 3j.

Figure 18 : Mode Données (exemple en anglais)

## 18.4.1.1.4 Onglet Fonctionnalités

Dans l'onglet Fonctionnalités, vous pouvez désactiver plusieurs fonctions à la fois, sans avoir à les désactiver l'une après l'autre.

Table 88 :

Élément de fonctionnalité	Description	Concerne les éléments d'interface suivants
Actualisation	Les utilisateurs peuvent actualiser les documents pour mettre à jour les données des sources de données.	Le bouton Actualiser de la barre d'outils Groupe d'actions standard utilisé en mode Lecture et Conception.
Exploration	Les utilisateurs peuvent explorer en avant et en arrière les données d'un document.	Le bouton Explorer disponible aux emplacements suivants : <ul style="list-style-type: none"><li>• La barre d'outils Groupe d'analyses en mode Lecture.</li><li>• Le sous-onglet Interagir de l'onglet Analyse en mode Conception.</li></ul>
Mode Lecture	Les utilisateurs peuvent afficher un document en mode Lecture.	Le bouton Lecture disponible aux emplacements suivants : <ul style="list-style-type: none"><li>• Menu contextuel de l'application</li><li>• Barre d'outils Contrôle de l'application</li></ul>
Mode Conception	Les utilisateurs peuvent afficher un document en mode Conception.	Le bouton Conception disponible aux emplacements suivants : <ul style="list-style-type: none"><li>• Menu contextuel de l'application</li><li>• Barre d'outils Contrôle de l'application</li></ul>
Mode Données	Les utilisateurs peuvent afficher un document en mode Données.	Le bouton Données disponible aux emplacements suivants : <ul style="list-style-type: none"><li>• Menu contextuel de l'application</li><li>• Barre d'outils Contrôle de l'application</li></ul>

## 18.4.1.1.5 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.

## 18.4.1.1.6 Personnalisation de 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 des dossiers Personnalisation, cliquez sur [Ajouter un dossier](#) pour ajouter le dossier contenant les documents Web Intelligence pour lesquels vous souhaitez appliquer la personnalisation aux groupes d'utilisateurs sélectionnés.
6. Effectuez l'une des actions suivantes :
  - Pour masquer des éléments dans Web Intelligence, désélectionnez-les dans l'onglet [Eléments de l'interface utilisateur](#) ou [Fonctionnalités](#).
  - Pour afficher des éléments masqués dans Web Intelligence, sélectionnez-les dans l'onglet [Eléments de l'interface utilisateur](#) ou [Fonctionnalités](#).
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.

## 18.4.1.2 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.

Dans la CMC, il est possible de définir l'alignement de contenu pour l'interface d'applet Web Intelligence. Sélectionnez l'une des options suivantes :

- *De droite à gauche uniquement lorsque les paramètres régionaux du produit et d'affichage préférés sont définis sur des langues dont le sens de lecture est de droite à gauche* (option par défaut)
- *De droite à gauche ou de gauche à droite selon les paramètres régionaux d'affichage préférés de l'utilisateur*
- *Toujours de droite à gauche*
- *Toujours de gauche à droite*

### Remarque

Le paramètre d'alignement de contenu s'applique à tous les utilisateurs.



En ce qui concerne l'interface Web Intelligence 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.

#### **i** Remarque

Pour en savoir plus sur la définition des paramètres régionaux, voir le *Guide de l'utilisateur de la zone de lancement BI*.

#### **i** Remarque

L'alignement de contenu s'applique uniquement à la création de documents et n'affecte pas les documents existants.

### **18.4.1.2.1 Pour définir l'alignement de contenu pour l'interface d'applet Web Intelligence**

Définir l'alignement de contenu pour l'interface d'applet Web Intelligence.

1. Connectez-vous à la CMC en tant qu'administrateur.
2. Dans la liste *Gérer*, sélectionnez *Applications*.
3. Cliquez sur *Web Intelligence*.
4. Cliquez sur ► *Gérer* ► *Propriétés* ►.
5. Faites défiler l'écran vers le bas jusqu'à la section *Alignement du contenu pour les nouveaux documents* et sélectionnez l'option appropriée.

### **18.4.1.3 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.

### 18.4.1.3.1 Pour activer les points d'extension de l'interface utilisateur Web Intelligence

Pour utiliser la fonctionnalité Extensions, vous devez avoir créé et déployé les groupes d'extensions appropriés dans votre installation. Déployez un groupe d'extension pour chaque fonctionnalité d'extension (par exemple, bouton Personnalisé ou Enregistrer au format HTML).

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 des dossiers Personnalisation, cliquez sur [Ajouter un dossier](#) pour ajouter le dossier contenant les documents Web Intelligence pour lesquels vous souhaitez activer les points d'extension pour groupes d'utilisateurs sélectionnés.
6. Cliquez sur l'onglet [Extensions](#) et sélectionnez les extensions personnalisées à utiliser par les utilisateurs.
7. 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 accessibles à tous les clients d'application Web Intelligence : Web, applet Java et Rich Client.

## 18.4.2 Zone de lancement BI

### 18.4.2.1 Activation du bouton Effacer pour les 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 barre 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.

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.

# 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 :

- L'outil de conception d'univers. Les connexions sont stockées dans le référentiel.
- L'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 \[page 134\]](#)

[Droits de connexion \[page 932\]](#)

### 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 \[page 134\]](#)

[Outil de conception d'univers \[page 942\]](#)

[Droits d'univers \(.unv\) \[page 928\]](#)

[Outil de conception d'information \[page 943\]](#)

[Droits d'univers \(.unx\) \[page 929\]](#)

### 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 Surveillance

### 20.1 A propos de la 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 lorsque ces seuils sont franchis. Cela contribue à réaliser des actions proactives en cas de panne ou arrêt imminent.
- 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 en fonction des groupes de serveurs, des catégories de service et des nœuds Enterprise au format graphique ou tabulaire.
- 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.

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 \[page 986\]](#)

---

## 20.2 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.

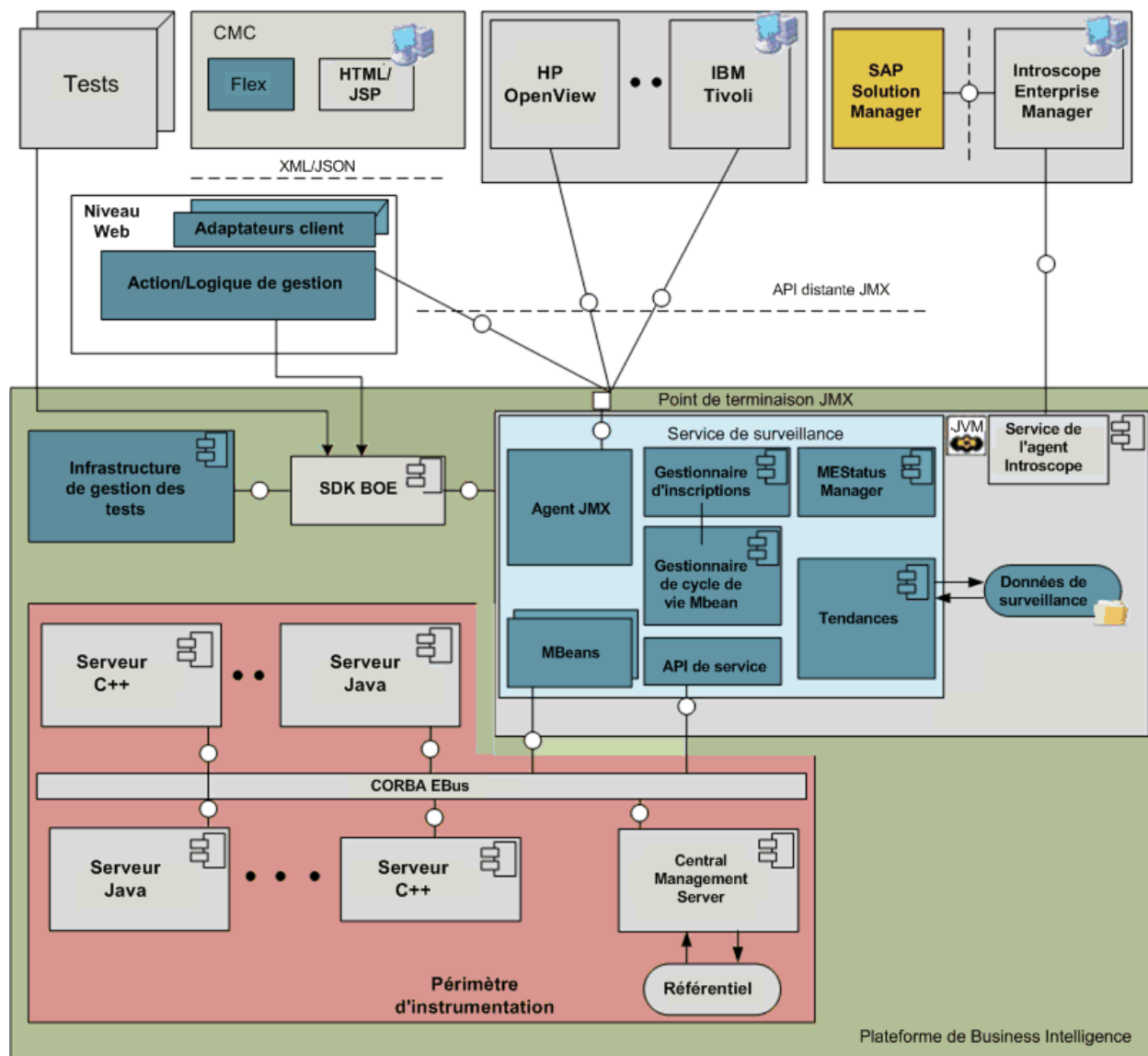
## Alerte

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 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 envoi 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 une base de données Derby dédiée 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 \[page 1024\]](#).

## 20.3 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.

### **i** 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 dans la base de données Derby intégrée (option par défaut).  
L'application de surveillance comprend une base de données Apache Derby intégrée, souvent appelée « base de données des tendances », où sont stockées par défaut les informations de surveillance. Les utilisateurs peuvent établir des rapports à partir de la base de données Derby. Cependant, elle ne fournit pas d'outils de basculement ou de sauvegarde et restauration des bases de données relationnelles traditionnelles. La base de données Derby doit également être actualisée manuellement pour renvoyer les dernières informations.
- Enregistrer les informations dans la base de données d'audit (la base de données relationnelle où le CMS stocke les données d'audit).  
Au lieu d'utiliser la base de données Derby par défaut, vous pouvez opter pour le magasin de données d'audit (ADS), souvent appelé base de données d'audit. Vous pouvez utiliser la base de données d'audit incluse dans la plateforme de BI ou une autre base de données prise en charge que vous avez configurée comme base de données d'audit. 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 restauration ainsi que la disponibilité en temps réel des données.

## Informations associées

[Configuration pour l'utilisation de la base de données Derby \[page 671\]](#)

[Configuration pour utiliser la base de données d'audit \[page 671\]](#)

### 20.3.1 Configuration pour l'utilisation de la base de données Derby

L'application de surveillance stocke par défaut les données de surveillance dans la base de données Derby intégrée. Pour utiliser la base de données Derby, confirmez les paramètres suivants dans la CMC :

1. Dans la zone [Gérer](#) de la page d'accueil de la CMC, cliquez sur [Applications](#).
2. Cliquez deux fois sur [Application de surveillance](#) pour ouvrir la page Propriétés.
3. Dans la zone [Paramètres de base de données des tendances](#), vérifiez que l'option [Utiliser la base de données incorporée](#) est sélectionnée.

Pour exécuter des requêtes dans la base de données Derby afin de créer des rapports et d'effectuer des analyses des données, un univers est nécessaire. Un univers est fourni avec le déploiement de la plateforme de BI, il se trouve à cet emplacement dans la CMC : ► [Universes \(Univers\)](#) ► [Monitoring TrendData Universes \(univers de données de tendance de surveillance\)](#) ►.

### 20.3.2 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 :

- Si la base de données des tendances Derby renferme des données, vous devrez 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. L'univers inclus dans la plateforme de BI est à utiliser uniquement avec la base de données Derby intégrée.

## Informations associées

[Migration de la base de données Derby vers la base de données d'audit \[page 672\]](#)

[Configuration de fichiers SBO \[page 675\]](#)

[Ajout de noms d'alias dans le fichier SBO \[page 677\]](#)

[Basculement vers la base de données d'audit \[page 678\]](#)

[Pour créer les tables de surveillance dans le magasin de données d'audit \[page 674\]](#)

### 20.3.2.1 Migration de la base de données Derby vers la base de données d'audit

Si vous voulez utiliser la base de données d'audit pour les données de surveillance et qu'il y a des données existantes dans la base de données des tendances Derby, vous devrez faire migrer celle-ci vers la base de données d'audit.

Avant de commencer à faire migrer les données, vérifiez ces prérequis :

- La base de données d'audit fonctionne et l'audit fonctionne correctement.
- Vous disposez des autorisations suffisantes et des applications client de base de données sur la base de données cible pour créer des tables, importer les fichiers de vidage CSV, etc.

- La base de données d'audit prend en charge l'importation de fichiers CSV.

Suivez cette procédure pour effectuer la migration de la base de données :

1. [Sauvegarde de la base de données Derby \[page 673\]](#)
2. [Exportation des données en fichiers CSV \[page 673\]](#)
3. [Pour créer les tables de surveillance dans le magasin de données d'audit \[page 674\]](#)
4. [Pour restaurer le contenu dans la base de données cible \[page 674\]](#)

#### **i** Remarque

En cas de cluster, les utilisateurs doivent utiliser la même instance de la base de données Derby pour toutes les instances de surveillance. Si l'utilisateur a plusieurs instances de base de données Derby dans un cluster, il doit importer les données d'une seule instance Derby. L'importation de données de plusieurs instances Derby entraînera des incohérences de données, elle est donc déconseillée.

### 20.3.2.1.1 Sauvegarde de la base de données Derby

1. Dans la zone [Gérer](#) de la page d'accueil de la CMC, cliquez sur [Applications](#).
2. Cliquez deux fois sur [Application de surveillance](#) pour ouvrir la page Propriétés.
3. Dans la zone [Paramètres de base de données des tendances](#), entrez un emplacement de fichier où sauvegarder la base de données des tendances Derby, puis cliquez sur [Enregistrer](#).
4. En regard de l'option [Exécuter la tâche de sauvegarde de base de données](#), cliquez sur [Maintenant](#).

Un message de confirmation s'affiche après la sauvegarde de la base de données. Contrôlez également l'emplacement de fichier entré comme emplacement de la sauvegarde et vérifiez si les fichiers de sauvegarde s'y trouvent.

### 20.3.2.1.2 Exportation des données en fichiers CSV

Cette section explique comment créer les fichiers de vidage CSV nécessaires à la migration. Les fichiers CSV contiennent les valeurs séparées par des virgules du contenu de la base de données Derby intégrée.

1. Dans la zone [Gérer](#) de la page d'accueil de la CMC, cliquez sur [Applications](#).
2. Cliquez deux fois sur [Application de surveillance](#) pour ouvrir la page Propriétés.
3. Dans la zone [Paramètres de base de données des tendances](#), en regard d'[Exporter les données de la base de données incorporée sous forme de fichiers CSV](#), cliquez sur [Exporter](#).

Les quatre fichiers CSV suivants sont créés par défaut dans l'emplacement de la base de données des tendances, à savoir : <Rép\_Install\_BOE>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB :

- Mot\_Mes\_Details.csv
- Mot\_Trend\_Data.csv
- Mot\_Trend\_Details.csv
- Mot\_Mes\_Metrics.csv

### 20.3.2.1.3 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.

### 20.3.2.1.4 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.

## 20.3.2.2 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 monitoring 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\_9D4EB94F9752458BB21A940COA892C6D"> 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*.

### 20.3.2.3 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>

## 20.3.2.4 Basculement 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 deux fois sur [Application de surveillance](#) pour ouvrir la page Propriétés.
3. Dans la zone [Paramètres de base de données des tendances](#), sélectionnez [Utiliser la base de données d'audit](#).

### i 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 : `<nom_serveur>`, `<port>`, `<nom_service>`.

### i 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

## 20.4 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. Accédez à l'onglet [Applications](#) de la CMC.
2. Cliquez avec le bouton droit sur [Application de surveillance](#) et sélectionnez [Propriétés](#). La fenêtre [Propriétés de l'application de surveillance](#) apparaît. Les propriétés configurables sont décrites dans le tableau suivant :

Table 89 :

Section	Champ	Description
	<a href="#">Activer l'application de surveillance</a>	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
	<i>URL du point de terminaison de l'agent JMX par défaut (IIOP)</i>	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	<i>Activer le protocole RMI pour JMX</i>	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	<i>Activer les métriques de l'hôte</i>	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	<i>Utiliser la base de données d'audit</i>	Sélectionnez cette option pour stocker l'historique des tendances des métriques dans la base de données d'audit du CMS.  <b>i Remarque</b> L'audit du CMS doit être configuré pour que cela fonctionne.
	<i>Utiliser la base de données incorporée</i>	Sélectionnez cette option pour stocker l'historique des tendances des métriques ou veilles dans la base de données intégrée à l'application de surveillance.
	<i>Supprimer les données anciennes lorsque la base de données atteint une taille supérieure à (Mo)</i>	Les données de la base de données des tendances sont effacées lorsque la base de données dépasse la taille indiquée. Une mémoire tampon de 30 % est créée pour la base de données. Par exemple, si vous avez défini une taille de 100 Mo pour cette propriété et si la base de données a atteint une taille supérieure à 100 Mo lors de la vérification du système, les données sont effacées jusqu'à ce que la taille de la base de données soit de 70 Mo.

Section	Champ	Description
	<i>Exécuter la tâche de nettoyage de la base de données tous les jours à</i>	La tâche de nettoyage de la base de données démarre à l'heure spécifiée. La base de données est nettoyée lorsque sa taille dépasse la taille maximum spécifiée.
	<i>Fréquence de sauvegarde de la base de données des tendances</i>	Indique le nombre d'heures entre chaque sauvegarde de la base de données des tendances. Si cette valeur est définie, une sauvegarde sera exécutée au démarrage du système ou chaque fois que le serveur de traitement adaptatif est redémarré, et également selon l'intervalle spécifié.
	<i>Répertoire de sauvegarde de la base de données des tendances</i>	Par défaut, l'emplacement n'est pas spécifié. Vous pouvez spécifier un emplacement ; toutefois, fournissez un chemin d'accès absolu et non relatif. Dans le cas d'un emplacement partagé, l'autorisation doit être accordée pour accéder à l'emplacement partagé.
	<i>Exécuter la tâche de sauvegarde de base de données</i>	La tâche de sauvegarde de la base de données démarre lorsque vous cliquez sur cette option. Spécifiez l'emplacement du répertoire de sauvegarde de la base de données avant de choisir cette option.
	<i>Exporter les données de la base de données incorporée sous forme de fichiers CSV</i>	Cliquez sur le bouton <a href="#">Exporter</a> pour exporter la base de données sous forme de fichiers CSV.
	<i>Emplacement de la base de données des tendances</i>	Par défaut, l'emplacement de la base de données des tendances est <code>&lt;REPINSTALL&gt;\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\Data/TrendingDB</code> . Vous pouvez également spécifier un autre emplacement ; toutefois, fournissez un chemin d'accès absolu et non relatif. Dans le cas d'un environnement en cluster, l'emplacement peut être partagé et l'autorisation doit être accordée pour accéder à l'emplacement partagé.

Section	Champ	Description
Autres paramètres	<i>Intervalle d'actualisation de métrique (en secondes)</i>	L'intervalle minimum pouvant être spécifié est de 15 secondes. Cet intervalle régit les éléments suivants : <ul style="list-style-type: none"> <li>○ Calcul d'inscription des veilles : les règles de mise en garde et de danger sont calculées en permanence selon l'intervalle de temps spécifié.</li> <li>○ 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 Événement de l'espion est sélectionné avec l'option suivante : <i>Modifier l'état de la veille chaque fois que la règle de mise en garde ou la règle de danger donne la valeur Vrai</i>.</li> <li>○ Période de tendance : le mode Historique des graphiques est enregistré en continu selon l'intervalle de temps spécifié.</li> </ul>
	<i>Intervalle d'actualisation automatique de l'interface utilisateur de surveillance (en secondes)</i>	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.
	<i>Fréquence des rappels d'alerte (jours)</i>	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`.

## 20.4.1 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 \[page 678\]](#).

## 20.4.2 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.

## 20.4.3 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.

## 20.5 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.

### 20.5.1 Intégration de l'application de surveillance à IBM Tivoli

Pour intégrer l'application de surveillance à IBM Tivoli, vous devez créer, installer et configurer un agent de surveillance IBM Tivoli. Exécutez les étapes suivantes pour créer un agent de surveillance IBM Tivoli :

1. Installez la version 6.2.1 du logiciel IBM Tivoli Monitoring Agent builder.
2. Créez un agent. Pour en savoir plus sur la création d'un agent, voir l'IBM Tivoli Monitoring Agent user's guide (Guide de l'utilisateur de l'agent de surveillance IBM Tivoli).

3. Dans l'étape « Définition des types de données de surveillance », sélectionnez *Données d'un serveur* dans la zone *Catégories de données de surveillance* et sélectionnez *JMX* dans la zone *Sources de données*.
4. Cliquez sur *Suivant*.
5. Dans la fenêtre *JMX Information (Informations JMX)*, cliquez sur *Browse (Parcourir)* pour voir tous les MBeans JMX sur le serveur MBean.

### Remarque

Si vous exécutez le navigateur pour la première fois, vous devez ajouter une nouvelle connexion.

6. Dans la fenêtre *Java Management Extensions (JMX) Browser (Navigateur Java Management Extensions (JMX))*, cliquez sur + en regard de *Connection Name (Nom de la connexion)* pour ajouter une nouvelle connexion.
7. Dans la fenêtre *MBean Server Connection Wizard (Assistant de connexion au serveur MBean)*, sélectionnez *Standard JMX Connections (JSR-160) (Connexions standard JMX (JSR-160))*.
8. Dans la fenêtre *Connection Properties (Propriétés de la connexion)*, fournissez les informations suivantes :

Champ	Description
Connection Name (Nom de la connexion)	JSR-160-Compliant Server (Serveur compatible JSR-160)
ID utilisateur	Nom d'utilisateur utilisé pour se connecter à la plateforme de BI
Mot de passe	Mot de passe utilisé pour se connecter à la plateforme de BI
Service URL (URL de service)	Fournissez l'URL du point de terminaison JMX

9. Cliquez sur *Terminer*.
10. Dans la zone *MBean Key Properties (Propriétés clé MBean)*, sélectionnez *Domain (Domaine)* et *Type*. Tous les MBeans apparaissent dans le champ texte en dessous.
11. Sélectionnez tous les MBeans ayant Servers (Serveurs) pour domaine, un MBean à la fois de sorte que les attributs soient répertoriés. Choisissez un attribut clé s'il est possible d'avoir plusieurs MBeans du même type. Par exemple, s'il existe deux instances d'un serveur en cours d'exécution, le PID de chaque instance peut alors être un attribut clé.
12. Sélectionnez un serveur et sélectionnez les options du groupe d'attributs JMX dans la fenêtre *JMX Agent-Wide Options (Agent JMX - Options élargies)*.
13. Dans la fenêtre *Data Source Definition (Définition de la source de données)*, sélectionnez l'agent que vous avez ajouté et cliquez sur *Add to Selected (Ajouter à la sélection)*. Cela vous permet d'accéder au début du cycle de création de l'agent et vous devez répéter les étapes ci-dessus pour ajouter un autre serveur à surveiller.
14. Après avoir créé l'agent, vous devez l'installer. Pour en savoir plus sur l'installation d'un agent, voir le guide IBM Tivoli Monitoring Agent user's guide à partir de la figure n° 154 et suivantes. Cette section fournit des informations sur l'installation locale de l'agent et la création d'une solution de l'agent pouvant être installée.

### Remarque

Si vous créez un agent pour la plateforme de BI à l'aide d'Agent Builder, la plateforme de BI doit être installée sur le même système. Toutefois, si vous installez un agent déjà créé à l'aide de son fichier d'installation, vous n'avez pas besoin que la surveillance de la plateforme de BI soit installée car vous pouvez fournir les détails de tout système ayant un point de terminaison JMX lors de la configuration.

Procédez comme suit pour configurer un agent installé :



1. Ouvrez *Manage Tivoli Enterprise Monitoring Services (Gérer les services de surveillance Tivoli Enterprise)* en mode TEMS. Vous verrez l'agent installé.
2. Cliquez sur le modèle d'agent avec le bouton droit de la souris et sélectionnez *Configure using defaults (Configurer à l'aide des paramètres par défaut)*.
3. Sélectionnez un nom d'instance.

L'agent peut être configuré à l'aide de deux protocoles différents : RMI et BOEIIOP.

Pour utiliser le protocole RMI :

Cliquez sur *Suivant*. N'apportez aucun changement aux paramètres Java.

Indiquez des valeurs pour les références de connexion JMX, telles que l'ID utilisateur, le mot de passe et l'URL de service. Pour en savoir plus, voir la section *Propriétés de configuration* dans les rubriques associées.

Cliquez sur *OK*.

Pour utiliser le protocole BOEIIOP :

Copiez les fichiers `bcm.jar` et `cryptojFIPS.jar` depuis `%REF_INSTALLATION%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` dans un dossier de votre système.

Copiez les fichiers jar répertoriés dans le tableau suivant dans un autre dossier.

Parmi les paramètres Java, définissez les arguments JVM comme suit : -

`Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring` et -  
`Djmx.boeiiop.bcm.dir=< emplacement du dossier où vous avez copié les fichiers bcm.jar et cryptojFIPS.jar`.

Sélectionnez *Suivant*.

Indiquez des valeurs pour les références de connexion JMX, telles que l'ID utilisateur, le mot de passe et l'URL de service. Pour en savoir plus, voir la section *Propriétés de configuration* dans les rubriques associées.

Définissez la valeur `<Répertoires Jar>` comme emplacement du dossier où vous avez copié la liste des fichiers Jar fournis dans le tableau.

Cliquez sur *OK*.

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

Fichiers 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

4. Cliquez avec le bouton droit sur l'agent et sélectionnez *Start (Démarrer)* dans la fenêtre *Manage Tivoli Enterprise Monitoring Services (Gérer les services de surveillance Tivoli Enterprise)*.
5. Ouvrez le client de navigateur ou de bureau IBM Tivoli Enterprise Portal. Un bouton apparaît dans la fenêtre *Navigator (Navigateur)*.
6. Cliquez sur le bouton *Navigateur*.  
L'agent est ajouté au Navigator (Navigateur).

## Informations associées

[Propriétés de configuration \[page 678\]](#)

## 20.5.2 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 Introscope Enterprise Manager », fournissez le nom de l'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\Wiley` lors de l'installation de la plateforme de BI.
2. Lancez la station de travail 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 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

communiqué 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.

## 20.6 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.

## 20.7 Dépannage

Cette section fournit des solutions détaillées à un vaste éventail de problèmes pouvant survenir dans votre travail avec l'application de surveillance.

### 20.7.1 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.

## Impossible de démarrer l'application de surveillance

Téléchargez et installez le dernier lecteur Flash.

## 20.7.2 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'Adaptive Job Server est activée.
- Contrôlez les paramètres SMTP dans l'instance de l'Adaptive Job Server de destination.

---

## 20.7.3 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'[Emplacement de la base de données des tendances](#) est spécifié dans la page [Applications](#) de la CMC. Pour un environnement en cluster, assurez-vous que l'utilisateur dispose de l'autorisation d'accéder à l'emplacement partagé. Pour en savoir plus, voir la section *Propriétés de configuration* dans les rubriques associées.
- 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.

### Informations associées

[Propriétés de configuration \[page 678\]](#)

## 20.7.4 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.

## 20.7.5 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. `saposc -s` pour consulter le statut.
  2. `saposc -m` pour obtenir un aperçu des données recueillies par SAPOSCOL.

## 20.7.6 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.

### Les données de graphique ne s'affichent pas en mode historique pour un scénario de cluster.

Assurez-vous que toutes les instances AdaptiveProcessingServer pointent vers le même emplacement de base de données Derby.

# 21 Audit

## 21.1 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 Community Network <http://scn.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. A 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.

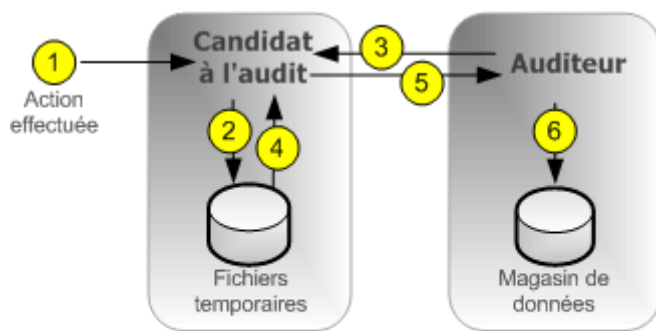
Le CMS contrôle également la synchronisation des événements d'audit se produisant sur différents ordinateurs. Chaque candidat à l'audit fournit un horodatage pour les événements d'audit qu'il consigne. Pour garantir la cohérence des horodatages des événements sur différents serveurs, le CMS diffuse périodiquement 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.



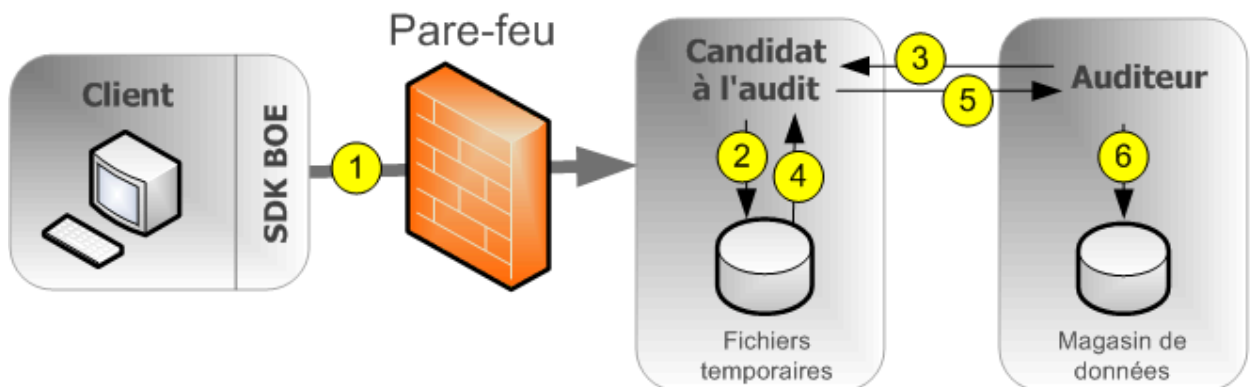


REMARQUE : le candidat à l'audit et l'auditeur peuvent également coexister sur le même serveur CMS.

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. A 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.



REMARQUE : le candidat à l'audit et l'auditeur peuvent également coexister sur le même serveur CMS.

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.

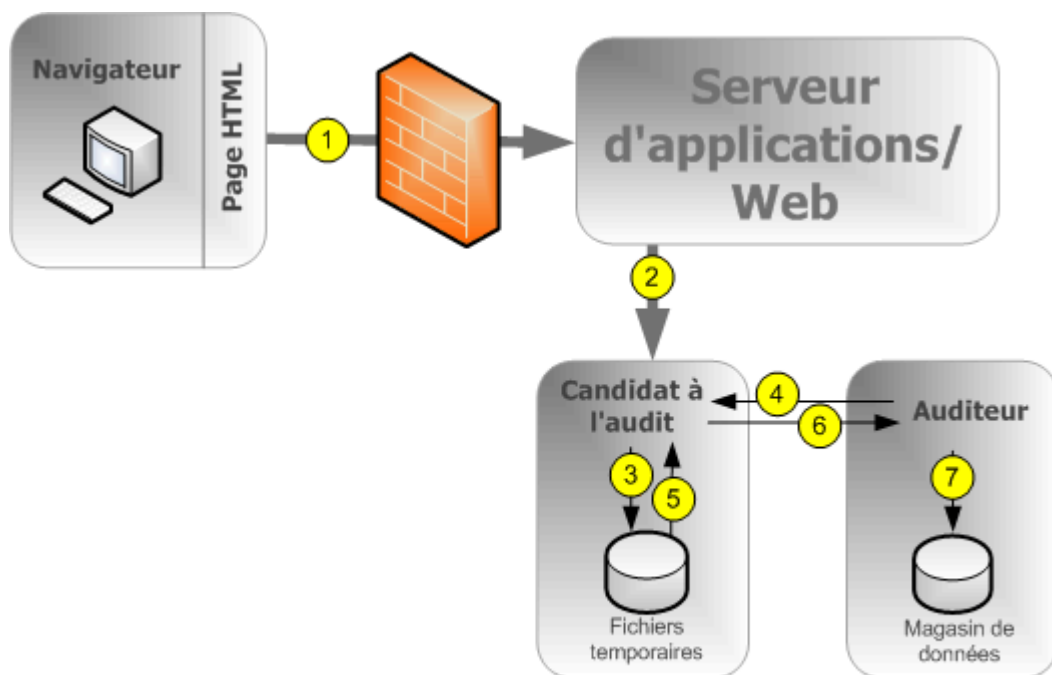
### i Remarque

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. A 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.

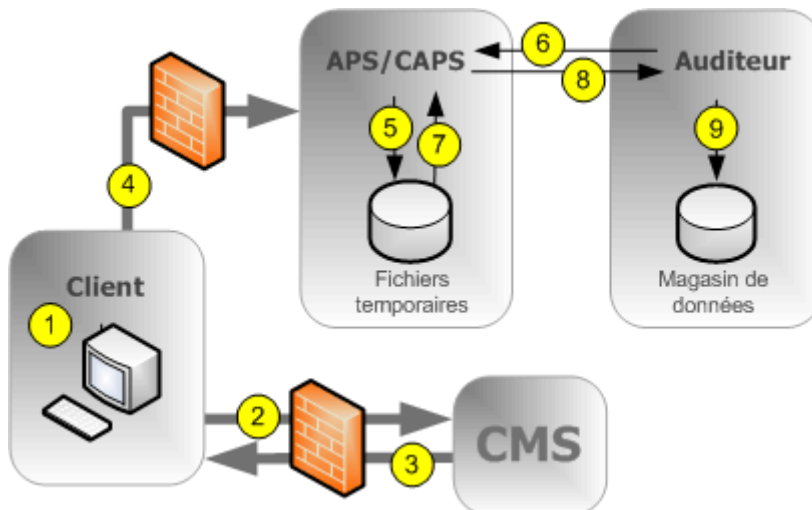


**REMARQUE** : le candidat à l'audit et l'auditeur peuvent également coexister sur le même serveur CMS.

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. A 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.

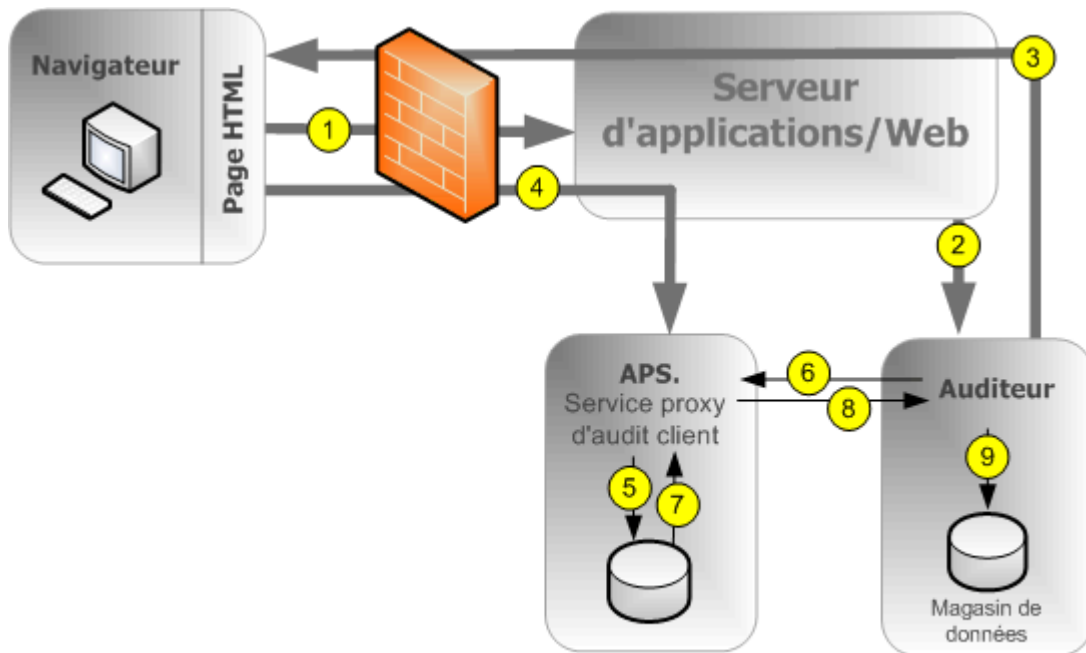
### **i** Remarque

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. A 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.

### i 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. A 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 :

- Central Management Console (CMC)
- Zone de lancement BI
- Open Document
- Analyse
- Fournisseur de services Web Live Office
- Web Intelligence Rich Client
- Dashboards et Presentation Design
- Applications d'analyse
- SAP BusinessObjects Design Studio, version 1.3 et versions supérieures

### **i** 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.

### **i** 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.

### **i** 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.

### **i** 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 \[page 1006\]](#)

## 21.2 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*

### 21.2.1 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.

### **i** 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	<p>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.</p> <p>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.</p> <p>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.</p>
Durée du dernier cycle d'interrogation	<p>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.</p> <ul style="list-style-type: none"><li>• Si ce délai est inférieur à 20 minutes (1 200 secondes), le chiffre apparaît sur fond vert.</li></ul>

Métrique	Détails
	<ul style="list-style-type: none"> <li>• Si ce délai se situe entre 20 minutes et 2 heures (7 200 secondes), le chiffre apparaît sur fond jaune.</li> <li>• Si ce délai est supérieur à 2 heures, le chiffre apparaît sur fond rouge.</li> </ul> <p>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.</p>
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.

## 21.2.2 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

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*.



## 21.2.2.1 Configuration des événements d'audit

1. Dans la Central Management Console, sélectionnez l'onglet [Audit](#).  
La page [Audit](#) apparaît.

2. Placez le curseur [Définir les événements](#) sur le niveau souhaité.

Le tableau suivant présente les paramètres possibles pour le curseur et les événements capturés à chaque niveau.

Niveau d'audit	Événements capturés
<a href="#">Désactivé</a>	Aucun
<a href="#">Minimal</a>	<ul style="list-style-type: none"><li>○ Connexion</li><li>○ Déconnexion</li><li>○ Modification des droits</li><li>○ Niveau d'accès personnalisé modifié</li><li>○ Modification de l'audit</li></ul>
<a href="#">Par défaut</a>	Événements de niveau <a href="#">Minimal</a> , plus : <ul style="list-style-type: none"><li>○ Affichage</li><li>○ Actualisation</li><li>○ Invite</li><li>○ Créer</li><li>○ Supprimer</li><li>○ Modifier</li><li>○ Enregistrer</li><li>○ Recherche</li><li>○ Modifier</li><li>○ Exécuter</li><li>○ Livraison</li></ul>
<a href="#">Compleète</a>	Événements de niveau <a href="#">Minimal</a> et <a href="#">Par défaut</a> plus : <ul style="list-style-type: none"><li>○ Déclenchement</li><li>○ Exploration hors du périmètre</li><li>○ Page extraite</li><li>○ Configuration de la gestion des promotions</li><li>○ Reprise</li><li>○ Ajout VMS</li><li>○ Extraction VMS</li><li>○ Vérification VMS</li><li>○ Retrait VMS</li><li>○ Exportation VMS</li><li>○ Verrouillage VMS</li><li>○ Déverrouillage VMS</li><li>○ Suppression de VMS</li><li>○ Connexion au cube</li><li>○ Session MDAS</li></ul>

Niveau d'audit	Événements capturés
	<p><b>i Remarque</b></p> <p>Si des modules complémentaires sont installés, il peut y avoir davantage d'événements.</p>
<i>Personnalisé</i>	Vous sélectionnez un ensemble d'événements personnalisé.

- Si vous avez sélectionné *Personnalisé*, cliquez sur les événements que vous souhaitez capturer dans la liste figurant sous le curseur *Définir les événements*.
- Sous *Définir les détails des événements*, cliquez sur les détails facultatifs que vous souhaitez enregistrer avec les événements. En limitant les détails enregistrés, vous augmenterez les performances du système.

Détail	Description
<i>Requête</i>	Si cette option est activée, les détails concernant les événements relatifs à la <i>Requête</i> (ID de détail 25) sont enregistrés pour tout événement envoyant une requête auprès d'une base de données.
<i>Détails du chemin d'accès au dossier</i>	Si cette option est activée, les détails suivants sont capturés : <ul style="list-style-type: none"> <li><i>Chemin du dossier d'objet</i> (ID de détail 71)</li> <li><i>Nom du dossier supérieur</i> (ID de détail 72)</li> <li><i>Chemin du dossier du conteneur</i> (ID de détail 64)</li> </ul>
<i>Détails des droits</i>	Si cette option est activée, les détails suivants sont capturés : <ul style="list-style-type: none"> <li><i>Droit ajouté</i> (ID de détail 55)</li> <li><i>Droit supprimé</i> (ID de détail 56)</li> <li><i>Droit modifié</i> (ID de détail 57)</li> </ul>
<i>Détails du groupe utilisateur</i>	Si cette option est activée, les détails suivants sont capturés : <ul style="list-style-type: none"> <li><i>Nom du groupe utilisateur</i> (ID de détail 16)</li> <li><i>ID du groupe utilisateur</i> (ID de détail 16)</li> </ul>
<i>Détails de la valeur de la propriété</i>	Si cette option est activée, les détails concernant les événements relatifs à la <i>Valeur de la propriété</i> (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.

- Cliquez sur *Enregistrer*.

### **i Remarque**

Pour un audit client, un délai de jusqu'à deux minutes peut être observé après l'application des modifications avant que le système ne commence à enregistrer les données de nouveaux événements. Veuillez à tenir compte de ce délai lors de l'implémentation des modifications dans le système.

## 21.2.3 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.

### i 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.

### 21.2.3.1 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.

Table 90 :

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

Type de base de données	Nom de la connexion
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.  
Lorsque IBM DB2 est installé par la plateforme de BI en tant que base de données par défaut, laissez les champs *Nom d'utilisateur* et *Mot de passe* vides.
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.

## 21.3 Événements 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, ainsi que serveurs et clients qui génèrent le type d'événement
Modification de l'audit	Les paramètres d'audit du système sont modifiés. <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> </ul>
Créer	Un nouvel objet est ajouté au système. <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> <li>• Service de modification et de visualisation Crystal Reports</li> <li>• Desktop Intelligence</li> <li>• Service du moteur d'informations</li> <li>• Gestion du cycle de vie</li> <li>• Web Intelligence</li> <li>• Service commun Web Intelligence</li> <li>• Service principal Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>
Connexion au cube	Une opération de connexion au cube OLAP est effectuée. <ul style="list-style-type: none"> <li>• Service MDAS (Multi-Dimensional Analysis Service)</li> <li>• Applications d'analyse</li> </ul>
Niveau d'accès personnalisé modifié	Les informations concernant les privilèges sont modifiées. <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> </ul>
Supprimer	Un objet est supprimé du système. <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> <li>• Service de gestion du cycle de vie</li> </ul>
Livraison	Un objet est envoyé ou livré à vers une destination. <ul style="list-style-type: none"> <li>• Service de planification de la mise à jour de l'authentification</li> <li>• Service de gestion centralisée</li> <li>• Service de planification Crystal Reports pour Enterprise</li> <li>• Service de planification Crystal Reports</li> <li>• Desktop Intelligence</li> <li>• Service de planification de livraison vers la destination</li> <li>• Service de planification de recherche de plateforme</li> <li>• Service de planification de la métrique</li> <li>• Service de planification du programme</li> <li>• Service de planification des requêtes de sécurité</li> <li>• Service de planification d'importation d'utilisateurs et de groupes</li> <li>• Service de planification et de publication Web Intelligence</li> </ul>
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. <ul style="list-style-type: none"> <li>• Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>

Événement	Description, ainsi que serveurs et clients qui génèrent le type d'événement
	<ul style="list-style-type: none"> <li>• Services communs Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de moteur d'informations</li> </ul>
Modifier	<p>Le contenu d'un objet est modifié.</p> <ul style="list-style-type: none"> <li>• Application Espaces de travail BI</li> <li>• Desktop Intelligence</li> <li>• Service de moteur d'informations</li> <li>• Web Intelligence</li> <li>• Service commun Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>
Configuration LCM	<p>Les détails de configuration de la console de gestion du cycle de vie (LCM, Lifecycle Management) sont modifiés.</p> <ul style="list-style-type: none"> <li>• Gestion du cycle de vie</li> </ul>
Connexion	<p>Un utilisateur se connecte au système.</p> <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> </ul>
Déconnexion	<p>Un utilisateur se déconnecte du système.</p> <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> </ul>
Modifier	<p>Les propriétés de fichier d'un objet sont modifiées.</p> <ul style="list-style-type: none"> <li>• Web Intelligence</li> <li>• Gestion du cycle de vie</li> <li>• Service de gestion centralisée</li> </ul>
Session MDAS	<p>Une opération de services d'analyse multidimensionnelle est effectuée</p> <ul style="list-style-type: none"> <li>• Service MDAS (Multi-Dimensional Analysis Service)</li> </ul>
Page extraite	<p>Un client SAP BusinessObjects Web Intelligence extrait des informations supplémentaires du référentiel.</p> <ul style="list-style-type: none"> <li>• Service de traitement Web Intelligence</li> <li>• Services communs Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de moteur d'informations</li> </ul>
Invite	<p>Les informations d'une invite d'objet sont saisies.</p> <ul style="list-style-type: none"> <li>• Service de mémoire cache Crystal Reports</li> <li>• Service de planification Crystal Reports pour Enterprise</li> <li>• Service de planification Crystal Reports</li> <li>• Service de mémoire cache des tableaux de bord</li> <li>• Desktop Intelligence</li> <li>• Service de moteur d'informations</li> <li>• Live Office</li> <li>• Web Intelligence</li> </ul>

Événement	Description, ainsi que serveurs et clients qui génèrent le type d'événement
	<ul style="list-style-type: none"> <li>• Service commun Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>
Actualisation	<p>Les données d'un objet sont mises à jour à partir de la base de données à la demande de l'utilisateur.</p> <ul style="list-style-type: none"> <li>• Service de mise en cache Crystal Reports</li> <li>• Service de planification Crystal Reports pour Enterprise</li> <li>• Service de planification Crystal Reports</li> <li>• Service de mise en cache Dashboards</li> <li>• Desktop Intelligence</li> <li>• Service de moteur d'informations</li> <li>• Live Office</li> <li>• Web Intelligence</li> <li>• Service commun Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>
Extraction	<p>Un objet est extrait du référentiel.</p> <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> <li>• Desktop Intelligence</li> </ul>
Modification des droits	<p>Les informations de sécurité d'un utilisateur, d'un groupe ou d'un objet sont modifiées.</p> <ul style="list-style-type: none"> <li>• Service de gestion centralisée</li> </ul>
Reprise	<p>LifeCycle Manager est utilisé pour rétablir un objet à sa version précédente.</p> <ul style="list-style-type: none"> <li>• Gestion du cycle de vie</li> </ul>
Exécuter	<p>Un travail est exécuté.</p> <ul style="list-style-type: none"> <li>• Service de planification de mise à jour de l'authentification</li> <li>• Service de planification Crystal Reports pour Enterprise</li> <li>• Service de planification Crystal Reports</li> <li>• Desktop Intelligence</li> <li>• Service de planification de livraison vers la destination</li> <li>• Service de planification de LCM</li> <li>• Gestion du cycle de vie</li> <li>• Service de planification de recherche de plateformes</li> <li>• Service de planification de la métrique</li> <li>• Service de planification du programme</li> <li>• Service de planification de la publication</li> <li>• Service de réplication</li> <li>• Service de planification des requêtes de sécurité</li> <li>• Service de planification d'importation d'utilisateurs et de groupes</li> <li>• Service de planification de la différence visuelle</li> </ul>

Événement	Description, ainsi que serveurs et clients qui génèrent le type d'événement
	<ul style="list-style-type: none"> <li>• Service de planification et de publication Web Intelligence</li> </ul>
Enregistrer	<p>Un objet est enregistré après avoir été mis à jour ou modifié.</p> <ul style="list-style-type: none"> <li>• Analysis, édition pour OLAP</li> <li>• Service de mise en cache Crystal Reports</li> <li>• Service de planification Crystal Reports pour Enterprise</li> <li>• Service de planification Crystal Reports</li> <li>• Service de modification et de visualisation Crystal Reports</li> <li>• Tableaux de bord</li> <li>• Desktop Intelligence</li> <li>• Service de moteur d'informations</li> <li>• Gestion du cycle de vie</li> <li>• Service MDAS (Multi-Dimensional Analysis Service)</li> <li>• SAP BusinessObjects Mobile</li> <li>• Web Intelligence</li> <li>• Service commun Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>
Recherche	<p>Une recherche est effectuée.</p> <ul style="list-style-type: none"> <li>• Service de recherche</li> <li>• Explorer</li> <li>• Gestion du cycle de vie</li> </ul>
Déclenchement	<p>Un événement de fichier est déclenché.</p> <ul style="list-style-type: none"> <li>• Service d'événement</li> <li>• Service de gestion centralisée</li> </ul>
Affichage	<p>Un objet est visualisé.</p> <ul style="list-style-type: none"> <li>• Applications d'analyse</li> <li>• Analysis, édition pour OLAP</li> <li>• Zone de lancement BI</li> <li>• Application Espaces de travail BI</li> <li>• CMC</li> <li>• Service de mise en cache Crystal Reports</li> <li>• Service de modification et de visualisation Crystal Reports</li> <li>• Service de mise en cache Dashboards</li> <li>• Desktop Intelligence</li> <li>• Service de moteur d'informations</li> <li>• Open Document</li> <li>• SAP BusinessObjects Mobile</li> <li>• Web Intelligence</li> <li>• Service commun Web Intelligence</li> <li>• Services principaux Web Intelligence</li> <li>• Service de traitement Web Intelligence</li> </ul>



Événement	Description, ainsi que serveurs et clients qui génèrent le type d'événement
Ajout VMS	Un objet est ajouté au système de gestion des versions de LCM. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Vérification VMS	Un objet est vérifié dans le système de gestion des versions de LCM. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Extraction VMS	Un objet est extrait du système de gestion des versions de LCM. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Exportation VMS	Une ressource est exportée du VMS. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Verrouillage VMS	Une ressource du VMS est verrouillée. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Déverrouillage VMS	Une ressource du VMS est déverrouillée. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Extraction VMS	Un objet est extrait du système de gestion des versions de LCM. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>
Suppression de VMS	Un objet est supprimé du système de gestion des versions de LCM. <ul style="list-style-type: none"> <li>Gestion du cycle de vie</li> </ul>

## Événements par type de service

Type de service	Types d'événement générés
Applications d'analyse	<ul style="list-style-type: none"> <li>Affichage</li> <li>Connexion au cube</li> </ul>
Service de planification de mise à jour de l'authentification	<ul style="list-style-type: none"> <li>Livraison</li> <li>Exécution</li> </ul>
Zone de lancement BI	Affichage
Service de gestion centralisée	<ul style="list-style-type: none"> <li>Modification de l'audit</li> <li>Création</li> <li>Niveau d'accès personnalisé modifié</li> <li>Suppression</li> <li>Livraison</li> <li>Connexion</li> </ul>

Type de service	Types d'événement générés
	<ul style="list-style-type: none"> <li>• Déconnexion</li> <li>• Modification</li> <li>• Extraction</li> <li>• Modification des droits</li> <li>• Déclenchement</li> </ul>
Central Management Console	Affichage
Service de planification Crystal Reports	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Exécution</li> <li>• Enregistrement</li> </ul>
Service de mise en cache Crystal Reports	<ul style="list-style-type: none"> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service de planification Crystal Reports pour Enterprise	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Exécution</li> <li>• Enregistrement</li> </ul>
Service de planification Crystal Reports	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Exécution</li> <li>• Enregistrement</li> </ul>
Service de modification et de visualisation Crystal Reports	<ul style="list-style-type: none"> <li>• Création</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service de mise en cache Dashboards	<ul style="list-style-type: none"> <li>• Invite</li> <li>• Actualisation</li> <li>• Affichage</li> </ul>
Application Dashboards	<ul style="list-style-type: none"> <li>• Enregistrement</li> </ul>
Desktop Intelligence (client)	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Invite</li> <li>• Extraction</li> <li>• Exécution</li> </ul>
Processus du planificateur Desktop Intelligence	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>
Service de planification de livraison vers la destination	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>

Type de service	Types d'événement générés
Service d'événement	Déclenchement
Service de moteur d'informations	<ul style="list-style-type: none"> <li>• Création</li> <li>• Exploration hors du périmètre</li> <li>• Modification</li> <li>• Page extraite</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service de planification de LCM	Exécuter
service LCM	<ul style="list-style-type: none"> <li>• Création</li> <li>• Suppression</li> <li>• Configuration LCM</li> <li>• Modification</li> <li>• Reprise</li> <li>• Exécution</li> <li>• Enregistrement</li> <li>• Ajout VMS</li> <li>• Vérification VMS</li> <li>• Retrait VMS</li> <li>• Suppression de VMS</li> <li>• Exportation VMS</li> <li>• Verrouillage VMS</li> <li>• Extraction VMS</li> <li>• Déverrouillage VMS</li> <li>• Recherche</li> </ul>
Live Office	<ul style="list-style-type: none"> <li>• Invite</li> <li>• Actualisation</li> </ul>
Service MDAS (Multi-Dimensional Analysis Service)	<ul style="list-style-type: none"> <li>• Connexion au cube</li> <li>• Session MDAS</li> <li>• Enregistrement</li> </ul>
OpenDocument	Affichage
Service de planification de recherche de plateformes	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>
Service de recherche de plateformes	Recherche
Service de planification de la métrique	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>
Service de planification du programme	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>
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	<ul style="list-style-type: none"> <li>• Connexion</li> <li>• Déconnexion</li> </ul>
Service de planification des requêtes de sécurité	<ul style="list-style-type: none"> <li>• Exécution</li> <li>• Livraison</li> </ul>
Service de planification d'importation d'utilisateurs et de groupes	<ul style="list-style-type: none"> <li>• Exécution</li> <li>• Livraison</li> </ul>
Service de planification de la différence visuelle	Exécuter
Application Web Intelligence	<ul style="list-style-type: none"> <li>• Création</li> <li>• Exploration hors du périmètre</li> <li>• Modification</li> <li>• Modification</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service commun Web Intelligence	<ul style="list-style-type: none"> <li>• Création</li> <li>• Exploration hors du périmètre</li> <li>• Modification</li> <li>• Page extraite</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Services principaux Web Intelligence	<ul style="list-style-type: none"> <li>• Création</li> <li>• Exploration hors du périmètre</li> <li>• Modification</li> <li>• Page extraite</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service de traitement Web Intelligence	<ul style="list-style-type: none"> <li>• Création</li> <li>• Exploration hors du périmètre</li> <li>• Modification</li> <li>• Page extraite</li> <li>• Invite</li> <li>• Actualisation</li> <li>• Enregistrement</li> <li>• Affichage</li> </ul>
Service de planification et de publication Web Intelligence	<ul style="list-style-type: none"> <li>• Livraison</li> <li>• Exécution</li> </ul>

## 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 multiple. Voir la rubrique associée pour en savoir plus sur les ID multiples.

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

[Tables du magasin de données d'audit \[page 1015\]](#)

### 21.3.1 Événements et détails d'audit

La section suivante répertorie tous les types d'événement, suivis par une description des propriétés et détails d'événement propres à ces événements. Au début de la section, une liste reprend les propriétés et détails communs à tous les types d'événement.

#### **i** Remarque


Certains programmes client ne disposent pas de leurs propres événements uniques et dépendent des événements communs et de plateforme pour capturer des informations pertinentes sur leur fonctionnement.

## Propriétés et détails d'événement universel

Le tableau suivant affiche quelles propriétés et détails d'événement sont enregistrés pour tous les événements.

## Remarque

Les propriétés de ce tableau sont les colonnes de la table ADS\_EVENT dans le magasin de données d'audit.

Propriété d'événement	Description
Event_ID	Identifiant unique pour l'événement.
Client_Type_ID	Identifiant du type d'application qui a réalisé l'événement.
Service_Type_ID	Affiche l'ID du type de service ou d'application qui a déclenché l'événement.
Start_Time	Date et heure auxquelles l'événement a débuté (heure GMT).
Duration	Durée de l'événement en millisecondes.
Session_ID	ID de la session durant laquelle l'événement a été déclenché.
Event_Type_ID	Type de l'événement (par exemple, 1002 pour affichage)
Status_ID	Enregistre si l'action réussit ou échoue ("0" = réussite, "1" = échec). Certains événements ont des types de statut supplémentaires, ceux-ci sont détaillés avec les descriptions de ces événements.
Object_ID	<div>CUID de l'objet affecté (le cas échéant). CUID de l'événement d'alerte pour les événements Déclencher.</div> <div> <b>Remarque</b> Tous les objets non enregistrés dans le référentiel CMS ont un ID ou 0. Ces objets peuvent être des documents qui n'ont pas encore été enregistrés dans la base de données du CMS ou sont stockés localement sur un ordinateur client, par exemple. Vous devrez utiliser la propriété Object_Name pour différencier ces objets.</div>
User_ID	CUID de l'utilisateur qui a exécuté l'événement.
User_Name	Nom d'utilisateur de l'utilisateur qui a exécuté l'événement.
Object_Name	Nom de l'objet affecté (le cas échéant). Nom de l'événement d'alerte pour les événements Déclencher.
Object_Type_ID	CUID du type d'objet (par exemple document, dossier, etc.)
Object_Folder_Path	Chemin complet du dossier où l'objet affecté est situé dans le référentiel CMS. Par exemple, Chiffre d'affaires/Amérique du Nord/Côte Est
Folder_ID	CUID du dossier où est stocké l'objet.
Top_Folder_Name	Nom du dossier de niveau supérieur où est stocké l'objet affecté. Par exemple, si l'objet est situé dans Chiffre d'affaires/Amérique du Nord/Côte Est, la valeur sera Chiffre d'affaires.
Top_Folder_ID	CUID du dossier de niveau supérieur où est situé l'objet affecté. Par exemple, si l'objet est situé dans Chiffre

Propriété d'événement	Description
	d'affaires/Amérique du Nord/Côte Est, la valeur sera le CUID du dossier Chiffre d'affaires.
Cluster ID	CUID du cluster de CMS qui a enregistré l'événement.
Action_ID	Identifiant unique qui peut être utilisé pour lier ensemble une séquence d'événements initiés par une action d'utilisateur unique.

### Remarque

Les propriétés de ce tableau sont les colonnes de la table ADS\_EVENT\_DETAIL\_TYPE\_STR dans le magasin de données d'audit.

Détail d'événement	ID	Description
Erreur	1	Enregistré uniquement si l'action échoue ; le texte ou tout message d'erreur résultant de la tentative.
ID de l'élément	2	Nom d'un objet résidant dans un objet conteneur (document Live Office ou tableau de bord, par exemple).
Nom de l'élément	3	ID généré pour un objet résidant dans un objet de conteneur (document Live Office ou tableau de bord, par exemple).
ID de type d'élément	5	Type d'objet d'un objet de conteneur qui est visualisé ou modifié. Généré uniquement le cas échéant.
ID de document parent	12	<ul style="list-style-type: none"> <li>Pour une instance de document : le CUID du document parent.</li> <li>Pour les documents parent : leur propre CUID.</li> </ul>
ID de l'univers	13	CUID de l'univers utilisé par le document ou l'objet. Un détail d'événement sera généré pour chaque univers si plusieurs sont utilisés.
Nom de l'univers	14	Nom de l'univers utilisé par le document ou l'objet. Un détail d'événement sera généré pour chaque univers si plusieurs sont utilisés.
Nom du groupe d'utilisateurs	15	Nom du groupe d'utilisateurs auquel appartient l'utilisateur qui réalise l'action. Si l'utilisateur appartient à plusieurs groupes, un détail d'événement sera généré pour chaque groupe.
ID du groupe d'utilisateurs	16	ID du groupe d'utilisateurs auquel appartient l'utilisateur qui réalise

Détail d'événement	ID	Description
		l'action. Si l'utilisateur appartient à plusieurs groupes, un détail d'événement sera généré pour chaque groupe.

## Evénements courants

Les types d'événement suivants sont communs à tous les serveurs et clients SAP BusinessObjects.

### Afficher

L'utilisateur a visualisé un document ou un objet.

- ID de type d'événement : 1002

Détail d'événement	ID	Description
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement.
ID du conteneur	32	CUID de l'objet de conteneur (un tableau de bord, par exemple) dans lequel réside l'objet (le cas échéant).
Type de conteneur	33	Type d'application du conteneur de l'objet (le cas échéant).

### i Remarque

Si vous utilisez un service de recherche, il se peut que vous remarquiez un grand nombre d'événements Visualiser générés par l'utilisateur "Compte système" au cours de l'indexation des documents. Cela est dû à l'ouverture de documents par le service d'indexation de recherche afin de créer l'index de recherche.

### Actualiser

Un objet a été actualisé depuis la base de données.

- ID de type d'événement : 1003

Détail d'événement	ID	Description
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement. <div> <h3>i Remarque</h3> <p>Pour Visualiser à la demande des rapports Crystal Reports, la valeur sera 0.</p> </div>
Nombre de lignes	63	Nombre d'enregistrements retournés par le serveur de base de données.



Détail d'événement	ID	Description
		<p><b>i Remarque</b></p> <p>Pour Visualiser à la demande des rapports Crystal Reports, la valeur sera 0.</p>
Requête	25	Enregistre la requête SQL 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 ou l'objet. Un détail d'événement est généré pour chaque univers auquel a accédé le document ou l'objet.
Périmètre du document	36	Enregistre les informations relatives au périmètre prévu du document à partir de ses paramètres de publication (par exemple : Pays=USA, Rôle=Directeur). Applicable uniquement aux workflows de publication.
ID d'instance de publication	37	ID de cette instance de la publication. Applicable uniquement aux workflows de publication.
Type d'objet Live Office	10701	Identifie le type d'objet qui est actualisé dans un document Live Office (un rapport Crystal, par exemple). Celui-ci sera uniquement généré pour les documents Live Office.

### Invite

Une valeur a été saisie pour une invite.

- ID de type d'événement : 1004

Détail d'événement	ID	Description
Nom de l'invite	26	Nom affecté à l'invite ("Date", par exemple). Un détail séparé est généré pour chaque invite d'un document ou d'un objet et ils seront regroupés.
Valeur de l'invite	27	Valeur saisie pour une invite. Un détail séparé est généré pour chaque valeur saisie. Ils peuvent être regroupés et liés à nouveau au nom de l'invite.
Périmètre du document	36	Informations relatives au périmètre prévu du document à partir de ses paramètres de publication (par exemple : Pays=USA, Rôle=Directeur).

Détail d'événement	ID	Description
ID d'instance de publication	37	ID de cette instance de la publication. S'applique uniquement aux workflows de publication.
Nom de conception	90	Nom du document Dashboards lors de sa conception. Celui-ci est uniquement généré pour les actualisations Dashboards ou un document Dashboards ou Live Office contenant une invite.
Type d'objet Live Office	10701	Identifie le type d'objet qui est actualisé dans un document Live Office (un rapport Crystal, par exemple). Celui-ci sera uniquement généré pour les documents Live Office dont l'objet incorporé contient une invite.

### Créer

L'utilisateur a créé un objet.

- ID de type d'événement : 1005

Détail d'événement	ID	Description
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement.
Ecraser	21	Enregistre si le document ou l'objet est nouveau ou remplace un objet existant (0 = Nouveau document ou objet, 1 = Remplacement du document ou de l'objet existant).
Actualisation à l'ouverture	23	Enregistre si le document ou l'objet est défini pour être automatiquement actualisé lors de l'ouverture (0 = Pas d'actualisation, 1 = Actualisation lors de l'ouverture). Généré uniquement le cas échéant.
Description	24	Enregistre toute information du champ de description du document ou de l'objet.

### Supprimer

L'utilisateur a supprimé un objet.

- ID de type d'événement : 1006

### Modifier

L'utilisateur a modifié une propriété de fichier ou les propriétés de fichier d'un objet.

- ID de type d'événement : 1007

Détail d'événement	ID	Description
Nom de la propriété	28	Nom de la propriété modifiée. Un détail d'événement sera généré pour chaque propriété modifiée.
Valeur de la propriété	29	Nouvelle valeur pour toute propriété modifiée du document ou de l'objet. Un détail d'événement sera généré pour chaque propriété modifiée.

### Enregistrer

Enregistrement ou exportation d'un document ou objet en local, à distance ou dans le référentiel CMS, soit sous son format existant, soit sous un autre.

- ID de type d'événement : 1008
- Statuts :
  - "0" indique que l'objet a été enregistré en local avec succès
  - "1" indique que la tentative a échoué
  - "2" indique que l'objet a été enregistré ou exporté avec succès dans un référentiel
  - "3" indique que l'objet a été enregistré ou exporté avec succès sous un nouveau format

Détail d'événement	ID	Description
Taille	17	Taille de l'objet (en octets) qui a été enregistré ou exporté.
Nom du fichier	18	Nom complet sous lequel a été enregistré le document ou l'objet. Si le fichier est enregistré en local par une application client, le nom contiendra également le chemin de fichier.
Ecraser	21	Enregistre si le document ou l'objet est nouveau ou remplace un fichier existant. "0" = Nouveau document ou objet, "1" = Remplacement du document ou de l'objet existant.
Mise en forme	22	Spécifie le format du document enregistré ou exporté, affiché sous forme d'extension de fichier courante à trois lettres ("doc" pour un fichier Microsoft Word ou "pdf" pour un fichier Adobe PDF, par exemple).
Actualisation à l'ouverture	23	Enregistre si le document ou l'objet est défini pour être automatiquement actualisé lors de l'ouverture ("0" = Pas d'actualisation, "1" = Actualisation lors de l'ouverture). Enregistré uniquement le cas échéant.

### Rechercher

Une recherche a été effectuée.

- ID de type d'événement : 1009

Détail d'événement	ID	Description
Mot clé	19	Mots clés de la recherche effectuée.
Catégorie	20	Catégorie utilisée dans la recherche (le cas échéant).
Nombre de lignes	63	Nombre de lignes renvoyées par la recherche.

### Modifier

L'utilisateur a modifié le contenu d'un objet.

- ID de type d'événement : 1010

Détail d'événement	ID	Description
Taille	17	Taille de l'objet (en octets) qui est sujet à l'événement.
Requête	25	Enregistre la nouvelle requête si la modification porte sur la requête SQL. (Ce paramètre est facultatif et peut être sélectionné dans la page d'audit de la CMC.)
Nom de l'objet d'univers	31	Nom de l'univers utilisé par le document ou l'objet. Un détail séparé est généré pour chaque univers auquel a accédé le document ou l'objet.
ID du conteneur	32	CUID du conteneur (un tableau de bord, par exemple) qui utilise l'objet (le cas échéant).
Type de conteneur	34	Type d'application du conteneur de l'objet (le cas échéant).
Chemin du dossier du conteneur	64	Chemin du dossier du conteneur de l'objet (le cas échéant).

### Exécuter

Un travail a été exécuté.

- ID de type d'événement : 1011
- Statuts :
  - "0" indique que le travail a réussi
  - "1" indique que le travail a échoué
  - "2" indique que le travail a échoué mais qu'une nouvelle tentative sera effectuée
  - "3" indique que le travail a été annulé

Détail d'événement	ID	Description
Taille	17	Taille (en octets) du document qui a été exécuté.
Périmètre du document	36	Informations relatives au périmètre prévu du document à partir de ses

Détail d'événement	ID	Description
		paramètres de publication (par exemple : Pays=USA, Rôle=Directeur).

### Livrer

Un objet a été livré.

- ID de type d'événement : 1012

Détail d'événement	ID	Description
Taille	17	Taille (en octets) de l'objet qui a été livré.
Type de destination	35	La destination de l'instance du document ou de l'objet. Par exemple, courrier électronique, FTP, disque non géré, boîte de réception ou imprimante.
Périmètre du document	36	Informations relatives au périmètre prévu du document à partir de ses paramètres de publication (par exemple : Pays=USA, Rôle=Directeur)
ID d'instance de publication	37	ID de cette instance du document ou de l'objet.
Domaine	38	Enregistre le nom de domaine du serveur SMTP des documents ou objets diffusés par courrier électronique (le cas échéant).
Nom de l'hôte	39	Enregistre le nom de l'hôte SMTP ou FTP des documents ou objets diffusés par courrier électronique ou FTP (le cas échéant).
Port	40	Enregistre le port du domaine du serveur SMTP ou FTP des documents ou objets diffusés par courrier électronique ou FTP (le cas échéant).
Adresse de l'expéditeur	41	Enregistre l'adresse de l'expéditeur des documents ou objets diffusés par courrier électronique (le cas échéant).
Adresse du destinataire	42	Enregistre l'adresse du destinataire des documents ou objets diffusés par courrier électronique (le cas échéant). Spécifiera également si l'adresse est incluse dans les champs A, Cc ou Cci. Un détail d'événement sera généré pour chaque destinataire prévu.
Nom du fichier	18	Enregistre le nom de fichier des documents ou objets diffusés par courrier électronique ou FTP, ou écrits directement sur un disque qui ne fait

Détail d'événement	ID	Description
		pas partie du déploiement Business Objects.
Nom du compte	45	Ceci enregistre l'un des suivants : <ul style="list-style-type: none"> <li>• Dans le cas des objets livrés par <i>boîte de réception</i>, une liste de noms de comptes utilisateur BusinessObjects.</li> <li>• Dans le cas des objets livrés par <i>FTP</i>, le nom de compte FTP.</li> <li>• Dans le cas des objets livrés par <i>disque non géré</i>, le compte de connexion utilisé.</li> <li>• Dans le cas des objets livrés par <i>SMTP</i>, le compte de connexion utilisé pour le serveur SMTP.</li> </ul>
Nom de l'imprimante	46	Nom de l'imprimante à laquelle a été livré le document ou l'objet (le cas échéant).
Nombre de copies	47	Nombre de copies du document ou de l'objet imprimé (le cas échéant).
Nom du destinataire	48	Noms d'utilisateur, nom du destinataire ou destinataires du document ou de l'objet. Un détail d'événement sera généré pour chaque destinataire prévu.
ID d'événement d'alerte	92	CUID de l'événement d'alerte. Celui-ci est généré uniquement si l'événement a été demandé par une alerte.
Nom d'événement d'alerte	93	Nom de l'événement d'alerte. Celui-ci est généré uniquement si l'événement a été demandé par une alerte.
Type de livraison	75	Indique comment la livraison a été initiée : <ul style="list-style-type: none"> <li>• "0" signifie planifié</li> <li>• "1" signifie envoyé à une destination</li> <li>• "2" signifie publié</li> <li>• "3" signifie qu'une alerte a été déclenchée</li> </ul>

#### Extraire

Un objet est extrait du CMS.

- ID de type d'événement : 1013

#### Se connecter

Un utilisateur se connecte.

- ID de type d'événement : 1014
- Statuts :

- "0" indique qu'une connexion de licence Utilisateur simultané s'est effectuée avec succès
- "1" indique qu'une tentative de connexion a échoué
- "2" indique qu'une connexion de licence Utilisateur nommé s'est effectuée avec succès
- "3" indique qu'une connexion non-utilisateur (système) s'est effectuée avec succès

Détail d'événement	ID	Description
Nombre d'utilisateurs simultanés	50	Nombre d'utilisateurs sur le système au moment du déclenchement de l'événement.
Nom d'hôte du client signalé par le client	51	Nom d'hôte du client tel que signalé par le client.
Nom d'hôte du client résolu par le serveur	52	Nom d'hôte du client tel que résolu par le serveur. Si le nom d'hôte du client ne peut être résolu, aucune valeur n'est enregistrée.
Adresse IP du client signalée par le client	53	Adresse IP du client telle que signalée par le client.
Adresse IP du client résolue par le serveur	54	Adresse IP du client telle que résolue par le serveur. Si l'IP du client ne peut être résolue, aucune valeur n'est enregistrée.

#### *Déconnexion.*

Un utilisateur se déconnecte.

- ID de type d'événement : 1015

Détail d'événement	ID	Description
Nombre d'utilisateurs simultanés	50	Nombre d'utilisateurs simultanés sur le système au moment du déclenchement de l'événement.

#### *Déclencher*

Un événement de fichier est déclenché.

- ID de type d'événement : 1016

Détail d'événement	ID	Description
Nom du fichier	18	Nom du fichier qui a été surveillé et a déclenché l'événement.

## 21.3.1.1 Événements 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 : droit ajouté=Exportation ; nouvelle valeur=Accordée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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 : droit supprimé=Exportation ; valeur précédente=Refusée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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 : droit modifié=Exportation ; valeur précédente=Accordée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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 : droit ajouté=Exportation ; nouvelle valeur=Accordée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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 : droit supprimé=Exportation ; valeur précédente=Refusée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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 : droit modifié=Exportation ; valeur précédente=Accordée ; périmètre=Objet actuel ; type d'objet applicable=tous les types d'objet.
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.
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	<p>Si la connexion du magasin de données d'audit est modifiée, enregistre les paramètres de la nouvelle connexion selon le format suivant :</p> <p>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.</p> <div> <p><b>i Remarque</b></p> <p>Les informations de mot de passe sont toujours masquées par * dans la base de données.</p> </div>
Intervalle de suppression automatique	105	Ce détail enregistre toute modification du champ <i>Supprimer les événements datant de plus de</i> dans la page Audit de la CMC. Cela définit le nombre de jours

Détail d'événement	ID	Description
		pendant lesquels les informations d'audit seront gérées dans l'ADS.

## 21.3.1.2 Événements 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 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

### 21.3.1.3 Événements 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.

### 21.3.1.4 Événements 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.
Élément 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.



## 22 Recherche de plateformes

### 22.1 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 est améliorée grâce aux fonctions suivantes :

- Effectuer une recherche sur le contenu de la plateforme de BI et d'Explorer.
- 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.

#### 22.1.1 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*.

## 22.1.2 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.

### Équilibrage 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.

## 22.2 Installation de la recherche de plateformes

### 22.2.1 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.

#### **i** Remarque

Les programmes client doivent respecter les normes OpenSearch pour communiquer avec la recherche de plateformes.

### **i** Remarque

Lorsque vous installez la plateforme de BI, le serveur d'applications Tomcat est installé par défaut.

## 22.2.1.1 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.

## 22.2.1.2 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.

## 22.2.2 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.

## 22.2.3 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 :

Table 91 :

Option	Description
Statistiques de recherche	<p>La recherche de plateformes fournit les statistiques de recherche suivantes :</p> <ul style="list-style-type: none"> <li>Statut de l'indexation : affiche le statut du processus d'indexation.</li> <li>Nombre de documents indexés : affiche le nombre de documents indexés.</li> <li>Dernier horodatage indexé : affiche l'horodatage de la dernière indexation du document.</li> </ul>
Arrêter/Démarrer l'indexation	<p>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.</p> <p>Pour arrêter l'indexation, cliquez sur <a href="#">Arrêter l'indexation</a>.</p>
Paramètres régionaux de l'index par défaut	<p>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.</p> <p>La recherche est basée sur les paramètres régionaux du produit du client et la pondération est accordée aux paramètres régionaux du produit du client.</p> <p>Vous pouvez configurer la pondération dans les propriétés de configuration de la CMC.</p>
Fréquence de l'analyse	<p>Vous pouvez indexer l'ensemble du référentiel de la plateforme de BI à l'aide des options suivantes :</p> <ul style="list-style-type: none"> <li>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.</li> <li>Analyse planifiée : avec cette option, l'indexation est basée sur la planification définie par les options de planification.</li> </ul> <p>Pour en savoir plus sur la planification d'un objet, consultez la section <i>Planification d'un objet</i> de l'application de recherche de plateformes dans l'<i>Aide en ligne de la CMC de la plateforme SAP BusinessObjects Business Intelligence</i>.</p> <div> <p><b>i Remarque</b></p> <ul style="list-style-type: none"> <li>Si vous sélectionnez <a href="#">Analyse planifiée</a> et définissez la <a href="#">Périodicité</a> sur une option autre que <a href="#">Maintenant</a>, l'application de recherche de plateformes affiche la date et l'horodatage de la prochaine indexation planifiée du document.</li> <li>Si vous sélectionnez <a href="#">Analyse planifiée</a>, le bouton <a href="#">Démarrer l'indexation</a> est activé et le bouton <a href="#">Arrêter l'indexation</a> est désactivé.</li> <li>Une fois la planification terminée, le bouton <a href="#">Arrêter l'indexation</a> est désactivé.</li> </ul> </div>

Option	Description
Emplacement de l'index	<p>Les index sont stockés dans des dossiers partagés aux emplacements suivants :</p> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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.</li> </ul> <p>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.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur&gt;\ContentStores.</p> <p>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 :</p> <ol style="list-style-type: none"> <li>1. {bobj.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur&gt;\ContentStores.</li> <li>2. {bobj.entreprise.home}\data\PlatformSearchData\workspace\&lt;Nom du serveur 1&gt;\ContentStores.</li> </ol> <ul style="list-style-type: none"> <li>○ 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.</li> </ul> <div> <p><b>i Remarque</b></p> <ul style="list-style-type: none"> <li>○ L'emplacement de l'index maître doit être un emplacement partagé.</li> <li>○ Vous devez cliquer sur <a href="#">Arrêter l'indexation</a> pour modifier l'emplacement de l'index.</li> <li>○ 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.</li> </ul> </div>

Option	Description
Niveau d'indexation	<p>Vous pouvez ajuster le contenu de la recherche en définissant le niveau d'indexation de l'une des façons suivantes :</p> <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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.</li> <li>○ Contenu complet : cet index comprend les métadonnées de plateformes, les métadonnées de documents et les autres contenus tels que : <ul style="list-style-type: none"> <li>○ Le contenu réel du document</li> <li>○ Le contenu des invites et listes de valeurs</li> <li>○ Diagrammes, graphiques et étiquettes</li> </ul> </li> </ul> <div> <p><b>i Remarque</b></p> <p>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.</p> </div> <div> <p><b>i Remarque</b></p> <p>Lorsque vous modifiez le niveau d'indexation, l'indexation est initialisée pour l'actualisation de l'ensemble du référentiel de la plateforme de BI.</p> </div>

Option	Description
Types de contenus	<p>Vous pouvez sélectionner les types de contenu suivants pour l'indexation :</p> <ul style="list-style-type: none"> <li>○ Crystal Reports</li> <li>○ Web Intelligence</li> <li>○ Univers</li> <li>○ Espace de travail BI</li> <li>○ Analysis Office</li> <li>○ Lumira</li> <li>○ Microsoft PowerPoint</li> <li>○ Adobe Acrobat</li> <li>○ Texte enrichi</li> <li>○ Texte</li> <li>○ Microsoft Word</li> <li>○ Microsoft Excel</li> </ul> <p>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.</p> <p>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.</p>
Régénérer l'index	<p>Cette option supprime les index existants et réindexe l'ensemble du référentiel.</p> <p>Vous pouvez sélectionner l'option <a href="#">Régénérer l'index</a>, 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.</p> <p>Si vous ne souhaitez pas que l'application de recherche de plateformes réindexe les documents, désélectionner l'option <a href="#">Régénérer l'index</a> avant de cliquer sur <a href="#">Démarrer l'indexation</a>.</p>



Option	Description
Documents exclus de l'indexation	<p>L'option <i>Documents exclus de l'indexation</i> 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.</p> <p>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 <i>Documents exclus de l'indexation</i> ne puissent pas être recherchés, vous devez régénérer l'index.</p> <p>Par défaut, seul le compte Administrateur dispose du contrôle complet de l'option <i>Documents exclus de l'indexation</i>. Les autres utilisateurs disposant des droits suivants peuvent seulement ajouter des documents aux <i>Documents exclus de l'indexation</i>.</p> <ul style="list-style-type: none"> <li>○ Droits de visualisation et de modification sur la catégorie</li> <li>○ Modifier le document directement</li> </ul>

5. Cliquez sur *Enregistrer et fermer*.

#### **i** 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.

## 22.3 Utilisation de la recherche de plateformes

### 22.3.1 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 \[page 623\]](#)

[Types de contenus pouvant être recherchés \[page 744\]](#)

### 22.3.2 Liste d'échecs d'indexation

La liste d'échecs d'indexation fournit la liste des documents qui n'ont pas pu être indexés. L'application de recherche de plateformes effectue trois tentatives pour indexer 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.

## 22.3.3 Recherche des résultats

### 22.3.3.1 Avant la recherche

#### 22.3.3.1.1 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.

## 22.3.3.1.2 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 :

Table 92 :

Type d'objet	Contenu indexé
Crystal Reports (2008, 2011 et 2013)	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)	<p>Données de toutes les cellules non vides, champs de la page</p> <p>Résumé des propriétés du document (titre, sujet, auteur, société, catégorie, mots clés et commentaires) et texte des entêtes et pieds de page des documents.</p> <p>Pour les cellules utilisant des calculs ou des formules, la valeur qui suit l'évaluation peut faire l'objet d'une recherche.</p> <p>Pour les valeurs numériques ou de date et heure, les données brutes peuvent faire l'objet d'une recherche.</p>
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 entêtes 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, Page AFDashboard, Dashboards, ObjectPackage, requête de service Web (QaaWS), Profil, Discussions, InformationDesigner, indicateurs pour la plateforme SAP BusinessObjects BI, MDAnalysis, Publications, Flash, Analyses et Hyperlien	Le contenu des métadonnées peut être recherché.

Type d'objet	Contenu indexé
Événements	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>La recherche de plateformes prend en charge les événements Crystal Reports pour Entreprise.</p> </div>
Espace de travail BI	<ul style="list-style-type: none"> <li>Le titre, la description et le contenu des modules BIW suivants sont indexés : <ul style="list-style-type: none"> <li>Module texte</li> <li>Module de page Web</li> <li>Module de liste de navigation</li> <li>Module de visualiseur</li> </ul> </li> <li>Le titre et la description d'un module composé sont indexés.</li> <li>Seul le titre d'un module de modèle d'espace de travail est indexé.</li> <li>Dans le cas d'un module de groupe, le titre et les métadonnées des modules en son sein sont indexés.</li> <li>Le titre, la description et le CUID des modules d'InfoObject sont indexés dans les espaces de travail BI.</li> </ul> <div> <p><b>i Remarque</b></p> <p>Etant 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.</p> </div> <ul style="list-style-type: none"> <li>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.</li> </ul>

Type d'objet	Contenu indexé
CR Next Gen	<p>Titre, description, formules de sélection, données enregistrées, champs de texte des sections, valeurs de paramètres et sous-rapports.</p> <p>Les objets suivants d'un rapport CR Next Gen ne sont pas pris en charge :</p> <ul style="list-style-type: none"> <li>• Rapport de tableau croisé</li> <li>• Extraction de données de diagramme</li> <li>• Extraction d'images et de métadonnées associées</li> <li>• OLE incorporé (par exemple, un document Word incorporé dans CR)</li> <li>• Extraction d'objet Flash</li> </ul> <p>En outre, il n'est pas possible de lire les données page par page à partir d'un rapport CR Next Gen.</p>
Univers	<p>Le contenu des données peut être recherché.</p> <div> <p><b>i Remarque</b></p> <p>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 :</p> <p><i>Select distinct SampleColumnName from SampleTableName LIMIT 1000.</i></p> <p>Suivez cette procédure pour désactiver l'indexation d'univers :</p> <ol style="list-style-type: none"> <li>1. Connectez-vous à la CMC (Central Management Console).</li> <li>2. Choisissez <i>Applications</i>.</li> <li>3. Accédez aux applications de recherche de plateformes et choisissez <i>Propriétés</i>.</li> <li>4. Accédez aux types de contenu et décochez <i>Univers</i>.</li> <li>5. Cliquez sur <i>Enregistrer et fermer</i>.</li> </ol> </div>
Document Lumira	Seul le contenu des métadonnées peut être recherché.
Document Analysis Office	Seul le contenu des métadonnées peut être recherché.

### **i Remarque**

La taille maximale prise en charge pour les documents agnostiques (MS Office 2003 et 2007 et documents PDF) est de 15 Mo.

## 22.3.3.2 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 concerne un nombre très important d'objets, elle peut échouer. Une nouvelle propriété "localizedsearch.folders" est ajoutée à `default/CmcApp.properties` et définie sur "true" (vrai) par défaut : `localizedsearch.folders=true`. Cette propriété doit être définie sur "false" (faux) pour désactiver la recherche localisée dans les dossiers : `localizedsearch.folders=false`. Redémarrez le serveur après avoir désactivé la recherche localisée. Des résultats non localisés seront renvoyés.

## 22.3.3.3 Après la recherche

### 22.3.3.3.1 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 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), Microsoft Excel (2003 et 2007) et Dashboards.
- 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.

## 22.3.3.3.2 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.

### 22.3.3.3.2.1 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. Ouvrir 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 \[page 623\]](#).

### 22.3.3.3.3 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.

## 22.3.3.3.4 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

## 22.3.3.3.5 Fédération des résultats de recherche SAP BusinessObjects Explorer

L'application de recherche de plateformes fédère les requêtes de recherche depuis SAP BusinessObjects Explorer et les InfoSpaces de surface en même temps que le contenu de la plateforme de BI.

Les résultats de la recherche SAP BusinessObjects Explorer sont groupés par catégories de métadonnées. Les facettes prises en charge pour les InfoSpaces incluent le type, l'emplacement et l'heure d'actualisation.

SAP BusinessObjects Explorer envoie la fréquence de terme à l'application Recherche de plateformes pour chaque terme de la requête de recherche. La recherche de plateformes calcule la pertinence en se basant sur la somme de la racine carrée des fréquences de termes. La valeur résultante est affectée en tant que score à chaque InfoSpace. Les résultats sont alors classés par score et envoyés au client.

## 22.4 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.

### 22.4.1 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.

## 22.4.2 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.

## 22.5 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.

## 22.6 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

## 22.7 Dépannage

### 22.7.1 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.

### 22.7.2 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 de 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.

### i 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.

### i 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 les versions 2008, 2011 et 2013. Elle n'indexe pas le contenu Crystal Reports pour Enterprise.

Cependant, avec Crystal Reports pour Enterprise, 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*.

---

## Impossible d'extraire des InfoSpaces SAP BusinessObjects Explorer

Vérifiez si les serveurs SAP BusinessObjects Explorer sont arrêtés ou désactivés. Activez les serveurs pour la recherche de plateformes afin d'extraire les résultats de la recherche depuis SAP BusinessObjects Explorer.

## 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 droits des utilisateurs, accédez à la zone [Authentification](#) de la CMC et sélectionnez [SAP](#).

## Informations associées

[Liste d'échecs d'indexation \[page 742\]](#)

[Configuration des propriétés de l'application dans la CMC \[page 623\]](#)

[Types de contenus pouvant être recherchés \[page 744\]](#)

## 23 Fédération

### 23.1 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 des 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, Flash, Word, TXT, RTF et Shockwave Flash	
Utilisateurs	utilisateurs, groupes, boîtes de réception, favoris et catégorie personnelle	



Catégorie	Types d'objets que vous pouvez répliquer	Remarques supplémentaires
Plateforme de Business Intelligence	Dossiers, événements, catégories, calendriers, niveaux d'accès, liens 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 gérant les informations répliquées de chaque objet. Par exemple, le logo correspondant, les informations de connexion à la base de données, etc. seront appliqués.

#### 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.

## 23.2 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.

<b>Application BI</b>	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.
<b>Site de destination</b>	Système de la plateforme de BI recevant un contenu de la plateforme de BI répliqué à partir d'un site d'origine.
<b>Local</b>	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.

<b>Instances finalisées exécutées localement</b>	Instances traitées sur le site de destination, puis retransmises au site d'origine.
<b>Sites d'origine multiples</b>	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.
<b>Réplication unidirectionnelle</b>	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.
<b>Site d'origine</b>	Système de la plateforme de BI d'où provient le contenu.
<b>Distant</b>	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.
<b>Connexion à distance</b>	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.
<b>Planification à distance</b>	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.
<b>Réplication</b>	Processus permettant de copier le contenu d'un système de la plateforme de BI vers un autre.
<b>Travail de réplication</b>	Objet contenant des informations sur la planification des réplifications et sur le contenu à répliquer ainsi que toute condition spécifique devant être appliquée lors de la réplication du contenu.
<b>Liste de réplication</b>	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.
<b>Objet de réplication</b>	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.
<b>Lot de réplifications</b>	Créé lors du transfert, le lot de réplifications 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 réplifications est implémenté sous la forme d'un fichier BIAR (BI Application Resource).
<b>Actualisation de la réplication</b>	Tous les objets d'une liste de réplication sont actualisés, quelle que soit la date de la dernière version modifiée.
<b>Réplication bidirectionnelle</b>	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.

## 23.3 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.

### 23.3.1 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	<p>Effectue des répliques uniquement à partir du site d'origine vers le site de destination.</p> <div><b>i Remarque</b> Les droits « Visualiser » et « Répliquer » sont requis pour tous les objets en cours de réplique, notamment les objets qui sont automatiquement répliqués par des calculs de dépendance.</div>	<ul style="list-style-type: none"><li>• Droits de « Visualiser » et « Répliquer » sur tous les objets à répliquer</li><li>• Droit de « visualisation » sur la liste de réplique</li></ul>
Réplication bidirectionnelle	Effectue des répliques à partir du site d'origine vers le site de destination, et du site de destination vers le site d'origine.	<ul style="list-style-type: none"><li>• Droits de « Visualiser » et « Répliquer » sur tous les objets à répliquer</li><li>• Droit de « visualisation » sur la liste de réplique</li></ul>

Action	Description	Droits requis
		<ul style="list-style-type: none"> <li>• Droit « Modifier les droits » sur les objets personnels afin de pouvoir répliquer les changements de mot de passe</li> </ul>
Planification	Autorise l'exécution de la planification à distance sur le site d'origine à partir du site de destination.	<ul style="list-style-type: none"> <li>• Droit de « Planifier » pour tous les objets devant être planifiés à distance</li> </ul>

## Informations associées

[Droits requis sur le site de destination \[page 760\]](#)

### 23.3.2 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 réplification. Il s'agit du compte de l'utilisateur ayant créé le travail de réplification.

#### Remarque

Tout comme d'autres objets planifiables, vous pouvez planifier le travail de réplification à la place d'un autre utilisateur.

Action	Description	Droits requis
Tous les objets	Réplique les objets, que la réplification soit unidirectionnelle ou bidirectionnelle.	<ul style="list-style-type: none"> <li>• Droits de « Visualisation », « Ajout », « Modification » et « Modification des droits » sur tous les objets</li> <li>• Droit de « Modifier le mot de passe utilisateur » pour tous les objets de l'utilisateur</li> </ul>
Première réplification	Lors de la première exécution d'un travail de réplification, aucun objet n'existe encore sur le site de destination. Par conséquent, le compte utilisateur sous lequel le travail de réplification est exécuté doit disposer de droits sur tous les dossiers et objets de niveau supérieur auxquels du contenu sera ajouté.	<ul style="list-style-type: none"> <li>• Droits de « Visualiser », « Ajouter », « Modifier » et « Modifier des droits » sur tous les dossiers de niveau supérieur et objets par défaut</li> </ul>

## Informations associées

[Droits requis sur le site d'origine \[page 759\]](#)

### 23.3.3 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.	<ul style="list-style-type: none"><li>Le compte sous lequel s'exécute le travail de réplication requiert des droits de « Suppression » sur les objets susceptibles d'être supprimés.</li></ul>
Désactivez le nettoyage pour certains objets	<p>Lorsque certains objets sont répliqués à partir du site d'origine, vous ne souhaitez 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.</p> <p>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 souhaitez peut-être pas perdre cet univers sur le site de destination s'il est supprimé du site d'origine.</p>	<ul style="list-style-type: none"><li>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.</li></ul>
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	<ul style="list-style-type: none"><li>Refusez les droits « Modifier » pour le compte utilisateur utilisé pour se connecter à l'objet Connexion à distance.</li></ul>

Action	Description	Droits requis
	<p>activer la planification à distance mais que vous ne voulez pas que les modifications apportées soient répercutées sur le site d'origine.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>	

## 23.3.4 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 pas 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.

### 23.3.5 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.

#### **i** Remarque

Les niveaux d'accès par défaut ne sont pas répliqués mais les références sont conservées.

## 23.4 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

### 23.4.1 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

## 23.4.2 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.

### **i** 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 \[page 789\]](#)

## 23.4.3 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.

## 23.5 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.

### **i** Remarque

Après la toute première réplique 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](#).

### **i** 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 identifiants 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.

## 23.6 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.

### **i** Remarque

Si vous utilisez la réplique 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 répliques 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 réplique qui contient les univers :

- [Inclure les connexions utilisées par les univers sélectionnés](#)
- [Inclure les univers requis par les univers sélectionnés](#)

### **i** 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 ».

## 23.7 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	<p>Objets tels que les vues d'entreprise, les connexions de données, les listes de valeurs, les fondations de données, etc.</p> <div> <b>Remarque</b> Tous les objets sont pris en charge, bien qu'ils ne le soient pas au niveau individuel.</div>
Rapports	<p>Rapports Crystal, documents Web Intelligence et objets Dashboards.</p> <div> <b>Remarque</b> Le module complémentaire et les modèles Full Client sont pris en charge.</div>

Catégorie	Objets pris en charge
Objets tiers	Fichiers Excel, PDF, PowerPoint, Flash, Word, texte, RTF et Shockwave Flash.
Utilisateurs	Utilisateurs, groupes, boîtes de réception, favoris, catégorie personnelle.
Plateforme Business Intelligence	Dossiers, événements, catégories, calendriers, rôles personnalisés, liens hypertexte, raccourcis, programmes, profils, lots d'objets, objets agnostiques.
Univers	Univers, connexions, surcharges d'univers.

### **i** 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

## 23.7.1 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.

### 23.7.1.1 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

## 23.7.1.2 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](#) ► [Nouvelle](#) ► [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 dépendants	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 dépendances prises en charge des objets Flash sélectionnés	Réplique tout rapport Crystal, lien hypertexte, document Web Intelligence ou univers dont l'objet Flash dépend.
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 connexion à un 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 en cet emplacement. Cependant, si

vous activez [Inclure les univers pour les 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 de référentiel](#) sous [Tout répliquer](#) pour répliquer tous les objets Vue d'entreprise, Eléments 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](#).

## 23.7.2 Modification des listes de réplication

Une fois la liste de réplication créée, vous pouvez modifier ses propriétés ou ses objets.

### 23.7.2.1 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 \[page 769\]](#)

## 23.7.2.2 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 \[page 769\]](#)

## 23.8 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.

### i 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.

### 23.8.1 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.

#### 23.8.1.1 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.

## 23.8.1.2 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 ».

Table 93 :

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	<p>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 :</p> <p><b>http://</b>  <b>&lt;nom_ordinateur_votreserveur_application&gt;:&lt;port&gt;/</b>  <b>dswsbobje</b></p> <p>Exemple : <b>http://</b>  <b>&lt;monordinateur.mondomaine.com&gt;:&lt;8080&gt;/dswsbobje</b></p>

Champ	Description
CMS de système distant	<p>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 : <b>CMS_Name:port</b>.</p> <p>Exemple : <b>&lt;monordinateur&gt;: 6400</b></p> <div> <p><b>i Remarque</b></p> <p>Si vous utilisez le port 6400 par défaut, l'indication du port est facultative.</p> </div>
Nom d'utilisateur	<p>Nom d'utilisateur utilisé pour la connexion au site d'origine.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>
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**.

## 23.8.2 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](#).

## 23.9 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.

### 23.9.1 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.

#### 23.9.1.1 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
<a href="#">Activer le nettoyage des objets sur la destination</a>	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>Le nettoyage des objets ne supprime pas les objets répliqués à l'aide de dépendances ou d'objets sélectionnés dans la liste de réplication.</p> </div>
<a href="#">Réplication unidirectionnelle</a>	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.
<a href="#">Réplication bidirectionnelle</a>	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.
<a href="#">Le site d'origine est prioritaire</a>	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.
<a href="#">Pas de résolution automatique de conflit</a>	Indique qu'aucune action n'est prise pour résoudre les conflits détectés.
<a href="#">Le site de destination est prioritaire</a> (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.
<a href="#">Réplication normale</a>	Indique que le travail de réplication est exécuté normalement.
<a href="#">Actualiser à partir du site d'origine</a>	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.
<a href="#">Actualiser à partir de la destination</a> (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.
<a href="#">Répliquer tous les objets</a> (disponible uniquement avec la réplication bidirectionnelle)	Réplique l'intégralité de la liste de réplication.

Option	Description
	<p><b>i Remarque</b></p> <p>Il s'agit de l'option la plus complète, mais aussi de la plus longue en termes de temps d'exécution.</p>
<i>Répliquer les planifications distantes</i> (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 des instances finalisées du site d'origine vers le site de destination.
<i>Répliquer les modèles de document</i>	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.
<i>Répliquer les instances finalisées exécutées localement</i>	Réplique les instances finalisées uniquement du site de destination vers le site d'origine.

10. Cliquez sur **OK**.

## 23.9.2 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.

### **i 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.

### 23.9.2.1 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.

### 23.9.3 Modification des travaux de réplication

Après la création d'un travail de réplication dans Fédération, vous pouvez modifier ses propriétés.

### 23.9.3.1 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.

### 23.9.4 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 Adaptive 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

## 23.10 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.

### 23.10.1 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.

## 23.10.2 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.

### i 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.

## 23.10.3 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.

### i 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 souhaitez 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 \[page 780\]](#)

## 23.11 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.

### 23.11.1 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 ».

#### **i 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.

#### **i 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.

## **23.11.2 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 réplifications 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 réplifications 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 ».

#### **i** 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.

#### **i** 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.

#### **i** 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.

## **23.12 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 souhaitez 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.

## 23.12.1 Variables de session

Si vous transférez de nombreux fichiers de contenu dans un même travail de réplication, vous souhaitez 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*.

## 23.12.2 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.

#### i 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>
```

#### **i** 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*.

## 23.12.3 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*.

## 23.13 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.

### 23.13.1 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) ».

#### **i** 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 réplifications, 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 \[page 759\]](#)

## 23.13.2 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 souhaitez 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.

## 23.13.3 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 répliques. 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 posséderont 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 \[page 759\]](#)

## 23.14 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.

### 23.14.1 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.

## 23.14.2 Importation de contenu répliqué et réplication continue

Après l'importation du contenu répliqué, vous souhaitez 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 ».

### i 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 réplifications 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.

## 23.14.3 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.

#### **i** 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.

## 23.14.4 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.

#### **i** Remarque

Une fois que vous avez copié un objet répliqué, le CUID de la copie est modifié et la copie ne contiendra aucune information de réplication.

## 23.15 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 `-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 "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dboj.enterprise.home=${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
```

3. Augmentez la valeur du paramètre `-Xmx1024m` pour définir la taille voulue.

### Exemple

Pour augmenter la mémoire à 2 Go, saisissez `-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 "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dobj.enterprise.home=${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.

Exemple : **JAVA\_OPTS="\$JAVA\_OPTS -Xmx1024m -XX:MaxPermSize=256m -Dobj.biar.suggestSplit=90 -Dobj.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,Dobj.federation.WSTimeout=<délai d'attente en minutes>`
  - **Unix** : `-javaArgs Xmx512m,Dobj.federation.WSTimeout=<délai d'attente en minutes>`

## Informations associées

[Dépannage des messages d'erreur \[page 798\]](#)

[Utilisation des services Web dans Fédération \[page 786\]](#)

[Limites de la version actuelle \[page 797\]](#)

## 23.15.1 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 \[page 779\]](#)

## 23.15.2 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 ASX00Fyvy0FJnRcD0dZNTZg (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. La requête a 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:MaxPermSize=256m".`
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) 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=<RépTemp>`.

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=<RépTemp> ».`

Dans les exemples ci-dessus, `<RépTemp>` représente l'emplacement du répertoire temporaire que vous souhaitez utiliser.

## 12) 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 \[page 794\]](#)

[Limites de la version actuelle \[page 797\]](#)

## 24 Configurations supplémentaires pour les environnements Enterprise Resource Planning

### 24.1 Configurations pour l'intégration SAP NetWeaver

#### 24.1.1 Intégration avec SAP Business Warehouse (BW)

##### 24.1.1.1 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 \[page 303\]](#)

##### 24.1.1.1.1 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.

#### **i** 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 \[page 139\]](#)

[Fonctionnement des droits sur la plateforme de BI \[page 125\]](#)

### 24.1.1.1.2 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.

## 24.1.1.2 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.

### 24.1.1.3 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.

#### 24.1.1.3.1 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.

#### 24.1.1.3.2 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.

#### 24.1.1.3.3 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.

### 24.1.1.3.4 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.

### 24.1.1.3.5 Configuration de BW Publisher avec une passerelle SAP locale

#### **i** 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 \[page 807\]](#).
- [Configuration d'une destination pour BW Publisher \[page 808\]](#).

### 24.1.1.3.6 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.

#### **24.1.1.4 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.

#### **24.1.1.5 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

#### **24.1.1.6 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.

## 24.1.1.7 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 \[page 311\]](#).
- [Configuration des dossiers et de la sécurité sur la plateforme de BI \[page 803\]](#).
- [Paramètres de sécurité par défaut des dossiers \[page 804\]](#).

## 24.1.1.8 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.

Table 94 : Autorisations réservées aux utilisateurs administratifs

Objet d'autorisation	Champ	Valeurs
S_RFC S_TCODE	RFC_TYPE	FUGR
	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&

Objet d'autorisation	Champ	Valeurs
	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)

Table 95 : 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

Table 96 :

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	
		ACTVT	Affichage (03)

### 24.1.1.9 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.

#### 24.1.1.9.1 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.

### **i** 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.

### **i** 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.



### **i** 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.

### **i** 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 \[page 806\]](#)

[Importation de rôles SAP \[page 311\]](#)

## 24.1.1.10 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 \[page 829\]](#)) peuvent utiliser le Workbench d'administration de contenu pour publier et gérer des rapports.

## 24.1.1.11 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 \[page 815\]](#)

### 24.1.1.12 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 \[page 816\]](#).

### 24.1.1.13 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.

## 24.1.1.14 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).

### 24.1.1.14.1 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 \[page 815\]](#)), ou mettre à jour manuellement le statut du rapport à l'aide de l'outil Maintenance des rapports.

### 24.1.1.14.2 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.

## 24.1.1.15 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.

## 24.1.1.16 Configurations pour le traitement de données SAP

### 24.1.1.16.1 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\_OPENSQ\_L\_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.

#### **i** 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 \[page 844\]](#)

### 24.1.1.16.2 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_OPENSQ_L_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.

## 24.1.1.17 Configurations pour les transports SAP

### 24.1.1.17.1 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\.`

#### **i** 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.

## **24.1.1.17.2 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 \[page 829\]](#)

## 24.1.17.2.1 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).

## 24.1.17.2.2 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.

## 24.1.1.17.2.3 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.

## 24.1.1.17.2.4 Transports

### 24.1.1.17.2.4.1 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.

Table 97 :

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/OPENSQ	Groupe de fonctions	Fonctions Open SQL
/CRYSTAL/OSQL_AUTH_FORMS	Programme	Programme d'aide

Objet	Type	Description
/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
/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

Objet	Type	Description
ZSSAUTHKEY	Tableau	Anciennes métadonnées de RLS
ZSSAUTHREF	Tableau	Anciennes métadonnées de RLS
ZSSAUTH FCN	Tableau	Anciennes métadonnées de RLS

## 24.1.1.17.2.4.2 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.

Table 98 :

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/FLAT	Groupe de fonctions	Fonctions wrapper InfoSet
/CRYSTAL/QUERY_BATCH	Programme	Exécution du mode batch
/CRYSTAL/QUERY_BATCH_STREAM	Programme	Exécution du mode batch en continu

## 24.1.1.17.2.4.3 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.

Table 99 :

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

Objet	Type	Description
/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

## 24.1.1.17.2.4.4 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.

Table 100 :

Objet	Type	Description
ZCIMPRBG	Programme	Programme principal
ZCRBGTOP	Programme	Programme d'inclusion
ZCDD	Transaction	Transaction du programme principal

## 24.1.1.17.2.4.5 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.

Table 101 :

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	Élément de données	Activité de rapport
/CRYSTAL/OBJ_POLICY	Élément 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_ADMIN_CLASS_D	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_CLASS_I	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_CTREE	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_FORMS	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_MODULES	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_PAIS	Programme	Composant de programme
/CRYSTAL/CONTENT_ADMIN_PBOS	Programme	Composant de programme
/CRYSTAL/ CONTENT_ADMIN_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_WORKER_FORMS	Programme	Composant de programme

Objet	Type	Description
/CRYSTAL/PUBLISH_WORKER_PROC	Programme	Composant de programme
/CRYSTAL/ PUBLISH_WORKER_PROC_I	Programme	Composant de programme
/CRYSTAL/ PUBLISH_WORKER_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
/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

## 24.1.1.17.2.4.6 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).

Table 102 :

Objet	Type	Description
/CRYSTAL/BC	ID	Classe de développement
/CRYSTAL/ODS_REPORT	Groupe de fonctions	Fonctions ODS

## 24.1.1.17.2.4.7 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.

Table 103 :

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

## 24.1.1.17.2.4.8 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).

Table 104 :

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_STREAMINFO	Classe	Exception
/CRYSTAL/CX_NO_MORE_CELLS	Classe	Exception

Objet	Type	Description
/CRYSTAL/CX_NO_MORE_MEMBERS	Classe	Exception
/CRYSTAL/CX_NO_MORE_PROPERTIES	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

## 24.1.1.18 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.



## 24.1.1.18.1 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 \[page 808\]](#)

## 24.1.1.19 Actions dans BW

Cette section contient une liste des actions disponibles dans BW.

### 24.1.1.19.1 Actions au sein de Crystal Reports

#### 24.1.1.19.1.1 Création d'un rapport à partir d'une requête dans un rôle BW

Table 105 :

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>**

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

<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.

## 24.1.1.19.12 Ouverture d'un rapport existant à partir d'un rôle BW

Table 106 :

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>**

Objet d'autorisation	Champ	Valeurs
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.

### 24.1.19.1.3 Actualisation ou affichage de l'aperçu d'un rapport

Table 107 :

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.

## 24.1.19.1.4 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Table 108 :

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.

## 24.1.19.1.5 Définition de l'emplacement de la source de données

Table 109 :

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>**

Objet d'autorisation	Champ	Valeurs
	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.

## 24.1.1.19.1.6 Enregistrement d'un rapport dans un rôle BW

Table 110 :

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.

## 24.1.1.19.1.7 Préparation d'un rapport pour la traduction lors de l'enregistrement dans BW

Table 111 :

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.

## 24.1.1.19.1.8 Enregistrement et publication simultanée d'un rapport sur la plateforme de BI

Table 112 :

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.

## 24.1.1.19.1.9 Démarrage de BEx Query Designer™

Table 113 :

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	<INFO_AREA> **
	RSINFOCUBE	<INFO_CUBE> **

Objet d'autorisation	Champ	Valeurs
S_RS_COMP1	RSZCOMPTP	REP
	RSZCOMPID	<COMP_ID>**
	RSZCOMPID	<COMP_ID>**
	RSZCOMPTP	REP
S_CTS_ADMI	RSZOWNER	<QUERY_OWNER>*
	ACTVT	16
	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.

## 24.1.1.19.2 Actions au sein de la zone de lancement BI

### 24.1.1.19.2.1 Connexion à la plateforme de BI à l'aide des références de connexion SAP

Table 114 :

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

### 24.1.1.19.2.2 Visualisation d'un rapport SAP BW à la demande

Table 115 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI

Objet d'autorisation	Champ	Valeurs
	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	OCRM_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.

## 24.1.1.19.2.3 Actualisation d'un rapport à partir du visualiseur

Table 116 :

Objet d'autorisation	Champ	Valeurs
S_RS_COMP	RSINFOAREA	<INFO_AREA>**
	RSINFOCUBE	<INFO_CUBE>**
	RSZCOMPTP	REP
	RSZCOMPID	<COMP_ID>**



Objet d'autorisation	Champ	Valeurs
S_RS_COMP1	RSZCOMPID	<COMP_ID>**
	RSZCOMPTP	REP
	RSZOWNER	<QUERY_OWNER>*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<INFO_AREA>**
	RSODSOBJ	OCRM_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.

## 24.1.19.2.4 Planification d'un rapport

Table 117 :

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

Objet d'autorisation	Champ	Valeurs
	RSZOWNER	<QUERY_OWNER>*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<INFO_AREA>**
	RSODSOBJ	OCRM_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.

## 24.1.19.2.5 Lecture des listes de choix dynamiques dans les paramètres de rapport

Table 118 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

## 24.1.19.3 Actions au sein de SAP NetWeaver (ABAP)

### 24.1.19.3.1 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.

## 24.1.1.19.3.2 Connexion à un serveur SAP

Table 119 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16

## 24.1.1.19.3.3 Création d'un rapport

Table 120 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	01

## 24.1.1.19.3.4 Ouverture ou affichage de l'aperçu d'un rapport existant

Table 121 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

### 24.1.1.19.3.5 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Table 122 :

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

### 24.1.1.19.3.6 Définition de l'emplacement de la source de données

Table 123 :

Objet d'autorisation	Champ	Valeurs
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

### 24.1.1.19.4 Actions au sein de Crystal Reports à l'aide du pilote InfoSet et reporting à partir d'InfoSet

#### 24.1.1.19.4.1 Connexion à un serveur SAP

Table 124 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST

Objet d'autorisation	Champ	Valeurs
	ACTVT	16

## 24.1.1.19.4.2 Création d'un rapport à partir d'un InfoSet sur SAP NetWeaver (ABAP)

Table 125 :

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 \[page 842\]](#)

## 24.1.1.19.4.3 Vérification de la base de données (actualisation des définitions des tables d'un rapport)

Table 126 :

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

## 24.1.1.19.4.4 Définition de l'emplacement de la source de données

Table 127 :

Objet d'autorisation	Champ	Valeurs	
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP	
		COARS	2

## 24.1.1.19.5 Actions au sein de Crystal Reports à l'aide du pilote InfoSet et reporting à partir d'une requête ABAP

### 24.1.1.19.5.1 Connexion à un serveur SAP

Table 128 :

Objet d'autorisation	Champ	Valeurs
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

### 24.1.1.19.5.2 Création d'un rapport à partir d'une requête ABAP sur SAP NetWeaver

Table 129 :

Objet d'autorisation	Champ	Valeurs
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	Nom du groupe de tables

## 24.1.1.19.5.3 Vérification de la base de données

Table 130 :

Objet d'autorisation	Champ	Valeurs
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

## 24.1.1.19.5.4 Définition de l'emplacement de la source de données

Table 131 :

Objet d'autorisation	Champ	Valeurs
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Nom du groupe de tables

## 24.1.1.19.6 Actions au sein de la plateforme de BI

### 24.1.1.19.6.1 Planification d'un rapport en mode dialogue (à l'aide d'une requête Open SQL)

Table 132 :

Objet d'autorisation	Champ	Valeurs
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

#### Remarque

La valeur de CLASS est BLANK (VIDE).

### 24.1.1.19.6.2 Planification d'un rapport en mode de traitement par lot à l'aide d'une requête Open SQL

Table 133 :

Objet d'autorisation	Champ	Valeurs
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQ, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE



Objet d'autorisation	Champ	Valeurs
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

**i Remarque**

La valeur de CLASS est BLANK (VIDE).

## 24.1.1.19.6.3 Système d'autorisation Crystal

Table 134 :

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)	<p>*</p> <p><b>i Remarque</b></p> <p>Pour plus de sécurité, vous pouvez répertorier explicitement les groupes d'utilisateurs dont les membres doivent accéder à la plateforme de BI.</p>

## 24.1.1.19.6.4 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.

Table 135 :

Objet d'autorisation	Champ	Valeurs
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

## 24.2 Configuration pour l'intégration JD Edwards

### 24.2.1 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.

#### 24.2.1.1 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](#).

#### 24.2.1.2 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*.

## 24.2.2 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`).

### 24.2.2.1 Pour activer la connectivité des données avec SSL pour JD Edwards EnterpriseOne

#### **i** 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.

## 24.2.2.2 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.ora.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.

## 24.3 Configuration pour l'intégration PeopleSoft Enterprise

### 24.3.1 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.

#### 24.3.1.1 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](#).

## 24.3.1.2 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](#).

## 24.3.2 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`).

### 24.3.2.1 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\`.

## 24.3.2.2 Pour activer le serveur de requêtes PeopleSoft avec SSL

### i 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.

## 24.3.2.3 Pour activer la passerelle de sécurité avec SSL

### i 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.

## 24.3.3 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*.

### 24.3.3.1 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.

### 24.3.3.2 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.

#### i 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.

## 24.4 Configuration pour l'intégration Siebel

### 24.4.1 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\`.



## 24.4.1.1 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**.

## 24.4.2 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 **Élément 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 **Éléments 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 \[page 854\]](#).

## 24.4.2.1 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, régénérez 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 apparaître 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.

## 24.4.3 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.

### 24.4.3.1 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.

### 24.4.3.2 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"
```

#### **i** 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.

#### **i** Remarque

La variable `userDomain` est sensible à la casse.

### 24.4.3.3 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.

#### **i** 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.

### 24.4.3.4 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`.

#### **i** Remarque

Les Outils Siebel sont nécessaires pour terminer les étapes de cette section.

## 24.4.4 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.

### 24.4.4.1 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.

### 24.4.4.2 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.

## 24.4.5 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.ora.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.`

### 24.4.5.1 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.

## 25 Gestion et configuration des journaux

### 25.1 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.

### 25.2 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 <code>.ini</code> ).
Aucun	Aucun suivi n'est effectué.



Niveau	Description
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	<p>Aucun message n'est filtré. Ce niveau est recommandé pour les besoins du débogage.</p> <div>  <b>Attention</b>            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.         </div>

## 25.3 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`.

## 25.3.1 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 \[page 596\]](#)

## 25.3.2 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 596]

### 25.3.3 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
<code>sap_log_level</code>	<code>log_information</code> <code>log_warning</code> <code>log_error</code> <code>log_fatal</code> <code>log_none</code>	<p>Détermine la gravité des messages du journal. La gravité par défaut est <code>log_error</code>.</p> <p>La gravité du journal respecte une hiérarchie, avec <code>log_information</code> au niveau supérieur et <code>log_none</code> 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 <code>log_warning</code>, les messages comprenant <code>log_warning</code>, <code>log_error</code> et <code>log_fatal</code> seront écrits dans le fichier journal.</p> <div><p><b>i Remarque</b></p><p><code>log_information</code> et <code>log_warning</code> peuvent être abrégés en <code>log_info</code> et <code>log_warn</code>.</p></div>
<code>sap_trace_level</code>	<code>trace_debug</code> <code>trace_path</code> <code>trace_information</code> <code>trace_error</code> <code>trace_none</code>	<p>Détermine la gravité des messages de suivi. La gravité par défaut du suivi est <code>trace_error</code>.</p>

Nom du paramètre	Valeurs possibles	Description
		<p>La gravité du suivi respecte une hiérarchie, avec <b>trace_debug</b> au niveau supérieur et <b>trace_none</b> 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 <b>trace_path</b>, les messages incluant <b>trace_path</b>, <b>trace_information</b> et <b>trace_error</b> seront écrits dans le fichier journal.</p> <p><b>i Remarque</b>  <b>trace_information</b> peut être abrégé en <b>trace_info</b>.</p>

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;
```

### 25.3.3.1 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.

## 25.4 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.

- Sous Windows, l'emplacement par défaut est `C:\SBOPWebapp_<APPLICATION>_<ADRESSEIP>_<PORT>\`  
Par exemple, `C:\SBOPWebapp_ZoneLancementBI_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

#### i 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 `dswebobje.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*.

## 25.4.1 Pour définir le niveau du journal 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, 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](#).

Le nouveau niveau du journal de suivi prend effet après la prochaine connexion à l'application Web.

## Informations associées

[Niveaux du journal de suivi \[page 596\]](#)

## 25.4.2 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 `dswsboobje.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 `dswsboobje.war` est disponible sous : `<REPINSTALL>\Tomcat\webapps\dswsboobje\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 `dswebobje.war` est `<REPINSTALL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\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
<code>sap_log_level</code>	<code>log_information</code> <code>log_warning</code> <code>log_error</code> <code>log_fatal</code> <code>log_none</code>	<p>Détermine la gravité des messages du journal. La gravité par défaut est <code>log_error</code>.</p> <p>La gravité du journal respecte une hiérarchie, avec <code>log_information</code> au niveau supérieur et <code>log_none</code> 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 <code>log_warning</code>, les messages comprenant <code>log_warning</code>, <code>log_error</code> et <code>log_fatal</code> seront écrits dans le fichier journal.</p> <div> <b>Remarque</b> <code>log_information</code> et <code>log_warning</code> peuvent être abrégés en <code>log_info</code> et <code>log_warn</code>.</div>
<code>sap_trace_level</code>	<code>trace_debug</code> <code>trace_path</code> <code>trace_information</code> <code>trace_error</code> <code>trace_none</code>	<p>Détermine la gravité des messages de suivi. La gravité par défaut du suivi est <code>trace_error</code>.</p>

Nom du paramètre	Valeurs possibles	Description
		<p>La gravité du suivi respecte une hiérarchie, avec <b>trace_debug</b> au niveau supérieur et <b>trace_none</b> 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 <b>trace_path</b>, les messages incluant <b>trace_path</b>, <b>trace_info</b> et <b>trace_error</b> seront écrits dans le fichier journal.</p> <div> <i>i</i> Remarque           <p><b>trace_information</b> peut être abrégé en <b>trace_info</b>.</p> </div>

- Enregistrez, puis fermez le fichier `BO_trace.ini`.
- 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.

## 25.4.2.1 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	<code>BOE.war</code>	<code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\warfiles \webapps\BOE\WEB-INF \TraceLog</code>
Zone de lancement BI	<code>BOE.war</code>	<code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\warfiles \webapps\BOE\WEB-INF \TraceLog</code>



Application Web	Fichier WAR	Emplacement prédéployé
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

- 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

### **i** Remarque

Si vous utilisez le serveur d'applications Web Tomcat fourni, ignorez l'étape 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
- 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/
- 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	<code>WebApp_BIlaunchpad</code>
Central Management Server	<code>WebApp_CMC</code>
OpenDocument	<code>WebApp_OpenDocument</code>

Les paramètres suivants sont utilisés pour configurer le suivi du serveur d'applications Web :

Nom du paramètre	Valeurs possibles	Description
<code>sap_log_level</code>	<code>log_information</code> <code>log_warning</code> <code>log_error</code> <code>log_fatal</code> <code>log_none</code>	<p>Détermine la gravité des messages du journal. La gravité par défaut est <code>log_error</code>.</p> <p>La gravité du journal respecte une hiérarchie, avec <code>log_information</code> au niveau supérieur et <code>log_none</code> 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 <code>log_warning</code>, les messages comprenant <code>log_warning</code>, <code>log_error</code> et <code>log_fatal</code> seront écrits dans le fichier journal.</p> <div> <p><b>i Remarque</b></p> <p><code>log_information</code> et <code>log_warning</code> peuvent être abrégés en <code>log_info</code> et <code>log_warn</code>.</p> </div>
<code>sap_trace_level</code>	<code>trace_debug</code> <code>trace_path</code> <code>trace_information</code> <code>trace_error</code> <code>trace_none</code>	<p>Détermine la gravité des messages de suivi. La gravité par défaut du suivi est <code>trace_error</code>.</p> <p>La gravité du suivi respecte une hiérarchie, avec <code>trace_debug</code> au niveau supérieur et <code>trace_none</code> 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 <code>trace_path</code>, les messages incluant <code>trace_path</code>, <code>trace_info</code> et <code>trace_error</code> seront écrits dans le fichier journal.</p>

Nom du paramètre	Valeurs possibles	Description
		<p><b>i</b> Remarque</p> <p><code>trace_information</code> peut être abrégé en <code>trace_info</code>.</p>

- Enregistrez, puis fermez le fichier `BO_trace.ini`.
- Utilisez Wdeploy pour déployer le fichier `.war` sur l'ordinateur hébergeant le serveur d'applications Web.

## 25.5 Configuration du suivi pour l'outil de gestion de mise à niveau

Il est impossible d'effectuer la configuration du suivi pour l'outil de gestion de mise à niveau à l'aide de la CMC. Vous devez effectuer le suivi de l'outil de gestion de mise à niveau à l'aide du 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/`

### 25.5.1 Pour configurer le suivi pour l'outil de gestion de mise à niveau

- 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/`
- Retirez les commentaires des lignes requises sous la section *Trace Syntax and Setting*.
- Utilisez une instruction `if` pour spécifier les paramètres de suivi. Par exemple :

```
if (process == "upgrademanagementtool") {
    sap_log_level=log_warning;
    sap_trace_level=trace_path;
}
```

#### ➔ Conseil

Le processus doit être spécifié comme `upgrademanagementtool` pour le paramètre de suivi à appliquer à l'outil de gestion de mise à niveau.

- Enregistrez, puis fermez le fichier `BO_trace.ini`.
- Les paramètres modifiés s'appliquent dans les cinq minutes.

---

## 25.6 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 \[page 863\]](#) 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.


## 26 Intégration à SAP Solution Manager

### 26.1 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://websmp205.sap-ag.de/bosap-support> 

### 26.2 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.

Table 136 :

Prise en charge de SAP Solution Manager	Nécessaire pour la plateforme de BI
enregistrement SLD	<ul style="list-style-type: none"> <li>SAPHOSTAGENT doit être installé pour permettre l'enregistrement des serveurs de la plateforme de BI.</li> </ul> <div> <p><b>i Remarque</b></p> <p>Le programme d'installation de la plateforme de BI enregistrera automatiquement les serveurs si SAPHOSTAGENT est déjà installé.</p> </div> <ul style="list-style-type: none"> <li>Doit créer un fichier connect.key pour le fournisseur de données créant des rapports sur les serveurs clés.</li> <li>(Facultatif) Pour l'enregistrement SLD avec WebSphere 6.1 ou 7, l'outil d'enregistrement SLDREG doit être installé sur chaque serveur d'applications WebSphere. Pour en savoir plus, voir la note SAP 1482727.</li> <li>(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.</li> <li>(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.</li> </ul>
Intégration SMD	<ul style="list-style-type: none"> <li>Doit télécharger et installer l'agent SMD (DIAGNOSTICS.AGENT) sur tous les hôtes des serveurs de la plateforme de BI.</li> <li>Le compte utilisateur SMAAdmin doit être activé sur la plateforme de BI.</li> </ul>
Instrumentation des performances	<ul style="list-style-type: none"> <li>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.</li> <li>L'agent SMD doit être installé.</li> <li>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.</li> </ul>
Passeport SAP	<ul style="list-style-type: none"> <li>Vous devez télécharger et installer l'outil client Passeport SAP.</li> </ul>

## 26.3 Gestion de l'enregistrement du répertoire du paysage système

### 26.3.1 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 répertoire du paysage système contient une description du paysage 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.

#### **i** 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.

### **26.3.1.1 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.

#### **i** 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.

## 26.3.2 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.

### **i** 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.

## 26.3.3 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.

## 26.4 Gestion des agents Solution Manager Diagnostics

### 26.4.1 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.

### 26.4.2 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 : <http://service.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.

## 26.4.3 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.

### 26.4.3.1 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*.

## 26.5 Gestion de l'instrumentation des performances

### 26.5.1 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.

## 26.5.2 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 \[page 877\]](#)

### 26.5.2.1 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 <code>true</code> 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 ( <code>DIAGNOSTICS.AGENT</code> ).
%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.

## 26.5.3 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.

## 26.5.4 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.

## 26.6 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.

### 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 : <http://service.sap.com/swdc> .

## 27 Administration de la ligne de commande

### 27.1 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.

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.

#### i Remarque

Lors de la saisie de paramètres de la ligne de commande Unix, vous devrez peut-être ignorer des 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`.

### 27.1.1 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.

#### 27.1.1.1 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.

#### i Remarque

Les arguments entre crochets [ ] sont facultatifs.

### **i** 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`.

### **i** 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.

Table 137 :

Option CCM	Arguments valides	Description
<code>-help</code>	n/a	Afficher l'aide de la ligne de commande.
<code>-start</code>	tout ou <b>&lt;nomsia&gt;</b>	Démarrer chaque Server Intelligence Agent en tant que processus. L'option <code>tout</code> démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
<code>-stop</code>	tout ou <b>&lt;nomsia&gt;</b>	Arrête chaque Server Intelligence Agent en mettant fin à son ID de processus. L'option <code>tout</code> démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
<code>-restart</code>	tout ou <b>&lt;nomsia&gt;</b>	Arrêter chaque Server Intelligence Agent en mettant fin à son identification de processus ; chaque SIA est ensuite redémarré. L'option <code>tout</code> démarre tous les nœuds de l'ordinateur, y compris les nœuds appartenant à d'autres clusters.
<code>-managedstart</code>	<b>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</b>	Démarrer un serveur.
<code>-managedstop</code>	<b>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</b>	Arrêter un serveur.

Option CCM	Arguments valides	Description
-managedrestart	<code>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</code>	Arrêter un serveur, puis redémarrer le serveur.
-managedforceterminate	<code>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</code>	Arrête le serveur immédiatement sans terminer les requêtes en cours de traitement.
-enable	<code>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</code>	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	<code>&lt;nom complet du serveur&gt;&lt;[autres informations d'authentification]&gt;</code>	Désactiver un serveur pour qu'il cesse de répondre aux requêtes de la plateforme de BI, mais reste démarré en tant que processus. Utiliser la forme complète du nom de serveur.
-display	<code>&lt; [autres informations d'authentification]&gt;</code>	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.

Table 138 :

Option d'authentification	Arguments valides	Description
-cms	<code>&lt;nomcms : numéroport&gt;</code>	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>	<p>Spécifiez le mot de passe correspondant. Si aucun mot de passe n'est spécifié, un mot de passe vide est utilisé.</p> <div> <p><b>i Remarque</b></p> <p>Pour spécifier l'argument <code>-password</code>, vous devez également spécifier l'argument <code>-username</code>.</p> </div>

Le CCM lit les chaînes de démarrage et les autres valeurs de configuration à partir du fichier `ccm.config`.

## Informations associées

[ccm.config \[page 886\]](#)

### 27.1.1.1.1 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 Adaptive Job Server en cours d'exécution sur un deuxième ordinateur :

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

## 27.1.1.1.2 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 \[page 893\]](#)

## 27.1.1.2 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

### i 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 ». Veuillez également à consulter Mise en cluster de Central Management Servers dans le chapitre « Administration du serveur » du *Guide d'administration de la plateforme 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 \[page 379\]](#)

[Présentation de la sauvegarde et de la restauration \[page 487\]](#)

### 27.1.1.3 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 nœuds

#### 27.1.1.3.1 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 nœuds
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.

---

## 27.1.2 Modèles de scripts

### 27.1.2.1 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 \[page 882\]](#).

### 27.1.2.2 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 \[page 882\]](#).

## 27.1.3 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.

### **bojrestart.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.

## 27.2 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.

### 27.2.1 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.

#### i 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.

#### i Remarque

Les arguments entre crochets [ ] sont facultatifs.

#### i Remarque

Les arguments identifiés par `<autres informations d'authentification>` sont présentés dans le deuxième tableau.

Table 139 :

Option CCM	Arguments valides	Description
<code>-help</code>	n/a	Afficher l'aide de la ligne de commande.
<code>-managedstart</code>	<code>all</code> ou <code>&lt;nom complet du serveur&gt; [&lt;autres informations d'authentification&gt;]</code>	Démarrer un serveur.

Option CCM	Arguments valides	Description
-managedstop	all ou <nom complet du serveur> <[autres informations d'authentification]>	Arrêter un serveur.
-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]>.

#### **i** Remarque

Vous devez toujours fournir les références de connexion d'un compte avec l'authentification Enterprise.

Table 140 :

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.
-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.  <div> <i>i</i> <b>Remarque</b>            Pour spécifier l'argument <code>-password</code>, vous devez également spécifier l'argument <code>-username</code>.         </div>
-authentication	<type d'authentification>	Spécifiez le type d'authentification. Seul <b>secEnterprise</b> est pris en charge.

Le CCM lit les chaînes de démarrage et les autres valeurs de configuration à partir du fichier `ccm.config`.

## 27.2.1.1 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 (NOMNEUD) "`

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 Adaptive Job Server en cours d'exécution sur un deuxième ordinateur :

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

## 27.3 Lignes de commande des serveurs

### 27.3.1 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.

#### **i** 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.

#### 27.3.1.1 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.

## 27.3.2 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.

Table 141 :

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.  <b>i Remarque</b> 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 <i>Guide d'administration de la plateforme de BI</i> .
-loggingPath	<chemin d'accès absolu>	Spécifie le chemin où les fichiers journaux sont créés.

### 27.3.2.1 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).

### 27.3.3 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\_cmd.

Table 142 :

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.
-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.

Option	Arguments valides	Comportement
-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.
-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 \[page 894\]](#)

### 27.3.4 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.

Table 143 :

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 \[page 894\]](#)

## 27.3.5 Serveur de traitement Dashboards et Dashboards Cache Server

Le serveur de traitement Dashboards et le Dashboards 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 :

- <REPINSTALL>\SAP BusinessObjects\BI platform 4.0\win64\_x64\xccache.exe
- <REPINSTALL>\SAP BusinessObjects\BI platform 4.0\win64\_x64\xcproc.exe.

Les chemins par défaut des serveurs sous UNIX sont :

- <REPINSTALL>/sap\_bobj/enterprise\_xi40/<plateforme>\_64/boe\_xccached
- <REPINSTALL>/sap\_bobj/enterprise\_xi40/<plateforme>\_64/xcprocd

Table 144 :

Option	Arguments valides	Comportement
-cache		Active la fonctionnalité Cache Server.
-dir	<cheminabsolu>	Spécifie le répertoire de la mémoire cache d'un Cache Server et le répertoire temporaire du serveur de traitement. Les répertoires créés sont absolutepath/cache et absolutepath/temp

Option	Arguments valides	Comportement
-deleteCache		Supprime le répertoire de la mémoire cache à chaque démarrage et arrêt du serveur.
-psdir	<cheminabsolu>	Spécifie le répertoire temporaire du serveur de traitement. Cette option annule l'option -dir.
-refresh	<minutes>	Partage les pages en mémoire cache pour le nombre de minutes spécifié.
-auditMaxEventsPerFile	<nombre>	Dans le Cache Server, indique le nombre maximal d'actions d'audit enregistrées dans le fichier journal d'audit. La valeur par défaut est 500. Si ce nombre maximal d'enregistrements est dépassé, le serveur ouvrira un nouveau fichier journal.

## Informations associées

[Options standard communes à tous les serveurs \[page 894\]](#)

### 27.3.6 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/<PLATFORME>/boe\_jobsd.

Table 145 :

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.

Option	Arguments valides	Comportement
-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.  <b>i Remarque</b> 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 <i>Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence</i> .

## Informations associées

[Options standard communes à tous les serveurs \[page 894\]](#)

## 27.3.7 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.

## 27.3.8 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.

Table 146 :

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 <i>Guide d'administration de la plateforme SAP BusinessObjects de Business Intelligence</i> .



Option	Arguments valides	Comportement
-ProcessAffinityMask	<masque>	<p>Utilise un masque pour spécifier exactement les processeurs centraux que le RAS doit utiliser lorsqu'il s'exécute sur un ordinateur multiprocesseur.</p> <p>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).</p> <p>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 deuxième et troisième processeurs, recourez au masque 0x0110.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div> <div> <p><b>i Remarque</b></p> <p>La valeur par défaut du masque est -1, ce qui a la même signification que 0x1111.</p> </div>

## Informations associées

[Options standard communes à tous les serveurs \[page 894\]](#)

## 27.3.9 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`.

Table 147 :

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 \[page 894\]](#)

### 27.3.10 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.

Table 148 :

Option	Arguments valides	Comportement
<code>-rootDir</code>	<code>&lt;cheminabsolu&gt;</code>	<p>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.</p> <div><p><b>i Remarque</b></p><p>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.</p></div>

Option	Arguments valides	Comportement
-tempDir	<cheminabsolu>	<p>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).</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>
-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.

## Informations associées

[Options standard communes à tous les serveurs \[page 894\]](#)

### 27.3.11 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.

Table 149 :

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 \[page 894\]](#)

## 28 Repository Diagnostic Tool

### 28.1 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 deux 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.

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.

### 28.2 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 de 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.

## 28.2.1 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/<plateforme>/boe_reposcan.sh <arguments> où  
<plateforme> désigne soit « linux_x64 », soit « solaris_sparcv9 », soit « 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 être 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.

#### **i** 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/enterprisexi_40/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 \[page 915\]](#)

[Incohérences entre le CMS et le FRS \[page 914\]](#)

## 28.2.2 Paramètres de l'outil de diagnostic de référentiel

Le RDT (Repository Diagnostic Tool, outil de diagnostic de référentiel) accepte les paramètres figurant dans le tableau suivant :

#### **i** Remarque



Les arguments de ligne de commande remplacent toutes les entrées du fichier de paramètres lors de l'exécution.



Table 150 : Paramètres généraux

Paramètre	Facultatif ou Obligatoire	Description
dbdriver	Obligatoire	<p>Type de pilote utilisé pour la connexion à la base de données du CMS. Les valeurs acceptées sont les suivantes :</p> <ul style="list-style-type: none"> <li>• db2databasesubsystem</li> <li>• maxdbdatabasesubsystem</li> <li>• mysqldatabasesubsystem</li> <li>• oracledatabasesubsystem</li> <li>• sqlserverdatabasesubsystem</li> <li>• sybasedatabasesubsystem</li> <li>• sqlanywheredatabasesubsystem</li> </ul>
connect	Obligatoire	<p>Détails de connexion utilisés pour la connexion à la base de données du CMS.</p> <p>Par exemple : -connect  "UID=root;PWD=&lt;mot_de_passe&gt;;DSN=&lt;dsn&gt;;HOST  NAME=&lt;nom_hôte&gt;;PORT=&lt;numéro_de_port&gt;"</p>

Paramètre	Facultatif ou Obligatoire	Description
dbkey	Obligatoire	<p>Saisissez la clé de cluster de votre déploiement de la plateforme de BI.</p> <p>Si vous ne connaissez pas la clé de cluster, réinitialisez-la en suivant ces étapes :</p> <div> <p><b>i Remarque</b></p> <p>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.</p> <ol style="list-style-type: none"> <li>1. Lancez le Central Configuration Manager (CCM).</li> <li>2. Dans le CCM, cliquez avec le bouton droit de la souris sur le Server Intelligence Agent (SIA) et sélectionnez <i>Arrêter</i>. Ne passez à l'étape 3 que lorsque le statut du SIA est « Arrêté ».</li> <li>3. Cliquez avec le bouton droit sur le SIA et choisissez <i>Propriétés</i>.</li> <li>4. Dans l'onglet Configuration, cliquez sur <i>Modifier</i> en regard de l'option <i>Configuration de clé de cluster</i>.</li> <li>5. Un message d'avertissement s'affiche. Cliquez sur Oui pour continuer.</li> <li>6. Dans la boîte de dialogue <i>Modifier la clé de cluster</i>, saisissez la même clé à huit caractères dans les champs <i>Nouvelle clé de cluster</i> et <i>Confirmer la nouvelle clé de cluster</i>.</li> </ol> <p><b>i Remarque</b></p> <p>Le RDT ne s'exécute pas si le paramètre dbkey est omis ou si la clé de cluster est erronée.</p> <p><b>i Remarque</b></p> <p>La clé de cluster affichée dans le CCM est cryptée et ne peut pas être utilisée dans le paramètre dbkey.</p> <p>Pour en savoir plus sur les clés de cluster, voir « Sécurisation de la plateforme de BI » dans le <i>Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence</i>.</p> </div>
inputfrsdir	Obligatoire	<p>Chemin d'accès au fichier du Input File Repository Server.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>

Paramètre	Facultatif ou Obligatoire	Description
outputfrsdir	Obligatoire	<p>Chemin d'accès au fichier du Output File Repository Server.</p> <div>  <b>Remarque</b>  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. </div>
outputdir	Facultatif	<p>Chemin d'accès au fichier où le RDT enregistre les fichiers journaux.</p> <p>Par défaut, il s'agit de &lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\reposcan sous Windows et ./sap_bobj/enterprisexi_40/reposcan sous Unix.</p>
count	Facultatif	<p>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.</p> <p>La valeur par défaut est 0.</p>
repair	Facultatif	<p>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.</p> <div>  <b>Attention</b>  Ce processus supprimera tous les objets ou fichiers orphelins de la base de données du référentiel. </div>
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	<p>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.</p> <p>Ce paramètre n'est utilisé que lorsque le RDT fonctionne en mode réparation.</p>

Paramètre	Facultatif ou Obligatoire	Description
startid	Facultatif	<p>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 – <b>startid=501</b> pour démarrer l'analyse au 501e objet.</p> <p>La valeur par défaut est <b>1</b>.</p>
optionsfile	Facultatif	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>
syscopy	Facultatif	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>Veillez à ne pas exécuter le RDT avec le paramètre <code>syscopy</code> sur votre système source.</p> </div>
trace	Facultatif	<p>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 :</p> <p>&lt;RÉP_INST_SAP_BOBJ&gt;\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging</p>

Les paramètres suivants sont utilisés si l'outil de diagnostic du référentiel est exécuté sur un CMS mis en cluster actif.

Table 151 : 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 <b>True</b> et <b>False</b> .  La valeur par défaut est <b>False</b> (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 <b>12</b> .

Les paramètres suivants sont utilisés lorsque le RDT utilise l'authentification SSL pour communiquer avec la base de données de CMS analysée.

Table 152 : 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 <b>ssl</b> .
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=<Mot de
passel>;DSN=<monDsn>;HOSTNAME=<monNomd'Hôte>;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 <clé de cluster>
-repair
```

## Exemple

Exemple Unix :

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Mot de passel>;DSN=<monDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <clé de cluster>
```

## 28.3 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.

Message d'avertissement	Incohérence	Suggestion	Action
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.

## 28.4 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.

Message d'avertissement	Incohérence	Suggestion	Action
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.  <ul style="list-style-type: none"> <li>• 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 ».</li> <li>• 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. »</li> </ul>	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.
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	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.



Message d'avertissement	Incohérence	Suggestion	Action
(ID d'objet d'événement = <ID>).			
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 événements 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.
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	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.

Message d'avertissement	Incohérence	Suggestion	Action
d'objet> (ID d'objet = <ID>) est manquant (ID d'objet de groupe de serveurs = <ID>).			
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.

## 29 Annexe relative aux droits

### 29.1 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*.

### 29.2 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
<i>Visualiser les objets</i>	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.
<i>Ajouter les objets au dossier</i>	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 <i>Favoris</i> ou les lots d'objets.
<i>Modifier les objets</i>	Permet de modifier le contenu d'un objet mais également les propriétés des objets et des dossiers.
<i>Modifier les droits des utilisateurs sur les objets</i>	Permet de modifier les paramètres de sécurité d'un objet.

Droit	Description
<i>Modifier en toute sécurité les droits des utilisateurs sur les objets</i>	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 <i>Guide d'administration de la plateforme SAP BusinessObjects Business Intelligence</i> .
<i>Définir les groupes de serveurs pour traiter les tâches</i>	<p>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.</p> <p>Pour spécifier un groupe de serveurs, vous avez également besoin du droit <i>Modifier les objets</i> sur l'objet.</p>
<i>Supprimer les objets</i>	Permet de supprimer les objets ainsi que leurs instances.
<i>Copier les objets dans un autre dossier</i>	<p>Permet de créer des copies des objets dans d'autres dossiers du CMS. Pour ce faire, vous avez également besoin du droit <i>Ajouter les objets au dossier</i> sur le dossier de destination.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>
<i>Répliquer le contenu</i>	Permet de répliquer les objets sur un autre système d'une fédération.
<i>Planifier l'exécution du document</i>	Permet de planifier les objets.
<i>Planifier de la part d'autres utilisateurs</i>	<p>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.</p> <p>Pour planifier un objet pour d'autres utilisateurs ou groupes, vous avez également besoin des droits suivants :</p> <ul style="list-style-type: none"> <li>• Ce droit sur l'utilisateur ou le groupe.</li> <li>• Droit <i>Planifier l'exécution du document</i> sur l'objet.</li> </ul>
<i>Planifier vers des destinations</i>	<p>Permet d'effectuer les opérations suivantes :</p> <ul style="list-style-type: none"> <li>• Planifier des objets vers des destinations autres que l'emplacement d'Enterprise par défaut.</li> <li>• Modifier les destinations par défaut spécifiées pour la planification.</li> </ul> <p>Pour planifier l'objet vers des destinations, vous avez également besoin des droits suivants :</p>

Droit	Description
	<ul style="list-style-type: none"> <li>• Droit <i>Planifier l'exécution du document</i> sur l'objet à planifier.</li> <li>• Droit <i>Ajouter les objets au dossier</i> sur la boîte de réception du destinataire (si vous souhaitez planifier vers une boîte de réception).</li> <li>• Droit <i>Copier les objets dans un autre dossier</i> sur l'objet à planifier (si vous souhaitez envoyer une copie vers une boîte de réception à la place d'un raccourci).</li> </ul>
<i>Afficher les instances du document</i>	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.
<i>Supprimer les instances</i>	Permet de supprimer uniquement les instances des objets. Si vous disposez du droit <i>Supprimer les objets</i> , vous n'avez pas besoin de ce droit pour supprimer les instances.
<i>Suspendre et reprendre les instances du document</i>	Permet de suspendre et de reprendre les instances de l'objet en cours d'exécution.
<i>Replanifier les instances</i>	Permet de replanifier les instances de l'objet.

## 29.3 Droits sur les types d'objet spécifiques

### 29.3.1 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).

### 29.3.2 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
<a href="#">Ajouter les objets au dossier</a>	Permet de créer des catégories à l'intérieur des catégories existantes. Ce droit n'est pas nécessaire pour ajouter des objets à une catégorie.
<a href="#">Modifier les objets</a>	<p>Permet d'effectuer les opérations suivantes :</p> <ul style="list-style-type: none"> <li>• Modifier les propriétés de la catégorie.</li> <li>• Déplacer la catégorie dans une autre catégorie, la première catégorie devenant ainsi sous-catégorie.</li> <li>• Ajouter des objets à la catégorie.</li> <li>• Supprimer des objets de la catégorie.</li> </ul> <p>Pour déplacer une catégorie dans une autre catégorie en tant que sous-catégorie, vous avez également besoin des droits suivants :</p> <ul style="list-style-type: none"> <li>• Droit <a href="#">Supprimer les objets</a> sur la catégorie d'origine.</li> <li>• Droit <a href="#">Ajouter les objets au dossier</a> sur la catégorie de destination.</li> </ul>
<a href="#">Supprimer les objets</a>	Permet de supprimer la catégorie.

### 29.3.3 Documents Desktop Intelligence

Les droits mentionnés dans cette section s'appliquent uniquement aux documents Desktop Intelligence.

Droit	Description
<a href="#">Utiliser la liste de valeurs</a>	Permet à l'utilisateur d'utiliser des listes de valeurs.
<a href="#">Télécharger les fichiers associés à l'objet</a>	Permet à l'utilisateur de télécharger le fichier associé à l'objet.
<a href="#">Exporter les données du rapport</a>	Permet à l'utilisateur d'exporter les données du document en formats Excel, PDF et CSV. Si vous ne disposez pas de ce droit, vous devez disposer du droit <a href="#">Enregistrer au format CSV</a> , <a href="#">Enregistrer au format Excel</a> ou <a href="#">Enregistrer au format PDF</a> ; ces droits permettent d'exporter des documents au format spécifié uniquement.
<a href="#">Visualiser le SQL</a>	Permet à l'utilisateur de voir le SQL généré pour la requête.
<a href="#">Actualiser les données du rapport</a>	Permet à l'utilisateur d'actualiser les données du document.
<a href="#">Actualiser la liste des valeurs</a>	Permet à l'utilisateur 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 <a href="#">Utiliser la liste des valeurs</a> sur le document.

Droits des documents spécifiques à PDF, XLS, Rich text, Text :

Droit	Description
<i>Ajouter les objets au dossier</i>	Permet aux utilisateurs d'ajouter des objets à un dossier. Ce droit s'applique également aux objets se comportant comme des dossiers tels que les boîtes de réception, les dossiers Favoris ou les lots d'objets.
<i>Copier les objets dans un autre dossier</i>	Permet aux utilisateurs de créer des copies d'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.
<i>Supprimer les instances</i>	Permet à l'utilisateur de supprimer les instances d'objet uniquement. Si vous disposez du droit "Supprimer les objets", vous n'avez pas besoin de ce droit pour supprimer les instances.
<i>Supprimer les objets</i>	Permet à l'utilisateur de supprimer cette catégorie.
<i>Modifier les objets</i>	Permet à l'utilisateur de modifier les propriétés d'une catégorie, de déplacer la catégorie dans une autre catégorie en tant que sous-catégorie, d'ajouter des objets à une catégorie et de supprimer les objets d'une catégorie.
<i>Modifier les droits des utilisateurs sur les objets</i>	Permet à l'utilisateur de modifier tous les droits sur cet objet, pour tout utilisateur.
<i>Suspendre et reprendre les instances du document</i>	Permet à l'utilisateur de suspendre ou de reprendre les instances de l'objet en cours d'exécution.
<i>Répliquer le contenu</i>	Permet à l'utilisateur de répliquer les objets dans un autre système lors d'un déploiement fédéré.
<i>Replanifier les instances</i>	Permet à l'utilisateur de replanifier les instances de l'objet.
<i>Modifier en toute sécurité les droits des utilisateurs sur les objets</i>	Permet à l'utilisateur d'accorder, de refuser ou d'annuler uniquement les droits dont il dispose.
<i>Afficher les instances du document</i>	Permet à l'utilisateur 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.
<i>Visualiser les objets</i>	Permet à l'utilisateur d'afficher la catégorie et les sous-catégories qu'elle contient.

## 29.3.4 Remarques

Les notes permettent aux utilisateurs d'effectuer des commentaires sur d'autres objets à l'aide de l'application Discussions. Les notes sont liées entre elles dans des threads de discussion ; ces threads sont considérés comme

des objets enfant des objets concernés par les discussions. Vous pouvez définir des droits au niveau des objets ou des dossiers pour contrôler l'utilisation des threads de discussion.

Les droits mentionnés dans cette section s'appliquent uniquement aux notes.

Droit	Description
Permet les threads de discussion	Ce droit permet d'effectuer les opérations suivantes : <ul style="list-style-type: none"><li>• Lancer des threads de discussion et y répondre.</li><li>• Visualiser les notes d'un thread de discussion.</li><li>• Modifier ou supprimer les notes que vous avez publiées.</li></ul>

## 29.3.5 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
<a href="#">Imprimer les données du rapport</a>	Permet d'imprimer le rapport.
<a href="#">Actualiser les données du rapport</a>	Permet d'actualiser les données du rapport.
<a href="#">Exporter les données du rapport</a>	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 <a href="#">Télécharger les fichiers associés à l'objet</a> .
<a href="#">Télécharger les fichiers associés à l'objet</a>	Ce droit permet d'effectuer les opérations suivantes : <ul style="list-style-type: none"><li>• Exporter le rapport au format RPT.</li><li>• Ouvrir le rapport dans Crystal Reports Designer.</li><li>• Planifier le rapport au format RPT vers des destinations externes.</li></ul>

## 29.3.6 Documents Web Intelligence

Les droits présentés dans cette section s'appliquent uniquement aux documents Web Intelligence.



Droit	Description
<i>Utiliser la liste de valeurs</i>	Permet d'utiliser les listes de valeurs.
<i>Exporter les données du rapport</i>	Permet d'exporter les données du document vers les formats XLS, PDF et CSV. Si vous ne disposez pas de ce droit, vous devez disposer du droit <i>Enregistrer au format CSV</i> , <i>Enregistrer au format Excel</i> ou <i>Enregistrer au format PDF</i> ; ces droits permettent d'exporter des documents au format spécifié uniquement.
<i>Script de requête : activer la visualisation (SQL, MDX...)</i>	Permet de visualiser les scripts de requêtes (SQL et MDX).
<i>Script de requête : activer la modification (SQL, MDX, etc.)</i>	Permet de modifier les scripts de requêtes (SQL et MDX). Vous pouvez également modifier les sources de données FHSQL (SQL à la carte)
<i>Actualiser les données du rapport</i>	Permet d'actualiser les données du document.
<i>Modifier la requête</i>	Permet de modifier les requêtes dans le document.
<i>Actualiser la liste des valeurs</i>	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 <i>Utiliser la liste des valeurs</i> sur le document.
<i>Enregistrer au format CSV</i>	Permet d'exporter des documents au format CSV uniquement. Si vous disposez déjà du droit <i>Exporter les données du rapport</i> sur un document, vous n'avez pas besoin de ce droit.
<i>Enregistrer au format Excel</i>	Permet d'exporter des documents au format Excel uniquement. Si vous disposez déjà du droit <i>Exporter les données du rapport</i> sur un document, vous n'avez pas besoin de ce droit.
<i>Enregistrer au format PDF</i>	Permet d'exporter des documents au format PDF uniquement. Si vous disposez déjà du droit <i>Exporter les données du rapport</i> sur un document, vous n'avez pas besoin de ce droit.
<i>Envoyer à</i>	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.

## 29.3.7 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, l'utilisateur pour lequel le compte est destiné est également considéré comme propriétaire du compte.

Droit	Description
<a href="#">Modifier les objets</a>	<p>Permet d'effectuer les opérations suivantes :</p> <ul style="list-style-type: none"><li>• Modifier les propriétés de l'utilisateur ou du groupe.</li><li>• Gérer l'appartenance au groupe.</li></ul> <p>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.</p>
<a href="#">Changer le mot de passe utilisateur</a>	<p>Permet d'effectuer les opérations suivantes :</p> <ul style="list-style-type: none"><li>• Modifier le mot de passe de votre compte utilisateur. Pour ce faire, vous devez également disposer du droit <a href="#">Modifier les objets</a> sur le compte utilisateur.</li><li>• Modifier le mot de passe du compte d'un autre utilisateur. Pour ce faire, vous devez également disposer des droits <a href="#">Modifier les objets</a> et <a href="#">Modifier les droits des utilisateurs sur les objets</a> sur le compte utilisateur.</li></ul> <div> <b>Remarque</b><p>Ce droit n'affecte pas les paramètres de mot de passe utilisateur suivants :</p><ul style="list-style-type: none"><li><a href="#">Le mot de passe n'expire jamais</a></li><li><a href="#">L'utilisateur doit modifier le mot de passe à la prochaine session</a></li><li><a href="#">L'utilisateur ne peut pas modifier le mot de passe</a></li></ul></div> <div> <b>Remarque</b><p>Ce droit ne s'applique pas aux références des données source des univers SAP BusinessObjects.</p></div>

Droit	Description
<i>S'abonner aux publications</i>	Permet d'ajouter l'utilisateur aux publications en tant que destinataire.
<i>Planifier de la part d'autres utilisateurs</i>	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 <i>Planifier de la part d'autres utilisateurs</i> sur l'objet.
<i>Ajouter des attributs utilisateur ou les modifier</i>	Permet de modifier la valeur de l'adresse électronique d'un utilisateur ou de personnaliser les attributs utilisateur. Ce droit est applicable aux utilisateurs.
<i>Ajouter des attributs utilisateur ou les modifier (droit du propriétaire)</i>	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.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	Affiche le menu <i>Préférences</i> 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.

## 29.3.8 Niveaux d'accès

Les droits mentionnés dans cette section s'appliquent uniquement aux niveaux d'accès.



Droit	Description
<i>Utiliser le niveau d'accès pour l'affectation de la sécurité</i>	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 <i>Modifier les droits des utilisateurs sur les objets</i> ou <i>Modifier en toute sécurité les droits des utilisateurs sur les objets</i> sur l'utilisateur ou le groupe principal et sur l'objet. Pour les cas où le droit <i>Modifier en toute sécurité les droits des utilisateurs sur les objets</i> est affecté, vous devez également disposer du même niveau d'accès sur l'objet.

## 29.3.9 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
<a href="#">Ajouter les objets au dossier</a>	Permet d'ajouter des ensembles de restrictions ou des objets à l'univers. Pour ce faire, vous devez également disposer du droit <a href="#">Modifier les restrictions d'accès</a> .
<a href="#">Visualiser les objets</a>	Permet d'accéder à l'univers et de le visualiser.
<a href="#">Modifier les objets</a>	Ce droit permet d'effectuer les opérations suivantes : <ul style="list-style-type: none"><li>• Modifier l'univers dans la CMC ou dans l'outil de conception d'univers.</li><li>• Verrouiller ou déverrouiller l'univers.</li></ul> Pour déverrouiller un univers, vous devez également disposer du droit <a href="#">Déverrouiller l'univers</a> .
<a href="#">Supprimer les objets</a>	Permet de supprimer l'univers.
<a href="#">Traduire les objets</a>	Permet de sauvegarder les noms d'objets d'univers traduits à l'aide de l'outil de gestion de la traduction. <div> <b>Remarque</b><p>Vous pouvez aussi sauvegarder des traductions si vous disposez explicitement du droit <a href="#">Modifier les objets</a> et que le droit <a href="#">Traduire les objets</a> ne vous a pas été explicitement refusé.</p></div>
<a href="#">Nouvelle liste de valeurs</a>	Ce droit permet d'effectuer les opérations suivantes : <ul style="list-style-type: none"><li>• Associer de nouvelles listes de valeurs à des objets.</li><li>• Modifier des listes de valeurs existantes.</li></ul> <div> <b>Remarque</b><p>Ce droit n'empêche pas de créer des listes de valeurs en cascade.</p></div>
<a href="#">Imprimer l'univers</a>	Permet d'imprimer l'univers.

Droit	Description
<i>Afficher les valeurs de table ou d'objet</i>	Permet d'afficher les valeurs associées aux tables ou aux objets de l'univers.
<i>Modifier les restrictions d'accès</i>	Permet de modifier les restrictions d'accès (surcharges) de l'univers.
<i>Déverrouiller l'univers</i>	<p>Permet d'effectuer les opérations suivantes :</p> <ul style="list-style-type: none"> <li>• Déverrouiller l'univers s'il a été verrouillé par un autre utilisateur.</li> <li>• Exporter l'univers à partir du CMS.</li> </ul> <p>Pour déverrouiller un univers, vous devez également disposer du droit <i>Modifier les objets</i>.</p>
<i>Accès aux données</i>	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.
<i>Créer et modifier des requêtes se basant sur un univers</i>	Permet de créer des documents et de modifier des requêtes basées sur l'univers.

## 29.3.10 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
<i>Visualiser les objets</i>	Permet d'accéder à l'univers et de le visualiser.
<i>Modifier les objets</i>	Permet de republier l'univers.
<i>Supprimer les objets</i>	Permet de supprimer l'univers.
<i>Extraire l'univers</i>	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.

Droit	Description
	<p><b>i Remarque</b></p> <p>Vous devez également disposer du droit <a href="#">Extraire l'univers</a> de l'application Outil de conception d'information.</p>
<a href="#">Modifier les profils de sécurité</a>	<p>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.</p> <p><b>i Remarque</b></p> <p>Ce droit n'est pas requis pour afficher les profils de sécurité ou modifier les options d'agrégation de profils de sécurité.</p>
<a href="#">Affecter des profils de sécurité</a>	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.
<a href="#">Accès aux données</a>	<p>Permet d'extraire les données de l'univers et d'actualiser les documents en fonction de l'univers.</p> <p>Dans l'outil de conception d'information, ce droit permet d'afficher un aperçu de l'ensemble de résultats dans l'Editeur de requête.</p>
<a href="#">Créer et modifier des requêtes se basant sur cet univers</a>	<p>Permet de créer et de modifier des requêtes basées sur un univers.</p> <p>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.</p>
<a href="#">Enregistrer pour tous les utilisateurs</a>	<p>Permet d'enregistrer l'univers pour tous les utilisateurs.</p> <p><b>i Remarque</b></p> <p>Vous devez également disposer du droit Enregistrer pour tous les utilisateurs de l'application <a href="#">Outil de conception d'information</a>.</p>

## 29.3.11 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 \[page 931\]](#)

### 29.3.11.1 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](#).

## 29.3.12 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
<i>Visualiser les objets</i>	Permet de visualiser la connexion.
<i>Modifier les objets</i>	Permet de modifier les paramètres de connexion.
<i>Télécharger la connexion localement</i>	<p>Permet d'utiliser des univers créés sur la connexion dans Web Intelligence Rich Client en mode hors ligne.</p> <p>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.</p> <p>Ce droit est également nécessaire pour modifier une connexion sécurisée dans l'outil de conception d'information.</p>
<i>Supprimer les objets</i>	Permet de supprimer la connexion.
<i>Copier les objets dans un autre dossier</i>	Permet de copier la connexion d'un dossier dans un autre.
<i>Accès aux données</i>	<p>Permet d'extraire du contenu de la base de données spécifiée dans la connexion.</p> <p>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 de l'Editeur de requête.</p>
<i>Utiliser la connexion pour les procédures stockées</i>	<p>Permet d'utiliser les procédures stockées dans la base de données spécifiée pour la connexion à l'univers.</p> <div><p><b>i Remarque</b></p><p>Ce droit s'applique aux univers .unv uniquement.</p></div>



## Droits de connexion OLAP

Droit	Description
<i>Visualiser les objets</i>	Permet de visualiser la connexion.
<i>Modifier les objets</i>	Permet de modifier les paramètres de connexion dans l'éditeur de connexion de l'outil de conception d'information.
<i>Supprimer les objets</i>	Permet de supprimer la connexion.
<i>Copier les objets dans un autre dossier</i>	Permet de copier la connexion d'un dossier dans un autre.

## 29.3.13 Applications

### 29.3.13.1 CMC

Droit	Description
<i>Se connecter à la CMC pour accéder à cet objet dans la CMC</i>	Permet à un utilisateur de se connecter à la CMC.
<i>Autoriser l'accès au Gestionnaire d'instances</i>	Permet à un utilisateur d'accéder au Gestionnaire d'instances.
<i>Autoriser l'accès à la requête de relation</i>	Permet à un utilisateur d'exécuter des requêtes de relation dans la CMC.
<i>Autoriser l'accès à la requête de sécurité</i>	Permet à un utilisateur d'exécuter des requêtes de sécurité dans la CMC.

### 29.3.13.2 Zone de lancement BI

Droit	Description
<i>Organiser</i>	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.
<i>Envoyer vers la boîte de réception Business Objects</i>	Permet à un utilisateur d'envoyer des objets dans les boîtes de réception BI destinataires.
<i>Envoyer vers la destination du courrier électronique</i>	Permet à un utilisateur d'envoyer des objets aux destinataires par courrier électronique.

Droit	Description
<i>Envoyer vers l'emplacement de fichier</i>	Permet à un utilisateur d'envoyer des objets vers un emplacement de fichier.
<i>Envoyer vers l'emplacement FTP</i>	Permet à un utilisateur d'envoyer des objets vers un emplacement FTP.
<i>Envoyer vers l'emplacement SFTP</i>	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.
<i>Envoyer vers StreamWork</i>	Permet à un utilisateur d'envoyer des objets vers StreamWork.

## 29.3.13.2.1 Droits pour les applications de collaboration

Ces droits d'accès s'appliquent à SAP Jam ou à SAP StreamWork lorsque l'application est configurée dans la plateforme de BI.

Droit	Description
<i>Commenter les documents possédés par l'utilisateur</i>	Permet à un utilisateur d'ajouter des commentaires pour des documents et des instances qu'il possède.
<i>Afficher les commentaires sur les documents possédés par l'utilisateur</i>	Permet à un utilisateur d'afficher des commentaires pour des documents et des instances qu'il possède.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	Affiche le menu <i>Préférences</i> 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 <i>Préférences</i> 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.

### 29.3.13.3 Espaces de travail BI

Droit	Description
<i>Créer et modifier des espaces de travail BI</i>	Permet à un utilisateur de créer des espaces de travail BI et de modifier des espaces de travail BI existants.
<i>Créer et modifier des modules</i>	Permet à un utilisateur de créer des modules et de modifier des modules existants.
<i>Modifier les espaces de travail BI</i>	Permet à un utilisateur de modifier les espaces de travail BI existants (mais ne lui permet pas de créer des espaces de travail).
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

### 29.3.13.4 Desktop Intelligence

Droit	Description
<i>Créer et modifier des connexions</i>	Permet aux utilisateurs de créer une nouvelle connexion ou de modifier une connexion existante.
<i>Gestion des fournisseurs de données</i>	Permet aux utilisateurs de modifier une requête ou de changer l'univers sur lequel elle est basée.
<i>Modifier le SQL à la carte</i>	Lorsqu'un utilisateur dispose du droit <i>Utiliser le SQL à la carte</i> , lui permet de modifier une requête utilisant des scripts SQL à la carte comme fournisseur de données.
<i>Utiliser le SQL à la carte</i>	Permet aux utilisateurs de créer une requête à l'aide des scripts SQL à la carte comme fournisseur de données.
<i>Actualiser la liste de documents et les catégories</i>	Permet à un utilisateur d'actualiser la liste de documents.
<i>Envoyer des documents au référentiel</i>	Permet à un utilisateur de publier un document dans le CMS dans le dossier <i>Public</i> ou les dossiers <i>Personnels</i> .

Droit	Description
<i>Envoyer des documents à une messagerie</i>	Permet à un utilisateur d'envoyer des documents joints à un e-mail, à partir de l'application Desktop Intelligence.
<i>Extraire des documents</i>	Permet à un utilisateur d'importer un document à partir du CMS.
<i>Exécuter le code VBA</i>	Permet à un utilisateur d'exécuter du code VBA.
<i>Installer des macros complémentaires</i>	Permet aux utilisateurs d'installer ou de désinstaller les macros complémentaires VBA.
<i>Gérer toutes les catégories d'entreprise</i>	Permet aux utilisateurs de créer, de modifier ou de supprimer tout document de la catégorie.
<i>Gérer mes catégories d'entreprise</i>	Permet à un utilisateur de créer, de modifier et de supprimer les catégories d'entreprise de l'application Desktop Intelligence.
<i>Modifier le périmètre d'analyse</i>	Permet à un utilisateur de modifier le périmètre d'analyse.
<i>Travailler en mode Exploration</i>	Permet à un utilisateur d'explorer des détails de rapports.
<i>Utiliser le mode Rotation</i>	Permet à un utilisateur d'utiliser le panneau Rotation.
<i>Modifier le code VBA</i>	Permet à un utilisateur de modifier des macros VBA dans des rapports.
<i>Convertisseur en euros</i>	Permet à un utilisateur de convertir les devises des rapports vers et depuis l'Euro.
<i>Copier dans le presse-papiers</i>	Permet à un utilisateur de couper et copier le contenu du document.
<i>Explorer en détail</i>	Permet aux utilisateurs d'explorer plus en détail un rapport en extrayant de nouvelles données.
<i>Modifier le taux de conversion en euros</i>	Permet aux utilisateurs de modifier les taux de conversion en euros utilisés par la fonction Convertisseur en euros.
<i>Interaction entre les rapports Desktop Intelligence</i>	Permet à un utilisateur de couper, de copier, de réinitialiser, de dupliquer et de supprimer des éléments individuels d'un rapport.
<i>Interaction entre les documents Desktop Intelligence</i>	Permet aux utilisateurs de renommer, de dupliquer, d'insérer ou de supprimer un rapport dans un document.
<i>Imprimer des documents</i>	Permet à un utilisateur d'imprimer un document.
<i>Actualiser le contenu Desktop Intelligence</i>	Permet aux utilisateurs d'actualiser le contenu de Desktop Intelligence.

Droit	Description
<i>Utiliser des modèles</i>	Permet à un utilisateur de créer un rapport avec un modèle et d'appliquer un modèle à un contenu existant d'un rapport.
<i>Créer des modèles</i>	Permet à un utilisateur d'enregistrer un document comme modèle.
<i>Enregistrer les documents pour tous les utilisateurs</i>	Permet à un utilisateur d'enregistrer un document sans contraintes de sécurité pour une utilisation hors ligne, afin que tous les utilisateurs puissent afficher le document lorsqu'il est enregistré localement.
<i>Créer des documents Desktop Intelligence</i>	Permet à un utilisateur de créer un nouveau document.
<i>Enregistrer des documents Desktop Intelligence</i>	Permet à un utilisateur d'enregistrer un document localement.
<i>Envoyer des documents vers la boîte de réception</i>	Permet à un utilisateur d'envoyer un document à une boîte de réception de zone de lancement BI.
<i>Utiliser les objets personnels</i>	Permet à un utilisateur de créer, de modifier et de supprimer des objets personnels.
<i>Actualiser la liste des valeurs</i>	Permet à un utilisateur d'actualiser les listes de valeurs.
<i>Utiliser la liste de valeurs</i>	Permet à un utilisateur de se servir des listes de valeurs d'un document et de les actualiser.
<i>Modifier la liste de valeurs</i>	Permet aux utilisateurs de modifier les listes de valeurs définies dans un univers.
<i>Utiliser des requêtes</i>	Permet aux utilisateurs de créer de nouvelles requêtes basées sur un univers.
<i>Modifier des requêtes</i>	Permet aux utilisateurs de modifier des requêtes basées sur un univers.
<i>Visualiser le SQL</i>	Permet à un utilisateur de voir le SQL généré pour une requête.
<i>Modifier le SQL de la requête</i>	Permet à un utilisateur de modifier le SQL généré pour une requête.
<i>Toujours régénérer le SQL</i>	Permet de régénérer les requêtes à chaque actualisation.
<i>Utiliser les procédures stockées</i>	Permet à l'utilisateur de créer des rapports à l'aide d'une procédure stockée comme fournisseur de données.
<i>Modifier les procédures stockées</i>	Permet à un utilisateur de modifier des paramètres dans des procédures stockées.

Droit	Description
<i>Utiliser les fichiers de données personnelles</i>	Permet aux utilisateurs de créer un rapport à l'aide de fichiers texte ASCII, Excel ou dBase en tant que fournisseur de données.
<i>Modifier les fichiers de données personnelles</i>	Permet aux utilisateurs de modifier le fournisseur de données personnelles.
<i>Modifier en toute sécurité les droits des utilisateurs sur les objets</i>	Permet à un utilisateur d'accorder, de refuser et d'annuler des droits d'accès non spécifiés.
<i>Modifier les droits des utilisateurs sur cet objet</i>	Permet à un utilisateur de modifier les droits d'accès pour un utilisateur d'un objet spécifique.
<i>Modifier cet objet</i>	Permet à un utilisateur de modifier les propriétés de l'application dans la CMC.
<i>Se connecter à Desktop Intelligence et visualiser cet objet dans Desktop Intelligence de la CMC</i>	Permet aux utilisateurs de se connecter à Desktop Intelligence et d'afficher l'objet dans la CMC.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

## 29.3.13.5 Web Intelligence

Les droits d'accès présentés dans cette section s'appliquent à l'application Web Intelligence (y compris à l'interface Rich Client) et peuvent affecter les visualiseurs et les éditeurs de requêtes de l'application.

Droit	Description
<i>Données : activer le suivi des données</i>	Permet à un utilisateur d'effectuer le suivi des données modifiées.
<i>Données : activer la mise en forme des données modifiées</i>	Permet à un utilisateur de sélectionner la mise en forme des données modifiées.
<i>Desktop Interface : activer Web Intelligence Desktop</i>	Permet à un utilisateur de se servir de l'interface Web Intelligence Desktop.

Droit	Description
<i>Desktop Interface : exporter des documents</i>	Permet à un utilisateur d'exporter des documents dans le CMS de l'interface Web Intelligence Desktop.
<i>Desktop Interface : importer les documents</i>	Permet à un utilisateur d'importer des documents depuis le CMS de l'interface Web Intelligence Desktop.
<i>Desktop Interface : installer à partir de la zone de lancement BI</i>	Permet à un utilisateur de télécharger l'interface Web Intelligence Desktop depuis la zone de lancement de BI.
<i>Desktop Interface : imprimer les documents</i>	Permet à un utilisateur d'imprimer des documents à partir de l'interface Web Intelligence Desktop.
<i>Desktop Interface : supprimer la sécurité des documents</i>	Permet à un utilisateur de supprimer un document de l'interface Web Intelligence Desktop.
<i>Desktop Interface : enregistrer le document pour tous les utilisateurs</i>	Permet à un utilisateur d'enregistrer des documents pour tous les utilisateurs à partir de l'interface Web Intelligence Desktop.
<i>Desktop Interface : enregistrer les documents localement</i>	Permet à un utilisateur d'enregistrer des documents sur un disque local de l'interface Web Intelligence Desktop.
<i>Desktop Interface : envoyer par courrier électronique</i>	Permet à l'utilisateur d'envoyer un document dans un message électronique à partir de l'interface Web Intelligence Desktop.
<i>Desktop Interface : activer les fournisseurs de données locaux</i>	Permet à un utilisateur de se servir des fournisseurs de données personnelles dans l'interface Web Intelligence Desktop.
<i>Documents : désactiver l'actualisation automatique à l'ouverture</i>	Empêche l'actualisation automatique des documents lorsqu'ils sont ouverts.
<i>Documents : activer l'enregistrement automatique</i>	Permet d'enregistrer automatiquement les documents si l'enregistrement automatique est activé par l'administrateur dans la CMC.
<i>Documents : autoriser la création</i>	Permet à un utilisateur de créer de nouveaux documents.
<i>Documents - activer la publication et la gestion du contenu</i>	Permet à un utilisateur de publier un document dans le CMS.
<i>Interactif : Reporting - Créer et modifier les alerteurs</i>	Permet à un utilisateur de créer et de modifier des alertes dans le visualiseur interactif.
<i>Interfaces : activer Rich Internet Application</i>	<p>Permet à un utilisateur de se servir de l'interface de visualisation et de modification dans Rich Internet Application.</p> <p>Rich Internet Application s'appelait l'Editeur de rapport Java dans les versions précédentes.</p>

Droit	Description
<i>Interfaces : activer l'interface de visualisation Web</i>	Permet à un utilisateur de se servir de l'interface de visualisation Web.  L'interface de visualisation Web s'appelait le Visualiseur DHTML dans les versions précédentes.
<i>Interfaces : activer le volet de requête Web</i>	Permet à un utilisateur de se servir de l'Editeur de requête Web.  L'Editeur de requête Web s'appelait Requête - HTML dans les versions précédentes.
<i>Général - Modifier Mes préférences</i>	Permet à un utilisateur de modifier les préférences dans la zone de lancement BI.
<i>Général - activer les menus contextuels</i>	Permet à un utilisateur de se servir des menus contextuels.
<i>Volet gauche - Activer le résumé du document</i>	Permet à un utilisateur d'afficher le résumé du document dans le volet de gauche.
<i>Volet gauche - activer la structure et les filtres du document</i>	Permet à un utilisateur d'afficher la structure et les filtres du document dans le volet de gauche.
<i>Script de requête : activer la modification (SQL, MDX...)</i>	Permet à un utilisateur de modifier les scripts de requête SQL et MDX.
<i>Script de requête : activer la visualisation (SQL, MDX...)</i>	Permet à un utilisateur d'afficher les scripts de requête SQL et MDX.
<i>Reporting : créer des sauts de page et les modifier</i>	Permet à un utilisateur de créer et de modifier des sauts.
<i>Reporting : créer des règles de mise en forme conditionnelle et les modifier</i>	Permet à un utilisateur de créer et de modifier des règles de mise en forme conditionnelles.
<i>Reporting : créer des calculs prédéfinis et les modifier</i>	Permet à un utilisateur de créer et de modifier des calculs prédéfinis.
<i>Reporting - créer et modifier des contrôles d'entrée</i>	Permet à un utilisateur de créer et de modifier des contrôles d'entrée.
<i>Reporting : créer et modifier des filtres de rapport et utiliser des contrôles d'entrée</i>	Permet à un utilisateur de créer et de modifier des filtres de rapport et des contrôles d'entrée (le volet Contrôles d'entrées dans le panneau gauche ne s'affiche pas en cas de désactivation).
<i>Reporting : créer des tris et les modifier</i>	Permet à un utilisateur de créer et de modifier des tris.
<i>Reporting : créer des formules et variables</i>	Permet à un utilisateur de créer des formules et des variables.



Droit	Description
<i>Reporting : activer la mise en forme</i>	Permet à un utilisateur de modifier la mise en forme du rapport.  Sans ce droit d'accès, les modes Conception et Données ne sont pas disponibles.
<i>Reporting : activer les dimensions fusionnées</i>	Permet à un utilisateur de synchroniser les données à l'aide de dimensions fusionnées dans les rapports et dans le gestionnaire de données.
<i>Reporting : insérer et supprimer des rapports, des tables, des diagrammes et des cellules</i>	<ul style="list-style-type: none"> <li>• Permet à un utilisateur d'insérer et de supprimer des rapports, des tables, des diagrammes et des cellules.</li> <li>• Autorise le workflow des doublons (copier/coller).</li> </ul>
<i>Modifier les préférences des objets que possède l'utilisateur</i>	Affiche le menu <i>Préférences</i> 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 <i>Préférences</i> 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.

## 29.3.13.6 Strategy Builder

Ces droits d'accès s'appliquent à Strategy Builder et peuvent affecter le pilotage des objectifs dans Performance Manager ou certaines fonctionnalités spécifiques de Strategy Builder.

Droit	Description
<i>Créer, modifier ou supprimer des objectifs</i>	Permet à un utilisateur d'ajouter, de modifier ou de supprimer des objectifs dans Performance Manager.
<i>Afficher les objectifs</i>	Permet à un utilisateur de voir les objectifs dans les analyses.
<i>Accéder à la gestion des objectifs</i>	Permet à un utilisateur de visualiser les objectifs dans la page <i>Pilotage des objectifs</i> de Performance Manager.
<i>Publier les objectifs</i>	Permet à un utilisateur de publier des objectifs dans Performance Manager.
<i>Accéder à Strategy Builder</i>	Permet à un utilisateur d'accéder à Strategy Builder dans Performance Manager.
<i>Créer, modifier ou supprimer des rôles</i>	Permet à un utilisateur d'administrer les rôles utilisés pour publier des objectifs et des métriques pour des publics particuliers dans Strategy Builder.

Droit	Description
<i>Créer, modifier ou supprimer des stratégies</i>	Permet à un utilisateur de créer des stratégies de liaison de rôles et de publication d'objectifs et de métriques dans Strategy Builder.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

## 29.3.13.7 Outil de conception d'univers

Droit	Description
<i>Vérifier l'intégrité de l'univers</i>	Permet à un utilisateur de vérifier l'intégrité de l'univers.
<i>Actualiser la fenêtre de structure</i>	Permet à un utilisateur d'actualiser la fenêtre Structure.
<i>Utiliser la liste des tables</i>	Permet à un utilisateur d'afficher les données de la base de données à l'aide de la liste des tables.
<i>Appliquer les contraintes de l'univers</i>	Permet à un utilisateur d'appliquer des contraintes d'univers prédéfinies aux utilisateurs d'un univers importé.
<i>Lier l'univers</i>	Permet à un utilisateur de lier deux univers et de partager des composants.
<i>Créer, modifier ou supprimer des connexions</i>	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.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

## 29.3.13.8 Outil de conception d'information

Droit	Description
<i>Administrer des profils de sécurité</i>	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.
<i>Partager des projets</i>	Permet à un utilisateur de partager un projet local et de synchroniser un projet partagé avec le projet local.
<i>Créer, modifier ou supprimer des connexions</i>	<ul style="list-style-type: none"><li>• Permet à un utilisateur de créer et de supprimer les connexions sécurisées de la vue Ressources publiées.</li><li>• Permet à un utilisateur de modifier des connexions dans l'éditeur de connexion.</li><li>• Permet à un utilisateur de publier des connexions dans un référentiel.</li></ul>
<i>Publier l'univers</i>	Permet à un utilisateur de publier des univers dans un référentiel.
<i>Extraire l'univers</i>	Permet à un utilisateur d'extraire des univers publiés dans un projet local qui sera modifié.
<i>Enregistrer pour tous les utilisateurs</i>	Permet à un utilisateur d'enregistrer tous les utilisateurs lors de l'extraction des univers.
<i>Calculer des statistiques</i>	Permet à un utilisateur de sélectionner des tables et des colonnes dans lesquelles calculer et publier des statistiques.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	Affiche le menu <i>Préférences</i> 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 <i>Préférences</i> 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.

## 29.3.13.9 Indicateurs pour la plateforme de BI

Droit	Description
<i>Utiliser Explorer</i>	Permet à un utilisateur de se servir de l'Explorateur de documents pour parcourir du contenu sur tous les serveurs de la plateforme de BI connectés.

Droit	Description
<i>Utiliser la recherche</i>	Permet à un utilisateur de se servir de la Recherche de contenu pour rechercher simultanément tous les référentiels de la plateforme de BI connectés.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

## 29.3.13.10 Alertes

Droit	Description
<i>Déclencher les alertes</i>	<p>Permet à un utilisateur de déclencher des événements d'alerte. Pour déclencher une alerte pour un document, les droits supplémentaires suivants sont requis :</p> <ul style="list-style-type: none"> <li>• Droits "Afficher" et "Planifier" pour le document</li> <li>• Droits "Afficher" et "Déclenchement" pour l'événement correspondant</li> </ul>
<i>S'inscrire aux objets</i>	<p>Permet à un utilisateur de s'inscrire à un événement d'alerte. Pour s'inscrire à un événement, les droits supplémentaires suivants sont requis :</p> <ul style="list-style-type: none"> <li>• Droits "Afficher" pour l'événement correspondant</li> <li>• Droit "S'inscrire" pour le compte de l'utilisateur</li> </ul> <p>Pour s'inscrire à une alerte pour un document, les droits supplémentaires suivants sont requis :</p> <ul style="list-style-type: none"> <li>• Droit "Afficher" pour le document</li> <li>• Droit "Afficher l'instance" pour le document</li> <li>• Droits "Afficher" pour l'événement correspondant</li> <li>• Droit "S'inscrire" pour le compte de l'utilisateur</li> </ul>
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> ne s'affichera dans les applications. Par exemple, sans ce droit, les utilisateurs ne peuvent pas</p>

Droit	Description
	sélectionner l'unité de mesure (pouces ou millimètres) pour les rapports dans l'application Web Intelligence ou la barre de lancement BI.

## 29.3.13.11 Explorer

Droit	Description
<i>Se connecter à Explorer et visionner cet objet dans la CMC</i>	Permet à un utilisateur de se connecter à Epxplorer et d'afficher des objets dans la CMC.
<i>Explorer les espaces d'informations</i>	Permet à un utilisateur d'explorer un espace d'informations.  Pour vous connecter à Explorer, le droit "Se connecter à Explorer et visionner cet objet dans la CMC" est également requis.
<i>Explorer les espaces d'informations : Exporter comme signet/ courrier électronique</i>	Permet à un utilisateur de créer des signets de d'envoyer par e-mail des signets en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>• "Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>• "Explorer les espaces d'informations"</li> </ul>
<i>Explorer les espaces d'informations : Exporter au format CSV</i>	Permet à un utilisateur d'exporter les résultats d'une exploration dans un fichier CSV ou Excel, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>• "Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>• "Explorer les espaces d'informations"</li> </ul>
<i>Explorer les espaces d'informations : Exporter au format d'image</i>	Permet à un utilisateur d'exporter les résultats d'une exploration sous forme d'une image, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>• "Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>• "Explorer les espaces d'informations"</li> </ul>
<i>Explorer les espaces d'informations : Exporter vers Web Intelligence</i>	Permet à un utilisateur d'exporter les résultats d'une exploration sous forme de requête, en combinaison avec les droits supplémentaires suivants :

Droit	Description
	<ul style="list-style-type: none"> <li>"Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>"Explorer les espaces d'informations"</li> </ul>
<i>Gérer les espaces d'informations</i>	Permet à un utilisateur d'accéder au menu <i>Gestion des espaces</i> et d'exécuter les tâches associées, en combinaison avec le droit "Se connecter à Explorer et visionner cet objet dans la CMC".
<i>Gérer les espaces d'informations : Créer un espace d'informations</i>	Permet à un utilisateur de créer un espace d'informations, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>"Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>"Gérer les espaces d'informations"</li> </ul>
<i>Gérer les espaces d'informations : Modifier un espace d'informations</i>	Permet à un utilisateur de modifier ou de supprimer un espace d'informations, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>"Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>"Gérer les espaces d'informations"</li> </ul>
<i>Gérer les espaces d'informations : planifier l'indexation</i>	Permet à un utilisateur de planifier l'indexation pour les données d'un espace d'informations, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>"Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>"Gérer les espaces d'informations"</li> </ul>
<i>Gérer les espaces d'informations : lancer l'indexation</i>	Permet à un utilisateur de lancer l'indexation pour les données d'un espace d'informations, en combinaison avec les droits supplémentaires suivants : <ul style="list-style-type: none"> <li>"Se connecter à Explorer et visionner cet objet dans la CMC"</li> <li>"Gérer les espaces d'informations"</li> </ul>
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

## 29.3.13.12 SAP BusinessObjects Mobile

Droit	Description
<i>Connexion à l'application SAP BusinessObjects Mobile</i>	Permet à un utilisateur de se connecter à la plateforme de BI à partir de l'application Mobile et d'afficher des documents.
<i>S'inscrire aux alertes de documents</i>	<p>Permet à un utilisateur de s'inscrire à des alertes de document et d'instance périodique.</p> <p>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.</p> <p>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 <i>Evénements</i> système sous <i>Evénements</i> dans la CMC.</p>
<i>Enregistrer les documents dans le stockage local d'un appareil</i>	<p>Permet à un utilisateur d'enregistrer des documents sur un périphérique mobile.</p> <p>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.</p>
<i>Envoyer les documents d'un appareil sous forme de courrier électronique</i>	Permet à un utilisateur d'envoyer des rapports dans un message électronique.
<i>Modifier les préférences des objets que possède l'utilisateur</i>	<p>Affiche le menu <i>Préférences</i> dans un objet d'application.</p> <p>Sans ce droit d'accès, un utilisateur ne peut pas définir de préférences personnelles dans une application et aucun menu <i>Préférences</i> 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.</p>

Pour en savoir plus, voir le *Guide d'installation et de déploiement de SAP BusinessObjects Mobile*.

## 30 Annexe relative aux propriétés des serveurs

### 30.1 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.

#### Remarque

Pour en savoir plus sur les propriétés et métriques du serveur de SAP BusinessObjects Explorer, voir le *Guide de l'administrateur de SAP BusinessObjects Explorer*.

#### 30.1.1 Propriétés courantes du serveur

Les propriétés de serveur décrites dans cette section s'appliquent à tous les types de serveur.

Table 153 : Propriétés du port de requêtes

Propriété	Description	Valeur par défaut
<i>Nom du serveur</i>	Nom du serveur.	La valeur par défaut est le nom du nœud sur lequel se trouve le serveur, ainsi que le nom du serveur.
<i>ID, CUID</i>	L'ID court et l'ID unique de cluster du serveur. Lecture seule.	Ces valeurs sont générées automatiquement.
<i>Nœud</i>	Nom du nœud où le serveur est situé.	Cette valeur est spécifiée au cours de l'installation.
<i>Description</i>	Description du serveur	La valeur par défaut est le nom du serveur.
<i>Paramètres de ligne de commande</i>	Paramètres de ligne de commande pour le serveur.	La valeur par défaut dépend du type de serveur.



Propriété	Description	Valeur par défaut
<i>Port de requêtes</i>	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>Si l'option <i>Affecter automatiquement</i> 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.</p> </div>	Par défaut, <i>Affecter automatiquement</i> a pour valeur <b>TRUE</b> et le champ <i>Port de requêtes</i> est vide.
<i>Affecter automatiquement</i>	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 <i>Affecter automatiquement</i> la valeur <b>FALSE</b> et spécifiez un <i>Port de requêtes</i> valide.	La valeur par défaut est <b>TRUE</b> .

Table 154 : Propriétés de démarrage automatique

Propriété	Description	Valeur par défaut
<i>Démarrer automatiquement ce serveur au démarrage du Server Intelligence Agent</i>	<p>Indique si le serveur démarre automatiquement lors du démarrage ou redémarrage du SIA (Server Intelligence Agent).</p> <p>Si ce paramètre a pour valeur <b>FALSE</b> lorsque le SIA démarre ou redémarre, le serveur reste arrêté.</p>	La valeur par défaut est <b>TRUE</b> .

Table 155 : Propriétés des identifiants de l'hôte

Propriété	Description	Valeur par défaut
<i>Affecter automatiquement</i>	Spécifie si le serveur se lie à une interface réseau affectée automatiquement. Si cette propriété est définie sur <b>FALSE</b> , le serveur se lie à une interface réseau spécifique. Si elle est définie sur <b>TRUE</b> , 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 <b>FALSE</b> et en fournissant un nom d'hôte ou une adresse IP valide.	La valeur par défaut est <b>TRUE</b> .
<i>Nom d'hôte</i>	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, <i>Affecter automatiquement</i> est défini sur <b>TRUE</b> et le champ <i>Nom d'hôte</i> est vide.
<i>Adresse IP</i>	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, <i>Affecter automatiquement</i> est défini sur <b>TRUE</b> et le champ <i>Adresse IP</i> est vide.

Table 156 : Propriétés des modèles de configuration

Propriété	Description	Valeur par défaut
<i>Utiliser le modèle de configuration</i>	Spécifie si un modèle de configuration doit être utilisé.	La valeur par défaut est <b>FALSE</b> .
<i>Restaurer les valeurs par défaut du système</i>	Spécifie si les paramètres par défaut d'origine doivent être restaurés pour le serveur.	La valeur par défaut est <b>FALSE</b> .
<i>Définir le modèle de configuration</i>	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 <b>TRUE</b> , tous les services de même type spécifiés dans <i>Utiliser le modèle de configuration</i> sont immédiatement reconfigurés de façon à utiliser les paramètres du service actuel.	La valeur par défaut est <b>FALSE</b> .

Table 157 : Propriétés du service de journal de suivi

Propriété	Description	Valeur par défaut
<i>Niveau de journalisation</i>	<p>Spécifie le degré d'avertissement minimal que vous souhaitez consigner et détermine le volume d'informations enregistré dans le fichier journal du serveur.</p> <p>Les niveaux de seuil de journalisation possibles sont les suivants :</p> <ul style="list-style-type: none"> <li>• <i>Non spécifié</i></li> <li>• <i>Aucun</i></li> <li>• <i>Faible</i></li> <li>• <i>Moyen</i></li> <li>• <i>Elevé</i></li> </ul>	La valeur par défaut est <b>Non spécifié</b> .


## 30.1.2 Propriétés des services principaux

La catégorie Services principaux comprend les serveurs suivants :

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Dashboard Server
- Dashboard Analytics Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Serveur conteneur d'applications Web

## Propriétés d'Adaptative Job Server

Table 158 : Propriétés générales

Propriété	Description	Valeur par défaut
<i>Répertoire temporaire</i>	<p>Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire. Vous pouvez rencontrer 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.</p> <div> <b>Remarque</b> Vous devez redémarrer le serveur pour valider les modifications.</div>	%DefaultDataDir%

L'Adaptive Job Server peut héberger plusieurs services différents. Chaque service contient les propriétés suivantes :

Table 159 : Propriétés des services

Propriété	Description	Valeur par défaut
<i>Nombre maximal de travaux simultanés</i>	<p>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.</p> <p>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.</p>	5
<i>Nombre maximal de demandes enfant</i>	Indique le nombre de travaux traités par l'enfant avant le redémarrage.	100

## Propriétés du serveur de traitement adaptatif

Table 160 : Propriétés générales

Propriété	Description	Valeur par défaut
<i>Délai d'expiration du démarrage des services (secondes)</i>	<p>Délai, en secondes, accordé par le serveur pour le démarrage des services.</p> <p>Lorsqu'un service ne démarre pas dans le délai spécifié, deux raisons sont possibles :</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>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.</p>	1 200

Table 161 : Propriétés du service proxy d'audit client

Propriété	Description	Valeur par défaut
Aucune configuration de propriété		

Table 162 : Propriétés du service de jetons de sécurité

Propriété	Description	Valeur par défaut
Aucune configuration de propriété		

Table 163 : Propriétés du service Insight to Action

Métrique	Description	
<i>Nombre maximal de connexions actives par session utilisateur</i>	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
<i>Nombre maximal de connexions inactives par session utilisateur</i>	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
<i>Temps d'attente maximal de connexion (en secondes)</i>	Durée pendant laquelle la structure Insight to Action doit attendre une réponse du serveur SAP avant d'expirer (en secondes).	30

Table 164 : Propriétés du service de publication

Propriété	Description	Valeur par défaut
<i>Taille du pool de threads</i>	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

Table 165 : Propriétés du service de traduction

Propriété	Description	Valeur par défaut
Pas de propriétés de configuration		

Table 166 : Propriétés du service de surveillance

Propriété	Description	Valeur par défaut
Pas de propriétés de configuration		

Table 167 : Propriétés du service de recherche de plateformes

Propriété	Description	Valeur par défaut
Pas de propriétés de configuration		

Table 168 : Propriétés du service de post-traitement de la publication

Propriété	Description	Valeur par défaut
Pas de propriétés 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.

Table 169 : Propriétés du service de gestion centralisée

Propriété	Description	Valeur par défaut
<i>Port du serveur de noms</i>	Spécifie le port sur lequel le CMS écoute les requêtes de service de noms d'origine.	6400
<i>Connexions à la base de données système requises</i>	<p>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.</p> <p>La métrique <i>Connexions à la base de données système établies</i> du CMS indique le nombre actuel de connexions établies.</p>	14

Propriété	Description	Valeur par défaut
<i>Reconnexion automatique à la bases de données système</i>	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 <b>FALSE</b> , 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.	<b>TRUE</b>

Table 170 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	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

Table 171 : Propriétés du service d'événements

Propriété	Description	Valeur par défaut
<i>Intervalle entre les interrogations d'événement (secondes)</i>	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.
<i>Intervalle de nettoyage (minutes)</i>	Fréquence (en minutes) d'exécution de l'utilitaire de nettoyage.	20

## Propriétés de l'Input File Repository Server

Table 172 : Propriétés du service de stockage des fichiers d'entrée

Propriété	Description	Valeur par défaut
<i>Répertoire de stockage des fichiers</i>	<p>Spécifie le répertoire dans lequel sont stockés les objets du référentiel des fichiers.</p> <div> <i>i</i> <b>Remarque</b>            Vous pouvez rencontrer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.         </div>	%DefaultInputFRSDir/%

Propriété	Description	Valeur par défaut
<i>Répertoire temporaire</i>	<p>Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire.</p> <div> <b>i Remarque</b>            Vous pouvez rencontrer 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 <i>Répertoire temporaire</i> soit situé sur le même système de fichiers que le <i>Répertoire de stockage des fichiers</i>.         </div>	%DefaultInputFRSDir/temp%
<i>Délai maximal d'inactivité (minutes)</i>	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
<i>Nombre maximal de nouvelles tentatives d'accès au fichier</i>	Nombre de tentatives d'accès à un fichier effectué par le serveur.	1

## Propriétés de l'Output File Repository Server

Table 173 : Propriétés du service de stockage des fichiers de sortie

Propriété	Description	Valeur par défaut
<i>Répertoire de stockage des fichiers</i>	<p>Spécifie le répertoire dans lequel sont stockés les objets du référentiel des fichiers.</p> <div> <b>i Remarque</b>            Vous pouvez rencontrer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.         </div>	%DefaultOutputFRSDir/%
<i>Répertoire temporaire</i>	<p>Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire.</p> <div> <b>i Remarque</b>            Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.         </div>	%DefaultOutputFRSDir/temp%
<i>Délai maximal d'inactivité (minutes)</i>	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

Propriété	Description	Valeur par défaut
<i>Nombre maximal de nouvelles tentatives d'accès au fichier</i>	Nombre de tentatives d'accès à un fichier effectué par le serveur.	1

## Propriétés du serveur conteneur d'applications Web

Table 174 : Propriétés générales

Propriété	Description	Valeur par défaut
<i>Délai d'expiration du démarrage des services (secondes)</i>	<p>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.</p> <p>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).</p>	1 200

Table 175 : Propriétés du service TraceLog

Propriété	Description	Valeur par défaut
<i>Niveau de journalisation</i>	<p>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).</p> <p>Les choix de menu disponibles sont :</p> <ul style="list-style-type: none"> <li>• <i>Non spécifié</i></li> <li>• <i>Aucun</i></li> <li>• <i>Faible</i></li> <li>• <i>Moyen</i></li> <li>• <i>Elevé</i></li> </ul>	Non spécifié

Table 176 : Propriétés du service BI du processus de gestion

Propriété	Description	Valeur par défaut
Pas de propriétés de configuration		



Table 177 : Propriétés du service du générateur de requêtes

Propriété	Description	Valeur par défaut
Pas de propriétés de configuration		

Table 178 : Service Web RESTful - propriétés de configuration des propriétés système

Propriété	Description	Valeur par défaut
<i>Afficher la pile d'erreurs</i>	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
<i>Nombre d'objets par défaut sur une page</i>	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
<i>Délai d'expiration du jeton de session de l'entreprise (minutes)</i>	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
<i>Taille du groupe de sessions</i>	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.	1 000
<i>Délai d'expiration du groupe de sessions (minutes)</i>	Le temps, en minutes, avant que les sessions en mémoire cache n'expirent.	2
<i>Activer l'authentification HTTP élémentaire</i>	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 doivent 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 <i>Plan d'authentification par défaut pour HTTP élémentaire</i> s'affiche.	Non sélectionné
<i>Plan d'authentification par défaut pour HTTP élémentaire</i>	Lorsque la case <i>Activer l'authentification HTTP élémentaire</i> 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 : <ul style="list-style-type: none"> <li>• <i>secEnterprise</i></li> <li>• <i>secDAP</i></li> <li>• <i>SAPR3</i></li> <li>• <i>secWinAD</i></li> </ul>	Vide. Néanmoins, si <i>Activer l'authentification HTTP élémentaire</i> est sélectionné, définissez-la par défaut sur <i>secEnterprise</i> .

Table 179 : Services Web RESTful - propriétés de la configuration de Cross-Origin Resource Sharing

Propriété	Description	Valeur par défaut
<i>Autoriser les origines</i>	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
<i>Age maximum (minutes)</i>	Correspond au temps maximum durant lequel les navigateurs peuvent cacher les requêtes HTTP.	1440

Table 180 : Service Web RESTful - propriétés de la configuration de l'authentification sécurisée

Propriété	Description	Valeur par défaut
<i>Extraction de la méthode</i>	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. <ul style="list-style-type: none"> <li><b>HTTP_HEADER</b> est utilisé pour les requêtes GET avec l'en-tête de requête accept=application/xml (ou application/json).</li> <li><b>QUERY_STRING</b> 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.</li> <li><b>COOKIE</b> 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.</li> </ul>	<b>HTTP_HEADER</b>
<i>Paramètre du nom d'utilisateur</i>	Il s'agit de l'étiquette utilisée pour identifier l'utilisateur sécurisé pour extraire un jeton de connexion.	<b>X-SAP-TRUSTED-USER</b>

Table 181 : Propriétés du service d'applications Web BOE

Type de propriété	Description	Valeur par défaut
<i>Type d'authentification</i>	Type d'authentification utilisé pour authentifier les utilisateurs se connectant à la zone de lancement BI.  Les valeurs acceptées sont les suivantes : <ul style="list-style-type: none"> <li><b>AD Kerberos</b></li> <li><b>AD Kerberos SSO</b></li> <li><b>Enterprise</b></li> <li><b>LDAP</b></li> </ul>	<i>Enterprise</i>
<i>Domaine AD par défaut</i>	Le domaine Active Directory par défaut est utilisé pour éviter aux utilisateurs d'avoir à spécifier un domaine lors de leur connexion. Par exemple, si le domaine par défaut est défini sur « mondomaine » et si un utilisateur se connecte avec le nom d'utilisateur « utilisateur », l'autorité de connexion Active Directory tente d'authentifier « utilisateur@mondomaine.com ».	Vierge

Type de propriété	Description	Valeur par défaut
<i>Nom principal de service</i>	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
<i>Fichier Keytab</i>	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

Table 182 : Propriétés de SDK Services Web et QaaWS

Propriété	Description	Valeur par défaut
<i>Activer la connexion unique Kerberos Active Directory</i>	Indique si la connexion unique Kerberos AD doit être activée pour SDK Services Web et QaaWS.	<b>FALSE</b>
<i>Domaine AD par défaut</i>	Le domaine Active Directory par défaut est utilisé pour éviter aux utilisateurs d'avoir à spécifier un domaine lors de leur connexion.	Vierge
<i>Nom principal de service</i>	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
<i>Fichier Keytab</i>	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

Table 183 : Propriétés de la configuration HTTP

Propriété	Description	Valeur par défaut
<i>Lier à toutes les adresses IP</i>	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.	<b>TRUE</b>
<i>Lier au nom d'hôte ou à l'adresse IP</i>	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 <i>Lier à toutes les adresses IP</i> doit être désactivée.	<b>localhost</b>
<i>Port HTTP</i>	Port sur lequel est fourni le service HTTP.	6405 La plage des valeurs autorisées s'étend de 1 à 65535.
<i>Taille maximale de l'en-tête HTTP</i>	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Table 184 : Propriétés de configuration du port HTTP via proxy

Propriété	Description	Valeur par défaut
<i>Activer HTTP via proxy</i>	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.	<b>FALSE</b>
<i>Lier à toutes les adresses IP</i>	Indique si le port HTTP via proxy doit être lié à toutes les interface réseau.	<b>TRUE</b>

Propriété	Description	Valeur par défaut
<i>Lier au nom d'hôte ou à l'adresse IP</i>	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 <i>Lier à toutes les adresses IP</i> doit être désactivée.	<b>localhost</b>
<i>Port HTTP</i>	Port sur lequel est fourni le service HTTP d'un déploiement avec proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTP via proxy</i> doit être activée.	6406  La plage des valeurs autorisées s'étend de 1 à 65535.
<i>Nom d'hôte du proxy</i>	Adresses IPv4 et IPv6, nom d'hôte ou nom de domaine complet du serveur proxy. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTP via proxy</i> doit être activée.	Vierge
<i>Port du proxy</i>	Port du serveur proxy ou du serveur proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTP via proxy</i> doit être activée.	0  La plage des valeurs autorisées s'étend de 1 à 65535.
<i>Taille maximale de l'en-tête HTTP</i>	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Table 185 : Propriétés de configuration HTTPS

Propriété	Description	Valeur par défaut
<i>Activer HTTPS</i>	Indique si la communication HTTPS/SSL doit être activée.	<b>FALSE</b>
<i>Lier au nom d'hôte ou à l'adresse IP</i>	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 <i>Activer HTTPS</i> doit être activée.	<b>localhost</b>
<i>Port HTTPS</i>	Port sur lequel est fourni le service HTTPS. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	443  La plage des valeurs autorisées s'étend de 1 à 65535.
<i>Nom d'hôte du proxy</i>	Adresses IPv4 et IPv6, nom d'hôte ou nom de domaine complet du serveur proxy. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	Vierge
<i>Port du proxy</i>	Port du serveur proxy ou du serveur proxy inverse. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	0  La plage des valeurs autorisées s'étend de 1 à 65535.
<i>Protocole</i>	Protocole de cryptage à utiliser. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	TLS  Les valeurs autorisées sont TLS ou SSL.
<i>Type de stockage des certificats</i>	Type du fichier contenant vos certificats et clés privées. Il s'agit le plus souvent de <i>PKCS12</i> . Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	PKCS12  Les valeurs autorisées sont PKCS12 ou JKS.

Propriété	Description	Valeur par défaut
<i>Emplacement du fichier de stockage des certificats</i>	Chemin d'accès complet au fichier de stockage des certificats. Pour pouvoir spécifier une valeur, la case à cocher <i>Activer HTTPS</i> doit être activée.	Vierge
<i>Mot de passe d'accès aux clés privées</i>	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 <i>Activer HTTPS</i> doit être activée.	Vierge
<i>Alias du certificat</i>	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 <i>Activer HTTPS</i> doit être activée.	Vierge
<i>Activer l'authentification du client</i>	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 <i>Activer HTTPS</i> .	<b>FALSE</b>
<i>Emplacement du fichier de la liste de certificats de confiance</i>	Chemin d'accès complet au fichier de la liste de certificats de confiance. Pour pouvoir spécifier une valeur, les cases à cocher <i>Activer HTTPS</i> et <i>Activer l'authentification du client</i> doivent être activées.	Vierge
<i>Mot de passe d'accès aux clés privées de la liste de certificats de confiance</i>	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 <i>Activer HTTPS</i> et <i>Activer l'authentification du client</i> doivent être activées.	Vierge
<i>Taille maximale de l'en-tête HTTP</i>	Taille maximale autorisée de l'en-tête HTTP de demande et de réponse, exprimée en octets.	32768

Table 186 : Propriétés d'exécution simultanée (par connecteur)

Propriété	Description	Valeur par défaut
<i>Nombre maximal de requêtes simultanées</i>	Le nombre de requêtes HTTP ou HTTPS simultanées que chaque connecteur (HTTP, HTTP via proxy, ou HTTPS) peut traiter simultanément.	<b>150</b>  La plage des valeurs autorisées s'étend de 1 à 1000.

Table 187 : Propriétés de configuration d'Active Directory

Propriété	Description	Valeur par défaut
<i>Emplacement du fichier Krb5.ini</i>	Chemin d'accès complet au fichier <code>krb5.ini</code> qui stocke les propriétés de configuration Kerberos.	Vierge
<i>Emplacement du fichier bscLogin.conf</i>	Chemin d'accès complet au fichier <code>bscLogin.conf</code> .	Vierge

## 30.1.3 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.

Table 188 : Données Excel, propriétés des service d'accès

Propriété	Description	Valeur par défaut
<i>Intervalle (en secondes) entre chaque nettoyage d'accès aux données Excel</i>	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.
<i>Intervalle (en secondes) entre chaque permutation d'accès aux données Excel</i>	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 <i>Intervalle (en secondes) entre chaque nettoyage d'accès aux données Excel</i> .	La valeur par défaut est 600 secondes.

Table 189 : Propriétés de l'opération de service

Propriété	Description	Valeur par défaut
<b>→ N'oubliez pas</b> Il n'est pas nécessaire de redémarrer le serveur après avoir modifié les propriétés d'opération de service suivantes.		
<i>Pool de connexion</i>	<p>Active ou désactive le pool de connexion.</p> <p>Les valeurs possibles sont :</p> <ul style="list-style-type: none"><li>• Activé - Avec délai d'expiration</li><li>• Activé - Sans délai d'expiration</li><li>• Désactivé</li></ul> <p><b>i Remarque</b></p> <p>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.</p>	Activé - Avec délai d'expiration

Propriété	Description	Valeur par défaut
<i>Délai d'expiration du pool de connexion</i>	<p>Spécifie la durée d'inactivité maximale pour les connexions dans le pool (en minutes).</p> <div> <i>i</i> <b>Remarque</b>            Cette propriété est l'équivalente du paramètre <code>Max Pool Time</code> du fichier <code>cs.cfg</code>. La désactivation du pool revient à définir la <code>Durée maximale du pool</code> sur 0. L'activation du pool sans délai d'expiration revient à définir la <code>Durée maximale du pool</code> sur -1. Pour en savoir plus, reportez-vous au <a href="#">Guide d'accès aux données</a>.         </div>	60
<i>Délai d'inactivité des objets provisoires</i>	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
<i>Intervalle de l'horloge des objets provisoires</i>	Spécifie l'intervalle entre les contrôles d'activité (en minutes). A intervalles réguliers, le serveur recherche des objets susceptibles d'être supprimés.	5
<i>Activer le bloc HTTP</i>	<p>Active ou désactive le bloc HTTP.</p> <div> <i>i</i> <b>Remarque</b>            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 <a href="#">taille du bloc HTTP</a> définie sur 0.         </div>	Activé
<i>Taille du bloc HTTP</i>	Spécifie la taille des réponses HTTP émises par le serveur (en kilooctets).	64

Table 190 : Propriétés de suivi de bas niveau

Propriété	Description	Valeur par défaut
<div>➔ <b>N'oubliez pas</b></div> <p>Il n'est pas nécessaire de redémarrer le serveur après avoir modifié les propriétés de suivi de bas niveau suivantes.</p>		
<i>Activer le suivi du travail</i>	<p>Active le suivi des travaux du serveur de connexion.</p> <div> <i>i</i> <b>Remarque</b>            La propriété <a href="#">Niveau de journalisation</a> doit être définie sur <i>Haut</i>.         </div>	Désactivé

Propriété	Description	Valeur par défaut
<i>Activer le suivi du middleware</i>	<p>Active le suivi de tout le middleware. Pour suivre un middleware spécifique, vous devez configurer le fichier <code>cs.cfg</code> et redémarrer le serveur.</p> <p><b>i Remarque</b></p> <p>La propriété <i>Niveau de journalisation</i> doit être définie sur <i>Elevé</i>.</p>	Désactivé

Table 191 : Propriétés de sources de données actives

Propriété	Description	Valeur par défaut
<p><b>⚠ Attention</b></p> <p>Vous devez redémarrer le serveur après avoir modifié les propriétés de sources de données actives suivantes.</p>		
<i>Activer la source de données</i>	<p>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.</p> <p><b>⚠ Attention</b></p> <p>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.</p> <p><b>➔ N'oubliez pas</b></p> <p>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.</p> <p><b>i Remarque</b></p> <p>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 <i>Métrique de service de connexion</i>.</p>	Non coché
<i>Couche réseau</i>	<p>Spécifie la couche réseau utilisée par la connexion.</p> <p><b>i Remarque</b></p> <p>Seul le nom non localisé est considéré. Vous trouverez la liste des couches réseau disponibles dans le fichier <code>driver.cfg</code>, situé dans le répertoire <code>&lt;connectionserver-install-dir&gt;\connectionServer\</code>.</p>	<ul style="list-style-type: none"> <li>• ODBC pour les serveurs CORBA natifs</li> <li>• JDBC pour le serveur CORBA adaptatif</li> </ul>



Propriété	Description	Valeur par défaut
<i>Base de données</i>	<p>Spécifie la base de données utilisée par la connexion.</p> <div> <p><b>i Remarque</b></p> <p>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 <code>. *</code> pour remplacer un caractère quelconque. Par exemple, l'expression <code>MS SQL Server.*</code> 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 <a href="http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions">http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions</a>.</p> </div>	Le champ reste vide jusqu'à ce que vous y saisissez un nom de base de données.

Table 192 : Propriétés du service personnalisé d'accès aux données

Propriété	Description	Valeur par défaut
<i>Intervalle (en secondes) entre chaque nettoyage d'accès aux données personnalisées</i>	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.
<i>Intervalle (en secondes) entre chaque permutation d'accès aux données personnalisées</i>	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 <i>Intervalle (en secondes) entre chaque nettoyage d'accès aux données personnalisées</i> .	La valeur par défaut est 600 secondes.

Table 193 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

Table 194 : Propriétés du service de gestion des promotions

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Table 195 : Propriétés du service ClearCase de la gestion des promotions

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Table 196 : Propriétés du service de différence visuelle

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

## Informations associées

[Propriétés courantes du serveur \[page 948\]](#)

### 30.1.4 Propriétés des services Crystal Reports

La catégorie de service Crystal Reports comprend les serveurs suivants :

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Propriétés du Report Application Server Crystal Reports 2013
- Serveur de traitement Crystal Reports 2013

#### Propriétés du Crystal Reports Cache Server

Toutes les propriétés qui s'appliquent à la fois aux Crystal Reports Cache Servers et aux Crystal Reports Processing Servers doivent avoir la même valeur. Par exemple, si vous attribuez au paramètre *Toujours actualiser le visualiseur par rapport aux données actuelles* la valeur **TRUE** sur le Cache Server, vous devez également attribuer la valeur **TRUE** à ce même paramètre sur le Processing Server.

#### **i** Remarque

Lorsque vous modifiez l'une de ces propriétés de serveur, redémarrez le serveur pour valider les modifications.

Table 197 : Propriétés du service de mémoire cache Crystal Reports

Propriété	Description	Valeur par défaut
<i>Toujours actualiser par rapport aux données actuelles</i>	<p>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.</p> <div><b>i</b> Remarque</div> <p>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 ► <i>Paramètres par défaut</i> ► <i>Visualisation du groupe de serveurs</i> .</p>	La valeur par défaut est <b>FALSE</b> .

Propriété	Description	Valeur par défaut
<i>Partager les données des rapports entre les clients</i>	Indique si les données des rapports sont partagées entre différents clients.  <div> <i>i</i> <b>Remarque</b>            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.         </div>	La valeur par défaut est <b>TRUE</b> .
<i>Délai d'expiration de la connexion inactive (minutes)</i>	Délai, en minutes, accordé par le Crystal Reports Cache Server 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.
<i>Délai d'expiration du cache de sécurité (en minutes)</i>	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.
<i>Ancienneté maximale des données à la demande envoyées aux clients (secondes)</i>	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).  <div> <i>i</i> <b>Remarque</b>            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.         </div>	La valeur par défaut est 0 seconde.
<i>Taille maximale de la mémoire cache (Ko)</i>	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.
<i>Répertoire des fichiers de mémoire cache</i>	Emplacement du répertoire de mémoire cache.	%DefaultDataDir%/CrystalReportsCachingServer/temp

Propriété	Description	Valeur par défaut
<i>Arguments de la machine virtuelle Java</i>	Indique les arguments de ligne de commande pouvant être fournis à la JVM.	La valeur par défaut est vide.
<i>Nom de la DLL</i>	Spécifie le nom du plug-in de type de document en cours de chargement.  Cette propriété est en lecture seule.	rasprocReport




## Propriétés du Crystal Reports Processing Server

Toutes les propriétés qui s'appliquent à la fois aux Crystal Reports Cache Servers et aux Crystal Reports Processing Servers doivent avoir la même valeur. Par exemple, si vous attribuez au paramètre *Toujours actualiser le visualiseur par rapport aux données actuelles* la valeur **TRUE** sur le Cache Server, 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.

Table 198 : Propriétés du service de traitement Crystal Reports

Propriété	Description	Valeur par défaut
<i>Délai d'expiration d'un travail inactif (minutes)</i>	Durée, en minutes, attendue par le Crystal Reports Processing Server entre les requêtes pour un travail donné.	La valeur par défaut est 20 Minutes.
<i>Nombre maximal de travaux à durée de vie par enfant</i>	Nombre maximal de travaux que chaque processus enfant peut gérer par cycle de vie.	La valeur par défaut est 1 000.
<i>Toujours actualiser par rapport aux données actuelles</i>	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.  <div>  <b>Remarque</b>            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 <b>Paramètres par défaut</b>   <a href="#">Visualisation du groupe de serveurs</a>  </div>	La valeur par défaut est <b>FALSE</b> .

Propriété	Description	Valeur par défaut
<i>Partager les données des rapports entre les clients</i>	<p>Indique si les données des rapports sont partagées entre différents clients. Indique si les données des rapports sont partagées entre différents clients.</p> <div> <i>i</i> <b>Remarque</b> <p>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.</p> </div>	La valeur par défaut est <b>TRUE</b> .
<i>Délai d'expiration de la connexion inactive (minutes)</i>	Délai, en minutes, accordé par le Crystal Reports Processing Server 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.
<i>Nombre maximal de travaux simultanés (0 pour automatique)</i>	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le Crystal Reports Processing Server. Si cette propriété a pour valeur « 0 », le serveur applique une valeur adaptée, en fonction du processeur et de la mémoire de l'ordinateur sur lequel le serveur s'exécute.	La valeur par défaut est 0.
<i>Ancienneté maximale des données à la demande envoyées aux clients (secondes)</i>	<p>Durée, en secondes, pendant laquelle le serveur utilise les données mises en cache pour répondre aux requêtes émanant de rapports à la demande.</p> <p>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.</p> <p>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).</p> <div> <i>i</i> <b>Remarque</b> <p>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.</p> </div>	La valeur par défaut est 0.
<i>Nombre maximal d'enfants prédémarrés</i>	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.

Propriété	Description	Valeur par défaut
<i>Répertoire temporaire</i>	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire.  <b>i Remarque</b> Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
<i>Chemin de classe Java</i>	Nom et chemin des classes Java requises par le serveur.	%CommonJavaLibDir%/procCR.jar
<i>Arguments de la machine virtuelle Java enfant</i>	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

Table 199 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

## Propriétés du Report Application Server Crystal Reports 2013

### **i Remarque**

Si vous modifiez l'une de ces propriétés, vous devez redémarrer le serveur pour valider les modifications.

Table 200 : Propriétés du service de modification et de visualisation Crystal Reports 2013

Propriété	Description	Valeur par défaut
<i>Autoriser les travaux du rapport à rester connectés à la base de données jusqu'à la fermeture du travail du rapport</i>	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 <b>FALSE</b> .
<i>Taille des données à parcourir (enregistrements)</i>	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.

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion inactive (minutes)</i>	<p>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.</p> <p>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 <code>ReportClientDocument</code> n'est pas fermé de manière explicite, le serveur attendra inutilement qu'un travail inactif se ferme).</p>	La valeur par défaut est 30 minutes.
<i>Taille du lot (enregistrements)</i>	<p>Nombre de lignes provenant de l'ensemble des résultats renvoyées par la base de données lors du transfert de chaque donnée.</p> <p>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.</p>	La valeur par défaut est 100 enregistrements.
<i>Nombre d'enregistrements de la base de données devant être lus lors de la prévisualisation ou de l'actualisation d'un rapport (-1 pour illimité)</i>	<p>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.</p> <p>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.</p>	La valeur par défaut est 20 000 enregistrements.
<i>Nombre maximal de travaux simultanés (0 pour illimité)</i>	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le RAS.	La valeur par défaut est 75 enregistrements.
<i>Ancienneté maximale des données à la demande envoyées à un client (en minutes)</i>	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.

Propriété	Description	Valeur par défaut
<i>Répertoire temporaire</i>	Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire.  <b>i Remarque</b> Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.	%DefaultDataDir%/CrystalReportsRasServer/temp

Table 201 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

## Propriétés du serveur de traitement Crystal Reports 2013

### **i Remarque**

Si vous modifiez l'une de ces propriétés, vous devez redémarrer le serveur pour valider les modifications.

Table 202 : Propriétés du service de traitement Crystal Reports 2013

Propriété	Description	Valeur par défaut
<i>Délai d'expiration d'un travail inactif (minutes)</i>	Durée, en minutes, attendue par le Crystal Reports Processing Server entre les requêtes pour un travail donné.	La valeur par défaut est 20 Minutes.
<i>Nombre maximal de travaux à durée de vie par enfant</i>	Nombre maximal de travaux que chaque processus enfant peut gérer par cycle de vie.	La valeur par défaut est 1 000.
<i>Toujours actualiser par rapport aux données actuelles</i>	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.  <b>i Remarque</b> 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 ► <a href="#">Paramètres par défaut</a> ► <a href="#">Visualisation du groupe de serveurs</a> ►.	La valeur par défaut est <b>FALSE</b> .



Propriété	Description	Valeur par défaut
<i>Partager les données des rapports entre les clients</i>	Indique si les données des rapports sont partagées entre différents clients. Indique si les données des rapports sont partagées entre différents clients.  <div> <i>i</i> <b>Remarque</b>            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.         </div>	La valeur par défaut est <b>TRUE</b> .
<i>Délai d'expiration de la connexion inactive (minutes)</i>	Délai, en minutes, accordé par le Crystal Reports Processing Server 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.
<i>Nombre maximal de travaux simultanés (0 pour automatique)</i>	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le Crystal Reports Processing Server. Si cette propriété a pour valeur « 0 », le serveur applique une valeur adaptée, en fonction du processeur et de la mémoire de l'ordinateur sur lequel le serveur s'exécute.	La valeur par défaut est 0.
<i>Ancienneté maximale des données à la demande envoyées aux clients (secondes)</i>	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).  <div> <i>i</i> <b>Remarque</b>            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.         </div>	La valeur par défaut est 0.
<i>Nombre maximal d'enfants prédémarrés</i>	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.

Propriété	Description	Valeur par défaut
<i>Répertoire temporaire</i>	<p>Répertoire dans lequel les fichiers temporaires sont créés lorsque cela est nécessaire.</p> <div> <i>i</i> <b>Remarque</b>            Vous pouvez remarquer des problèmes de performance si ce répertoire ne dispose pas d'un espace disque suffisant.         </div>	%DefaultDataDir%/CrystalReports2013Processing-Server/temp
<i>Autoriser les travaux du rapport à rester connectés à la base de données jusqu'à la fermeture du travail du rapport</i>	Indique si le travail du rapport reste connecté à la base de données jusqu'à sa fermeture.	La valeur par défaut est FALSE.
<i>Enregistrements de base de données lus lors de la prévisualisation ou de l'actualisation (0 pour illimité)</i>	<p>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.</p> <p>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.</p>	La valeur par défaut est 20 000.

Table 203 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

## 30.1.5 Propriétés d'Analysis Services

La catégorie des services d'Analysis comprend le serveur de traitement adaptatif :

Table 204 : Propriétés du service MDAS (Multi-Dimensional Analysis Service)

Propriété	Description	Valeur par défaut
<i>Nombre maximal de sessions client</i>	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.
<i>Nombre maximal de cellules renvoyées par une requête</i>	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.
<i>Nombre maximal de membres renvoyés lors du filtrage</i>	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.

Table 205 : Propriétés de service des applications Web BEx

Propriété	Description	Valeur par défaut
<i>Nombre maximal de sessions client</i>	Nombre maximal de sessions client autorisées sur le service.	La valeur par défaut est 15 sessions.
<i>Système maître SAP BW</i>	Nom de la connexion OLAP au système BW que vous avez créée dans la plateforme de BI.	La valeur par défaut est SAP_BW.
<i>Destination RFC du serveur JCo</i>	Nom de destination RFC du serveur JCo que vous avez saisi dans le système BW.	Par défaut, cette valeur est vide.
<i>Hôte passerelle du serveur JCo</i>	Nom de l'hôte passerelle du serveur JCo que vous avez défini dans le système BW.	Par défaut, cette valeur est vide.
<i>Service de passerelle du serveur JCo</i>	Nom du service de passerelle du serveur JCo que vous avez défini dans le système BW.	Par défaut, cette valeur est vide.
<i>Nombre de connexions du serveur JCo</i>	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.

## 30.1.6 Propriétés des services de fédération de données

La catégorie de service Data Federation inclut le serveur de traitement adaptatif :

Table 206 : Propriétés des services de fédération de données

Propriété	Description	Valeur par défaut
<i>Nombre maximal de connexions</i>	Nombre maximal de connexions autorisées sur le serveur.	La valeur par défaut est 32 767.
<i>Taille du pool de threads d'exécution</i>	Nombre maximal de requêtes pouvant être exécutées en parallèle à un moment donné.	La valeur par défaut est 10.
<i>Délai d'inactivité de la connexion</i>	Durée, en secondes, après laquelle une connexion inactive est fermée.	La valeur par défaut est de 10 800 secondes.
<i>Délai d'inactivité de l'instruction</i>	Durée, en secondes, après laquelle une instruction de requête est fermée.	La valeur par défaut est de 600 secondes.

## 30.1.7 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

Table 207 : Paramètres de ligne de commande

Propriété	Description	Valeur par défaut
Développer jusqu'au niveau	<p>Spécifie le niveau auquel les données sont récupérées à partir des requête BEx.</p> <p>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.</p>	<p>-</p> <p><b>Dsap.sl.bics.expandToLevel=n</b></p> <p>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.</p>

Propriété	Description	Valeur par défaut
Sélection de variables Option de sélection	<p>Spécifie l'option de sélection pour la sélection de variables.</p> <p>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.</p> <p>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.</p> <div> <p><b>i Remarque</b></p> <p>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".</p> </div>	<p>-</p> <p><b>Dsap.sl.bics.variableComplexSelectionMapping=n</b></p> <p>où n peut être intervalle ou valeurs multiples.</p> <div> <p><b>i Remarque</b></p> <p>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 :</p> <ul style="list-style-type: none"> <li>• Un document doit être purgé.</li> <li>• Les valeurs par défaut pour les invites de requête doivent être modifiées afin d'être compatibles avec la sélection de valeurs multiples.</li> </ul> </div>

Table 208 : Propriétés du service de surveillance de Web Intelligence

Propriété	Description	Valeur par défaut
<i>Activer la surveillance</i>	Spécifie si la surveillance est activée pour le service.	<b>TRUE</b>
<i>Délai de boucle de thread de surveillance (en secondes)</i>	Spécifie la durée en secondes entre les tentatives d'un service pour effectuer un test ping sur les clients.	300
<i>Intervalle (en secondes) entre chaque nettoyage de ressource surveillée par défaut</i>	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	1200
<i>Intervalle (en secondes) entre chaque permutation de ressource surveillée par défaut</i>	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
<i>Activer le profilage de service</i>		<b>TRUE</b>
<i>Activer la surveillance d'activité de service</i>		<b>TRUE</b>

Table 209 : Propriétés du service de visualisation

Propriété	Description	Valeur par défaut
<i>Délai d'expiration avant nettoyage du moteur de visualisation (en secondes)</i>	Temps d'attente, en secondes, avant que le service obtienne un client inactif et effectue un nettoyage de sa session.	1200
<i>Délai d'expiration avant permutation du moteur de visualisation (en secondes)</i>	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 <i>Délai d'expiration avant nettoyage du moteur de visualisation (en secondes)</i> .	600

Table 210 : Propriétés du service Rebean

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Table 211 : Propriétés du service de récupération de documents

Propriété	Description	Valeur par défaut
Aucune propriété de configuration		

Table 212 : Propriétés du service de pont DSL

Propriété	Description	Valeur par défaut
<i>Intervalle (en secondes) entre chaque nettoyage du moteur du pont DSL</i>	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.

Table 213 : Propriétés du service du moteur d'informations

Propriété	Description	Valeur par défaut
<i>Activer la mémoire cache des listes de valeurs</i>	Indique si la mise en cache des listes de valeurs est activée sur le Web Intelligence Processing Server.	<b>TRUE</b>
<i>Taille de lot de la liste des valeurs (entrées)</i>	Nombre maximal d'entrées (ou de valeurs) pour chaque lot de listes de valeurs.	1000
<i>Taille maximale du tri personnalisé (entrées)</i>	Nombre maximal d'entrées du tri personnalisé.	100

Propriété	Description	Valeur par défaut
<i>Taille maximale du cache d'univers (univers)</i>	Nombre d'univers à mettre en cache sur le Web Intelligence Processing Server.	20
<i>Taille maximales de la liste de valeurs (entrées)</i>	Nombre maximal d'entrées (ou de valeurs) pour chaque liste de valeurs.	50000

Table 214 : Propriétés des services principaux Web Intelligence

Propriété	Description	Valeur par défaut
<i>Délai d'expiration avant recyclage (secondes)</i>	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 <i>Nombre maximal de documents avant recyclage</i> .	1200
<i>Délai d'expiration pour inactivité de document (secondes)</i>	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.
<i>Intervalle d'interrogation du serveur (secondes)</i>	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
<i>Nombre maximal de documents par utilisateur</i>	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.
<i>Nombre maximal de documents avant recyclage</i>	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 <i>Délai d'expiration avant recyclage (secondes)</i> .	50
<i>Activer les messages d'erreur en cas de taille maximale de carte de document</i>	Indique si le <i>&lt;Nombre maximal de connexions&gt;</i> est restreint. Si cette propriété est activée, la valeur définie pour la propriété <i>&lt;Nombre maximal de connexions&gt;</i> est reconnue par le serveur, sinon elle est ignorée.	<b>TRUE</b>
<i>Délai d'expiration de la connexion inactive (minutes)</i>	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

Propriété	Description	Valeur par défaut
<i>Nombre maximal de connexions</i>	<p>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.</p> <div> <i>i</i> Remarque           <p>Pour que cette propriété soit reconnue par le serveur, la propriété <code>&lt;Activer les messages d'erreur en cas de taille maximale de carte de document&gt;</code> doit être activée.</p> </div>	<p>50</p> <p>La plage valide est comprise entre 5 et 65 535.</p>
<i>Activer l'analyse de mémoire</i>	<p>Indique si l'analyse de mémoire est activée. Si tel est le cas, les propriétés suivantes sont également activées et reconnues par le serveur.</p> <ul style="list-style-type: none"> <li><code>&lt;Seuil maximal de la mémoire (Mo)&gt;</code></li> <li><code>&lt;Seuil supérieur de la mémoire (Mo)&gt;</code></li> <li><code>&lt;Seuil inférieur de la mémoire (Mo)&gt;</code></li> </ul> <p>Lorsque la mémoire de traitement du serveur dépasse le <code>&lt;Seuil supérieur de la mémoire&gt;</code>, seul l'enregistrement de document est autorisé. Lorsque la mémoire de traitement dépasse le <code>&lt;Seuil maximal de la mémoire&gt;</code>, toutes les opérations s'arrêtent et échouent.</p>	<b>TRUE</b>
<i>Seuil inférieur de la mémoire (Mo)</i>	Seuil inférieur de consommation de mémoire.	<b>3500</b>
<i>Seuil supérieur de la mémoire (Mo)</i>	Seuil supérieur de consommation de mémoire.	<b>4500</b>
<i>Seuil maximal de la mémoire (Mo)</i>	Seuil maximal de consommation de mémoire.	<b>6000</b>
<i>Activer la surveillance du service APS</i>	Active la surveillance du serveur par le service APS hébergé sur le serveur de traitement adaptatif.	<b>TRUE</b>
<i>Nombre de tentatives après échec de la commande ping du service APS</i>	Indique le nombre de fois où le serveur tente d'atteindre le service APS avant de décider que c'est impossible.	3
<i>Période de thread de la surveillance de service APS</i>	Spécifie le temps d'attente entre les tentatives pour joindre le service APS.	300
<i>Activer les journaux d'activité actuels</i>	<p>Indique si des traces complètes sont générées dans les fichiers journaux du serveur.</p> <div> <i>i</i> Remarque           <p>Cette propriété doit être activée uniquement à des fins de débogage lors du dépannage des problèmes. Défini sur <b>FALSE</b> pendant le fonctionnement normal.</p> </div>	<b>FALSE</b>



Table 215 : Propriétés du service de traitement Web Intelligence

Propriété	Description	Valeur par défaut
<i>Activer l'utilisation de l'URL HTTP</i>	Spécifie si le serveur peut accéder à des fichiers stockés à distance.	<b>TRUE</b>
<i>Valeur proxy</i>	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

Table 216 : Propriétés des service communs Web Intelligence

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la mémoire cache (minutes)</i>	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
<i>Intervalle de nettoyage de la mémoire cache de document (minutes)</i>	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
<i>Désactiver le partage de la mémoire cache</i>	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.	<b>FALSE</b>
<i>Activer la mémoire cache de document</i>	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.	<b>TRUE</b>
<i>Activer la mémoire cache en temps réel</i>	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.	<b>TRUE</b>
<i>Taille maximale de la mémoire cache du document (Ko)</i>	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
<i>Espace maximum de réduction du cache du document (pourcentage)</i>	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

Propriété	Description	Valeur par défaut
<i>Taille maximale du flux de caractères (Mo)</i>	<p>Taille maximale du flux de caractères envoyé au client Web Intelligence.</p> <p><b>i Remarque</b></p> <p>Si la propriété <i>Taille maximale du flux de caractères (Mo)</i> est dépassée, le document Web Intelligence n'est pas créé et le client reçoit un message d'erreur.</p>	<p>5</p> <p>La plage valide est comprise entre 1 et 65 535 Mo.</p>
<i>Taille maximale des flux binaires (Mo)</i>	<p>Taille maximale, en Mo, du flux binaire envoyé au client Web Intelligence.</p> <p><b>i Remarque</b></p> <p>Si la propriété <i>Taille maximale des flux binaires (Mo)</i> est dépassée, le document Web Intelligence n'est pas créé et le client reçoit un message d'erreur.</p>	<p>50</p> <p>La plage valide est comprise entre 1 et 65 535 Mo.</p>
<i>Répertoire des images</i>	Emplacement du répertoire des images.	Vierge
<i>Répertoire de la mémoire cache de sortie</i>	Emplacement de la mémoire cache.	Vierge

Table 217 : Propriétés générales

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	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 \[page 982\]](#)

### 30.1.7.1 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 :

$$4500\text{MB} - .20 * 4500\text{MB} = 3600\text{MB}$$

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.

## 30.1.8 Propriétés de Dashboards Services

### Propriétés de Dashboards Cache Server

Table 218 : Propriétés de Dashboards Cache Service

Propriété	Description	Valeur par défaut
<i>Taille maximale de la mémoire cache (Ko)</i>	Espace disque (en kilo-octets) consacré à la mise en mémoire cache des requêtes. Une taille de cache importante peut être nécessaire si le serveur doit gérer un grand nombre de requêtes ou des requêtes particulièrement complexes.	La valeur par défaut est 256 000 Kilo-octets.
<i>Délai d'expiration de la connexion inactive (minutes)</i>	Délai, en minutes, accordé par le Dashboards Cache Server 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 15 minutes.
<i>Partager les données entre les clients</i>	Indique si les données des rapports sont partagées entre différents clients.	La valeur par défaut est <b>TRUE</b> .
<i>Ancienneté maximale des données à la demande envoyées aux clients (secondes)</i>	<p>Durée, en secondes, pendant laquelle le serveur utilise les données mises en cache pour répondre aux requêtes à la demande.</p> <p>Si le serveur reçoit une 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.</p> <p>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 (les modifications importantes sont fréquentes), il peut être judicieux de désactiver la réutilisation des données en attribuant à ce paramètre la valeur 0.</p> <div><b>i Remarque</b> Cette propriété peut être définie dans un objet de rapport ; les valeurs spécifiées dans l'objet de rapport remplacent les paramètres du serveur.</div>	La valeur par défaut est 0 seconde.
<i>Délai d'expiration du cache de sécurité (en minutes)</i>	Durée, en minutes, pendant laquelle le serveur utilise des références de connexion, des propriétés de requête et des informations de connexion à la base de données mises en cache pour servir des requêtes avant d'interroger le CMS.	La valeur par défaut est 20 Minutes.
<i>Arguments de la machine virtuelle Java</i>	Indique les arguments de ligne de commande pouvant être fournis à la JVM.	Xmx858M

## Propriétés de Dashboards Processing Server

Table 219 : Propriétés de Dashboards Processing Service

Propriété	Description	Valeur par défaut
<i>Nombre maximal de travaux simultanés</i>	Nombre maximal de travaux indépendants pouvant être exécutés simultanément sur le serveur. Si cette propriété a pour valeur « 0 », le serveur applique une valeur adaptée, en fonction du processeur et de la mémoire de l'ordinateur sur lequel le serveur s'exécute.	La valeur par défaut est 0.
<i>Nombre maximal de travaux à durée de vie par enfant</i>	Nombre maximal de travaux que chaque processus enfant peut gérer par cycle de vie.	La valeur par défaut est de 10 000.
<i>Nombre maximal d'enfants prédémarrés</i>	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.
<i>Délai d'expiration de la connexion inactive (minutes)</i>	Délai, en minutes, accordé par le serveur 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 15 minutes.
<i>Délai d'expiration d'un travail inactif (minutes)</i>	Temps d'attente du serveur, en minutes, entre les requêtes pour un travail donné.	La valeur par défaut est 15 minutes.
<i>Arguments de la machine virtuelle Java enfant</i>	Indique les arguments de ligne de commande fournis aux processus enfant créés par le serveur.	Xmx858M,Dswfinjection.lang.directory=%CommonJavaLibDir%,Dbusinessobjects.connectivity.directory=%CONNECTION-SERVER_DIR%

Table 220 : Propriétés du service de connexion unique

Propriété	Description	Valeur par défaut
<i>Délai d'expiration de la connexion unique (secondes)</i>	Durée de validité, en secondes, d'une connexion unique avant qu'elle n'expire.	La valeur par défaut est 86 400 secondes.

## 31 Annexe métrique système

### 31.1 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 :

Table 221 :

Etat des serveurs	Description
<i>Etat</i>	Etat indique l'état général d'un serveur Valeurs possibles : <ul style="list-style-type: none"><li>• 0 = Rouge (Danger)</li><li>• 1 = Orange (Attention)</li><li>• 2 = Vert (Sain)</li></ul>
<i>Etat activé du serveur</i>	Cet état indique si un serveur est activé ou désactivé. Valeurs possibles : <ul style="list-style-type: none"><li>• 0 = Désactivé</li><li>• 1 = Activé</li></ul>
<i>Etat en cours d'exécution du serveur</i>	Cet état indique l'état d'exécution du serveur. Valeurs possibles : <ul style="list-style-type: none"><li>• 0 = ARRETE</li><li>• 1 = DEMARRAGE EN COURS</li><li>• 2 = INITIALISATION EN COURS</li><li>• 3 = EXECUTION EN COURS</li><li>• 4 = ARRET EN COURS</li><li>• 5 = ECHEC</li><li>• 6 = EXECUTION_AVEC_ERREURS</li><li>• 7 = EXECUTION_AVEC_AVERTISSEMENTS</li></ul>

#### Remarque

Pour en savoir plus sur les propriétés et métriques du serveur SAP BusinessObjects Explorer, voir le *Guide de l'administrateur de SAP BusinessObjects Explorer*.

## 31.1.1 Métriques communes du serveur

Ces métriques décrivent l'ordinateur sur lequel s'exécute le serveur spécifié.

Table 222 : Métriques spécifiques à l'ordinateur

Métrique	Description
<i>Nom de l'ordinateur</i>	Nom d'hôte de l'ordinateur sur lequel s'exécute le serveur.
<i>Système d'exploitation</i>	Système d'exploitation de l'ordinateur sur lequel s'exécute le serveur.
<i>Type de processeur</i>	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).
<i>Processeurs</i>	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).
<i>RAM (Mo)</i>	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).
<i>Heure locale</i>	Heure locale.
<i>Taille du disque (Go)</i>	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).
<i>Espace disque utilisé (Go)</i>	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.

Table 223 : Métriques spécifiques au serveur

Métrique	Description
<i>Nom du serveur</i>	Nom et numéro de port du serveur CMS sur lequel ce serveur publie son adresse.
<i>Nom enregistré</i>	Nom interne du serveur. Il ne s'agit pas du nom qui figure dans l'écran <i>Serveurs</i> de la CMC.
<i>Version</i>	Version du serveur.
<i>Heure de début</i>	Heure de démarrage du serveur la plus récente.
<i>PID</i>	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.
<i>Nom d'hôte</i>	Liste au format CSV de tous les noms d'hôte actuellement utilisés sur le serveur.
<i>Adresse IP de l'hôte</i>	Liste au format CSV des adresses IP pour lesquelles le serveur est à l'écoute des requêtes.

Métrique	Description
<i>Port de requêtes</i>	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.
<i>Threads serveur occupé</i>	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.

Table 224 : Métriques d'audit

Métrique	Description
<i>Nombre actuel d'événements d'audit en attente</i>	<p>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.</p> <div> <p><b>i Remarque</b></p> <p>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.</p> </div>

Table 225 : Journalisation des métriques de service

Métrique	Description
<i>Répertoire de journalisation</i>	Les fichiers journaux du serveur se trouvent à cet emplacement.

## 31.1.2 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).

Table 226 : Métriques du Central Management Server

Métrique	Description
<i>La connexion à la base de données d'audit est établie</i>	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
<i>Auditeur CMS</i>	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.
<i>Nom de la connexion à la base de données d'audit</i>	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.
<i>Nom d'utilisateur de la base de données d'audit</i>	Nom du compte utilisateur utilisé pour se connecter à la base de données d'audit.
<i>Date de la dernière mise à jour de la base de données d'audit</i>	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.
<i>Durée du dernier cycle d'interrogation du thread d'audit (secondes)</i>	<p>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.</p> <ul style="list-style-type: none"> <li>• Une valeur inférieure à 20 minutes indique que le système est sain.</li> <li>• Une valeur comprise entre 20 minutes et 2 heures indique que le système est occupé.</li> <li>• 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.</li> </ul>
<i>Utilisation du thread d'audit</i>	<p>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.</p> <p>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.</p>
<i>Serveurs CMS en cluster</i>	Liste séparée par des points-virgules des noms d'hôte et numéros de port des serveurs CMS en cours de fonctionnement dans le cluster.
<i>Nombre de sessions établies par des utilisateurs simultanés</i>	Total des sessions des utilisateurs ayant une licence d'accès simultané.
<i>Nombre de sessions établies par des utilisateurs nommés</i>	Total des sessions des utilisateurs ayant une licence nommée.
<i>Nombre maximum de sessions depuis le démarrage</i>	Nombre maximum de sessions utilisateur simultanées gérées par le CMS depuis son démarrage.
<i>Nombre de sessions établies par des serveurs</i>	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.

Métrique	Description
<i>Nombre de sessions établies par tous les utilisateurs</i>	Nombre de sessions utilisateur simultanées gérées par le CMS lors du chargement de l'écran <i>Métriques</i> . 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.
<i>Travaux en échec</i>	Nombre de travaux échoués sur le système.
<i>Travaux en suspens</i>	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.
<i>Travaux en cours d'exécution</i>	Nombre de travaux s'exécutant actuellement.
<i>Travaux terminés</i>	Nombre de travaux réalisés sur le système.
<i>Travaux en attente</i>	Nombre de travaux dans le système qui sont planifiés et en attente de ressources disponibles.
<i>Licences Utilisateur simultané</i>	Nombre de licences Utilisateurs simultané indiqué par le code clé.
<i>Licences Utilisateur nommé</i>	Nombre de licences Utilisateur nommé indiqué par le code clé.
<i>Date de version</i>	Date de version du CMS.
<i>Nom de la connexion à la base de données système</i>	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.
<i>Nom du serveur de la base de données système</i>	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.
<i>Nom de l'utilisateur de la base de données système</i>	Nom du compte utilisateur utilisé pour se connecter à la base de données système du CMS.
<i>Nom de la source de données</i>	Nom de la connexion à la base de données système du CMS.
<i>Numéro de version</i>	Numéro de version du CMS. Ce numéro peut être utilisé pour identifier la version de la plateforme SAP BusinessObjects Business Intelligence qui est installée.
<i>Version du produit</i>	Version du produit du CMS.
<i>Version de la ressource</i>	Version de la ressource du CMS.
<i>Temps de réponse moyen de validation depuis le démarrage (ms)</i>	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.
<i>Temps de réponse moyen des requêtes depuis le démarrage (ms)</i>	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.
<i>Temps de réponse maximum de validation depuis le démarrage (ms)</i>	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.
<i>Temps de réponse maximum des requêtes depuis le démarrage (ms)</i>	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.

Métrique	Description
<i>Nombre de validations depuis le démarrage</i>	Nombre de validations sur la base de données système du CMS depuis le démarrage du serveur.
<i>Nombre de requêtes depuis le démarrage</i>	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.
<i>Nombre de connexions utilisateur depuis le démarrage</i>	Nombre total de connexions des utilisateurs depuis le démarrage du serveur. Un nombre important peut indiquer un système plus actif ou fortement chargé.
<i>Connexions à la base de données système établies</i>	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 <i>Connexions à la base de données système requises</i> (zone <i>Central Management Service</i> de l'écran <i>Propriétés</i> ), 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.
<i>Connexions à la base de données système en cours d'utilisation</i>	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 <i>Connexions à la base de données système requises</i> dans l'écran <i>Propriétés</i> peut améliorer les performances du CMS. L'ajustement de la configuration de la base de données système du CMS peut également améliorer les performances.
<i>Demandes à la base de données système en suspens</i>	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 <i>Connexions à la base de données système requises</i> . L'ajustement de la configuration de la base de données système du CMS peut également améliorer les performances.
<i>Nombre d'objets dans le cache système du CMS</i>	Nombre total d'objets actuellement dans le cache système du CMS.
<i>Nombre d'objets dans la BD système du CMS</i>	Nombre total d'objets actuellement dans la base de données système du CMS.
<i>Comptes utilisateur simultanés existants</i>	Nombre total des utilisateurs existants ayant une licence d'accès simultané dans le cluster.
<i>Comptes utilisateur nommé existants</i>	Nombre total des utilisateurs existants ayant une licence nommée dans le cluster.

### 31.1.3 Métrique du serveur de connexion

La métrique suivante est propre au Connection Server.

Table 227 : Métriques du service de connectivité

Métrique	Description
<i>Sources de données</i>	<p>Répertorie dans un tableau les sources de données activées via la page <a href="#">Propriétés</a>. Affiche les informations suivantes pour chaque couche réseau et paire de bases de données :</p> <ul style="list-style-type: none"> <li>• <i>Statut (Chargé ou Echec)</i> : statut actuel du pilote</li> <li>• <i>Connexions disponibles</i> : nombre de connexions pouvant être utilisées dans le pool</li> <li>• <i>Travaux (CORBA)</i> : nombre de travaux en cours de traitement (déploiement à 2 niveaux)</li> <li>• <i>Travaux (HTTP)</i> : nombre de travaux en cours de traitement (déploiement de niveau Web)</li> </ul> <p><b>i Remarque</b></p> <p>Pour plus d'informations sur les pools de connexion, voir le <i>Guide d'accès aux données</i>.</p>

### 31.1.4 Métriques de l'Event Server

Le tableau suivant décrit les métriques de serveur figurant dans l'écran [Métriques](#) pour les serveurs Event Server.

Table 228 : Métrique de service d'événement

Métrique	Description
<i>Liste des fichiers contrôlés</i>	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.
<i>Fichiers contrôlés</i>	Nombre total des fichiers contrôlés par l'Event Server.

### 31.1.5 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.

Table 229 : Métrique de service de stockage de fichiers

Métrique	Description
<i>Fichiers actifs</i>	Nombre de fichiers du File Repository Server actuellement en cours d'accès.
<i>Données écrites (Mo)</i>	Total des mégaoctets écrits dans les fichiers du serveur.
<i>Données envoyées (Mo)</i>	Total des mégaoctets lus dans les fichiers du serveur.

Métrique	Description
<i>Liste des fichiers actifs</i>	Tableau affichant les fichiers du File Repository Server actuellement en cours d'accès.
<i>Connexions actives</i>	Nombre total de connexions actives à partir des clients et vers les autres serveurs.
<i>Espace disque disponible dans le répertoire racine (Go)</i>	Volume total d'espace disponible sur le disque contenant le fichier exécutable du serveur, en giga-octets.
<i>Espace disque libre dans le répertoire racine (Go)</i>	Volume total d'espace libre sur le disque contenant le fichier exécutable du serveur, en giga-octets.
<i>Espace disque total dans le répertoire racine (Go)</i>	Espace disque total sur le disque contenant le fichier exécutable du serveur, en giga-octets.
<i>Espace disque disponible dans le répertoire racine (%)</i>	Volume d'espace disque, en pourcentage, disponible sur le disque contenant le fichier exécutable du serveur.

## 31.1.6 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.

Table 230 : Métriques du serveur de traitement adaptatif

Métrique	Description
<i>Threads de la couche de transport</i>	Nombre total de threads dans l'ensemble des pools de la couche de transport.
<i>Taille du pool de threads de la couche de transport</i>	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.
<i>Processeurs disponibles</i>	Nombre de processeurs disponibles pour la machine virtuelle Java (JVM) sur laquelle le serveur est exécuté.
<i>Taille maximale de la mémoire (Mo)</i>	Mémoire maximale en mégaoctets que la machine virtuelle Java va tenter d'utiliser.
<i>Mémoire libre (Mo)</i>	Quantité de mémoire (en mégaoctets) disponible sur la JVM pour l'allouer à de nouveaux objets.
<i>Mémoire totale (Mo)</i>	Mémoire totale en mégaoctets dans la machine virtuelle Java. Cette valeur peut varier au cours du temps selon l'environnement hôte.
<i>Pourcentage d'utilisation du processeur (les 5 dernières minutes)</i>	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.
<i>Pourcentage d'utilisation du processeur (les 15 dernières minutes)</i>	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.

Métrique	Description
<i>Pourcentage d'utilisation du système interrompu lors du GC (les 5 dernières minutes)</i>	<p>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.</p> <p>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.</p>
<i>Pourcentage d'utilisation du système interrompu lors du GC (les 15 dernières minutes)</i>	<p>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.</p> <p>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.</p>
<i>Nombre d'erreurs de page lors du GC (les 5 dernières minutes)</i>	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.
<i>Nombre d'erreurs de page lors du GC (les 15 dernières minutes)</i>	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.
<i>Nombre de GC complets</i>	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.
<i>Nombre de contentions de verrouillage de la JVM</i>	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.
<i>Informations de débogage de la JVM</i>	Informations de débogage sur la machine virtuelle Java SAP comprenant l'état, le port et éventuellement le client associé.
<i>Informations de version de la JVM</i>	Informations de version sur la machine virtuelle Java SAP.
<i>Nombre de threads bloqués de la JVM</i>	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.
<i>Indicateurs de trace JVM</i>	Les indicateurs de trace actuellement activés pour la JVM. Ceci indique le niveau de traçage de la JVM.
<i>Services</i>	Liste au format CSV des services hébergés par le serveur.

Table 231 : Métriques de service DSL Bridge

Métrique	Description
<i>DSLServiceMetrics.queryCount</i>	Nombre de requêtes de données ouvertes entre les clients et le service.

Métrique	Description
<i>DSLServiceMetrics.activeConnectionCount</i>	Nombre de connexions actuellement ouvertes entre les clients et le service.
<i>DSLServiceMetrics.activeSessionCount</i>	Nombre de sessions actuellement ouvertes entre les clients et le service.
<i>DSLServiceMetrics.activeOLAPConnectionCount</i>	Nombre de connexions actuellement ouvertes entre les clients OLAP et le service.

Table 232 : Métriques de service proxy d'audit client

Métrique	Description
<i>Nombre d'événements d'audit reçus depuis le démarrage du serveur</i>	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.

Table 233 : Métriques du service de recherche de plateformes

Métrique	Description
<i>Nombre de tentatives d'extraction réussies depuis le démarrage du service</i>	Nombre de tentatives réussies d'extraction des documents depuis le démarrage du service de recherche de plateformes.
<i>Horodatage de la dernière mise à jour de l'index</i>	Date et heure de la dernière mise à jour de l'index
<i>Horodatage de la dernière génération de stockage de contenus</i>	Date et heure de la génération du dernier stockage du contenu.
<i>Nombre de tentatives d'extraction échouées depuis le démarrage du service</i>	Nombre de tentatives échouées d'extraction des documents depuis le démarrage du service de recherche de plateformes.
<i>Service disponible</i>	TRUE si le service est disponible. Sinon, FALSE.
<i>Exécution de l'indexation</i>	TRUE si l'indexation est en cours d'exécution. Sinon, FALSE.
<i>Nombre de documents indexés</i>	Affiche le nombre de documents ayant été annexés depuis le démarrage du service.

Table 234 : Métriques du service MDAS (Multi-Dimensional Analysis Service)

Métrique	Description
<i>Nombre de sessions</i>	Nombre actuel de connexions entre les clients MDAS et le serveur.
<i>Nombre de cubes</i>	Nombre de sources utilisées pour fournir des données aux connexions n'ayant pas expiré.
<i>Nombre de requêtes</i>	Nombre de requêtes de données ouvertes entre les clients MDAS et le serveur.

Table 235 : Métriques du service de fédération de données

Métrique	Description
<i>Nombre de requêtes en cours d'exécution</i>	Nombre total de requêtes en cours (consommant ou non de la mémoire).
<i>Nombre de connexions</i>	Nombre total de connexions d'utilisateur au moteur de requête de fédération de données.
<i>Nombre total d'octets transférés des sources de données</i>	Volume des données lues à partir des sources de données (en octets).

Métrique	Description
<i>Nombre total d'enregistrements transférés des sources de données</i>	Nombre total de lignes lues à partir des sources de données.
<i>Nombre total d'octets produits par l'exécution de la requête</i>	Volume des données de sortie des requêtes (en octets).
<i>Nombre total d'enregistrements produits par l'exécution de la requête</i>	Nombre total de lignes de sortie des requêtes.
<i>Nombre de requêtes consommant de la mémoire</i>	Nombre de requêtes en cours consommant de la mémoire.
<i>Nombre total d'octets de mémoire utilisés par l'exécution de la requête</i>	Volume de mémoire actuellement utilisé par les requêtes en cours d'exécution (en octets).
<i>Nombre total d'octets du disque utilisés par l'exécution de la requête</i>	Volume du disque actuellement utilisé par les requêtes en cours d'exécution (en octets).
<i>Nombre de requêtes utilisant le disque</i>	Nombre total de requêtes en cours utilisant le disque.
<i>Nombre de requêtes en attente de ressources</i>	Nombre total de requêtes en cours en attente d'exécution
<i>Nombre de threads actifs</i>	Nombre total de threads actifs utilisés pour l'exécution des requêtes.
<i>Nombre total d'octets de mémoire utilisés par le cache des métadonnées</i>	Volume de mémoire utilisé pour la mise en cache de la configuration connecteurs, des métadonnées et des statistiques (en octets).
<i>Nombre d'échecs de requêtes</i>	Nombre total de requêtes échouées (exceptions survenues).
<i>Nombre de requêtes dans l'étape d'analyse des requêtes</i>	Nombre total de requêtes en cours d'exécution actuellement à l'étape d'analyse.
<i>Nombre de requêtes dans l'étape d'optimisation de la requête</i>	Nombre total de requêtes en cours actuellement à l'étape d'optimisation.
<i>Nombre de requêtes dans l'étape d'exécution de la requête</i>	Nombre total de requêtes en cours actuellement à l'étape d'exécution.
<i>Nombre de connecteurs chargés</i>	Nombre total de connecteurs chargés dans le service.
<i>Nombre de connexions actives aux connecteurs chargés</i>	Nombre total de connexions actives aux connecteurs chargés dans le service.
<i>Le service de fédération de données est disponible</i>	<i>TRUE</i> si le service est disponible. Sinon, <i>FALSE</i> .



Table 236 : Métriques du service de connectivité

Métrique	Description
<i>Sources de données</i>	<p>Répertorie dans un tableau les sources de données activées dans la page <a href="#">Propriétés</a>. Affiche les informations suivantes pour chaque couche réseau et paire de bases de données :</p> <ul style="list-style-type: none"> <li>Statut (« Chargé » ou « Echech ») : statut actuel du pilote</li> <li>Connexions disponibles : nombre de connexions pouvant être utilisées dans le pool</li> <li>Travaux (CORBA) : nombre de travaux en cours de traitement (déploiement à 2 niveaux)</li> <li>Travaux (HTTP) : nombre de travaux en cours de traitement (déploiement de niveau Web)</li> </ul> <p>Pour plus d'informations sur les pools de connexion, voir le <i>Guide d'accès aux données</i>.</p>

Table 237 : service de surveillance des métriques

Métrique	Description
<i>Durée moyenne de l'état de la veille pour les 15 derniers cycles (msec)</i>	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.
<i>Nombre de métriques créées par l'utilisateur</i>	Nombre total de métriques créées par l'utilisateur dans le cluster, pour tous les utilisateurs.
<i>Nombre de veilles</i>	Nombre total de veilles dans le cluster, y compris les veilles désactivées et activées.
<i>serviceBean.monitoringAppPropEnabled</i>	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.
<i>Intervalle d'actualisation des métriques de surveillance (en secondes)</i>	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.
<i>Service disponible</i>	TRUE si le service de surveillance est actif. Sinon, FALSE. Seul le service de surveillance est actif dans le cluster.
<i>Nombre de métriques de tendances</i>	Nombre total de métriques actuellement enregistrées dans la base de données de surveillance.

Table 238 : Métriques de service des applications Web BEx

Métrique	Description
<i>Nombre de sessions</i>	Nombre total de sessions actives dans le service des applications Web BEx.

## 31.1.7 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.

## **i** Remarque

Les serveurs conteneurs d'applications Web possèdent également toutes les métriques décrites à la section Métriques du serveur de traitement adaptatif.

Table 239 : Métriques de serveurs conteneurs d'applications Web

Métrique	Description
<i>Liste des connecteurs WACS en cours d'exécution</i>	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.
<i>Echecs des connecteurs WACS au démarrage</i>	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 [\[page 993\]](#)

## 31.1.8 Métriques d'Adaptative Job Server

Table 240 : Métriques de Job Server

Métrique	Description
<i>Demandes de travaux reçues</i>	Nombre de travaux supposés s'être exécutés sur le serveur.
<i>Travaux simultanés</i>	Nombre de travaux s'exécutant simultanément sur le serveur. Si ce nombre est élevé, le serveur est occupé.
<i>Nombre maximal de travaux</i>	Nombre maximal de travaux simultanés exécutés en même temps sur le serveur. Ce nombre ne diminue jamais jusqu'au redémarrage du serveur.
<i>Echecs de création de travaux</i>	Nombre de travaux ayant échoué sur le serveur.
<i>Répertoire temporaire</i>	Répertoire dans lequel les fichiers temporaires sont créés. Il peut être spécifié dans l'écran <i>Propriétés</i> du serveur.  Vous pouvez rencontrer des problèmes si ce répertoire ne dispose pas d'un espace disque suffisant.
<i>Paramètres par défaut valides pour la destination Système de fichiers</i>	<i>TRUE</i> si le serveur peut envoyer des documents à la destination Système de fichiers spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .
<i>Paramètres par défaut valides pour la destination FTP</i>	<i>TRUE</i> si le serveur peut envoyer des documents à la destination FTP spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .

Métrique	Description
<i>Paramètres par défaut valides pour la destination SFTP</i>	<i>TRUE</i> si le serveur peut envoyer des documents à la destination SFTP spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .  Vous pouvez rencontrer des problèmes si l'empreinte ne correspond pas exactement au serveur SFTP.
<i>Paramètres par défaut valides pour la destination boîte de réception</i>	<i>TRUE</i> si le serveur peut envoyer des documents à la destination boîte de réception spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .
<i>Paramètres par défaut valides pour la destination courrier électronique</i>	<i>TRUE</i> si le serveur peut envoyer des documents à la destination courrier électronique spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .
<i>Services de planification</i>	Tableau affichant les services en cours d'exécution sur le serveur.
<i>Enfants</i>	Tableau affichant les processus enfant en cours d'exécution sur le serveur.
<i>Paramètres par défaut valides pour la destination SAP StreamWork</i>	<i>TRUE</i> si le serveur peut envoyer des objets à la destination SAP StreamWork spécifiée dans l'écran <i>Destination</i> du serveur. Sinon, <i>FALSE</i> .

Le tableau suivant décrit les métriques de chaque service de planification en cours d'exécution sur le serveur.

Table 241 : Planification des métriques de service

Métrique	Description
<i>Service de planification</i>	Nom du service.
<i>Demandes de travaux reçues</i>	Nombre de travaux supposés s'être exécutés sur le service.
<i>Travaux simultanés</i>	Nombre de travaux simultanés s'exécutant simultanément sur le service. Si ce nombre est élevé, le service est occupé.
<i>Nombre maximal de travaux</i>	Nombre maximal de travaux simultanés exécutés en même temps sur le service.
<i>Nombre maximal de travaux simultanés autorisés</i>	Nombre de processus indépendants simultanés (processus enfant) autorisés par le service.  Il peut être spécifié dans l'écran <i>Propriétés</i> du serveur.
<i>Echecs de création de travaux</i>	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.

Table 242 : Métriques enfant

Métrique	Description
<i>Service de planification</i>	Nom du processus enfant.
<i>PID</i>	Identifiant du processus enfant.
<i>Demandes de travaux reçues</i>	Nombre de travaux supposés s'être exécutés sur le processus enfant.
<i>Travaux simultanés</i>	Nombre de travaux simultanés s'exécutant simultanément sur le processus enfant. Normalement, ce nombre doit être de « 1 ».
<i>Nombre maximal de travaux</i>	Nombre maximal de travaux simultanés exécutés en même temps sur le processus enfant.
<i>Nombre maximal de travaux autorisés</i>	Nombre de travaux simultanés autorisés par le processus enfant.

Métrique	Description
<i>Echecs de communication</i>	Nombre d'échecs de communication s'étant produits avec l'Adaptive Job Server. Si ce nombre est important, le processus enfant va redémarrer.
<i>Initialisation en cours</i>	<i>TRUE</i> si le processus enfant est en cours d'initialisation. Sinon, <i>FALSE</i> .
<i>Arrêt en cours</i>	<i>TRUE</i> si le processus enfant est en cours d'arrêt. Sinon, <i>FALSE</i> .

## 31.1.9 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 2013.

Table 243 : Métriques de Crystal Reports Processing Server

Métrique	Description
<i>Travaux en cours</i>	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.
<i>Nombre de requêtes servies</i>	Nombre total de requêtes servies par le serveur depuis son démarrage.
<i>Nombre de travaux en cours</i>	Nombre de travaux en cours que le serveur et ses processus enfant sont en train de traiter.
<i>Type d'objet</i>	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
<i>Durée de traitement moyenne (ms)</i>	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.
<i>Durée de traitement maximale (ms)</i>	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.
<i>Durée de traitement minimale (ms)</i>	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.
<i>Nombre de requêtes en attente</i>	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.
<i>Nom de la DLL de l'objet</i>	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
<i>Nombre de connexions ouvertes</i>	Nombre de connexions actuellement ouvertes entre le serveur et les clients.
<i>Taux d'échec des requêtes</i>	Nombre de requêtes que le serveur n'a pas pu traiter en tant que pourcentage des 500 dernières requêtes reçues par le serveur.
<i>Données transférées (Ko)</i>	Total des données (en kilo-octets) transmises aux clients depuis le démarrage du serveur.
<i>Nombre de requêtes ayant échoué</i>	Nombre de requêtes que le serveur n'a pas pu finaliser depuis son démarrage.

Métrique	Description
<i>Nombre maximal de processus enfant</i>	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.

Table 244 : Métriques de Crystal Reports Cache Server

Métrique	Description
<i>Taux d'accès à la mémoire cache (%)</i>	Pourcentage de requêtes sur les 500 dernières, qui ont été servies avec des données cachées.
<i>Serveurs de traitement connectés</i>	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.
<i>Nombre de requêtes servies</i>	Nombre total de requêtes servies par le serveur depuis son démarrage.
<i>Type d'objet</i>	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
<i>Durée de traitement moyenne (msec)</i>	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.
<i>Durée de traitement maximale (msec)</i>	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.
<i>Durée de traitement minimale (msec)</i>	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.
<i>Nombre de requêtes en attente</i>	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.
<i>Nom de la DLL de l'objet</i>	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
<i>Taille de la mémoire cache</i>	Volume de données (en kilo-octets) actuellement mises en cache par le serveur sur le disque.
<i>Nombre de connexions ouvertes</i>	Nombre de connexions actuellement ouvertes entre le serveur et les clients.
<i>Données transférées (Ko)</i>	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 2013.

Table 245 : Métriques du Report Application Server Crystal Reports 2013

Métrique	Description
<i>metric_currentdoccount</i>  <b>i Remarque</b> Cette métrique apparaît en tant que « document_s_ » sur la page de surveillance de la CMC.	Nombre de documents actuellement traités par le serveur.
<i>metric_totaldoccount</i>  <b>i Remarque</b> 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.
<i>metric_currentagentthreadcount</i>  <b>i Remarque</b> 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.
<i>metric_totalagentthreadcount</i>  <b>i Remarque</b> 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.

### 31.1.10 Métriques de Web Intelligence Server

Table 246 : Métriques du service de traitement Web Intelligence

Métrique	Description
<i>Cache size (Kb)</i> (Taille de la mémoire cache (Ko))	Volume actuel en kilo-octets de données stockées dans le cache.
<i>Number of out-of-date documents in cache</i> (Nombre maximum de documents dans le cache)	Nombre de documents supprimés du cache en raison de leur ancienneté depuis le démarrage du serveur.
<i>Cache high mark count</i> (Nombre de marques supérieures du cache)	Nombre de fois où le cache a atteint la taille maximale autorisée sur le serveur depuis son démarrage.
<i>CPU usage (%)</i> (Utilisation du processeur (%))	Pourcentage du temps processeur total utilisé par le serveur depuis son démarrage.

Métrique	Description
<i>Total CPU time (seconds)</i> (Temps total du processeur (secondes))	Temps processeur total utilisé par le serveur depuis son démarrage, exprimé en secondes.
<i>Memory high threshold count</i> (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.
<i>Memory max threshold count</i> (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.
<i>Virtual memory size (Mb)</i> (Taille de la mémoire virtuelle (Mo))	Volume total de la mémoire en mégaoctets affecté au serveur.
<i>Current number of client calls</i> (Nombre actuel d'appels client)	Nombre actuel d'appels CORBA traités par le serveur.
<i>Nombre d'erreurs d'extension distante</i>	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.
<i>Current number of tasks</i> (Nombre actuel de tâches)	Nombre actuel de tâches exécutées sur le serveur.
<i>Total number of client calls</i> (Nombre total d'appels client)	Nombre total d'appels CORBA reçus par le serveur depuis son démarrage.
<i>Total number of tasks</i> (Nombre total de tâches)	Nombre total de tâches exécutées sur le serveur depuis son démarrage.
<i>Délai d'inactivité (secondes)</i>	Temps écoulé, en secondes, depuis la dernière requête d'un client reçue par le serveur.
<i>Current number of active sessions</i> (Nombre actuel de sessions actives)	Nombre actuel de sessions pouvant accepter des requêtes de la part de clients.
<i>Nombre de documents ouverts à partir du cache</i>	Nombre de documents pour lesquels le dernier résultat de demande a été lu directement à partir du cache.
<i>Number of documents</i> (Nombre de documents)	Nombre de documents ouverts sur le serveur.
<i>Current number of sessions</i> (Nombre actuel de sessions)	Nombre actuel de sessions créées sur le serveur.
<i>Number of document swap</i> (Nombre de permutations de documents)	Nombre de documents pour lesquels un thread de nettoyage a planifié des requêtes de permutation.
<i>Number of swapped documents</i> (Nombre de documents permutés)	Nombre de documents permutés par des requêtes de permutation.
<i>Number of sessions timeout</i> (Nombre d'expirations de session)	Nombre de sessions ayant expiré depuis le démarrage du serveur.
<i>Total number of sessions</i> (Nombre total de sessions)	Nombre de sessions créées sur le serveur depuis son démarrage.
<i>Number of users</i> (Nombre d'utilisateurs)	Nombre total d'utilisateurs connectés au serveur.
<i>Nombre de threads actifs</i>	Nombre de demandes de prise en charge de threads reçues par le serveur (pool de threads asynchrone)
<i>Nombre total de threads</i>	Nombre total de threads ayant été créés depuis le démarrage du serveur (pool de threads asynchrone)

## 31.1.11 Métriques du serveur Dashboards

Table 247 : Métriques du serveur de traitement Dashboards

Métrique	Description
<i>Travaux en cours</i>	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.
<i>Nombre de requêtes servies</i>	Nombre total de requêtes servies par le serveur depuis son démarrage.
<i>Nombre de travaux en cours</i>	Nombre de travaux en cours que le serveur et ses processus enfant sont en train de traiter.
<i>Type d'objet</i>	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
<i>Durée de traitement moyenne (msec)</i>	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.
<i>Durée de traitement maximale (msec)</i>	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.
<i>Durée de traitement minimale (msec)</i>	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.
<i>Nombre de requêtes en attente</i>	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.
<i>Nom de la DLL de l'objet</i>	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
<i>Nombre de connexions ouvertes</i>	Nombre de connexions actuellement ouvertes entre le serveur et les clients.
<i>Taux d'échec des requêtes</i>	Nombre de requêtes que le serveur n'a pas pu traiter en tant que pourcentage des 500 dernières requêtes reçues par le serveur.
<i>Données transférées (Ko)</i>	Total des données (en kilo-octets) transmises aux clients depuis le démarrage du serveur.
<i>Nombre de requêtes ayant échoué</i>	Nombre de requêtes que le serveur n'a pas pu finaliser depuis son démarrage.
<i>Nombre maximal de processus enfant</i>	Nombre maximal de processus enfant simultanés autorisés sur le serveur.

Table 248 : Métriques de Cache Server

Métrique	Description
<i>Taux d'accès à la mémoire cache (%)</i>	Pourcentage de requêtes sur les 500 dernières, qui ont été servies avec des données cachées.
<i>Serveurs de traitement connectés</i>	Tableau répertoriant les serveurs de traitement Dashboards de votre déploiement. Ce tableau indique le nom du serveur et le nombre de connexions ouvertes avec le serveur.
<i>Nombre de requêtes servies</i>	Nombre total de requêtes servies par le serveur depuis son démarrage.



Métrique	Description
<i>Type d'objet</i>	Type d'InfoObject que le serveur traite en priorité. La valeur de cette métrique ne change pas.
<i>Durée de traitement moyenne (msec)</i>	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.
<i>Durée de traitement maximale (msec)</i>	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.
<i>Durée de traitement minimale (msec)</i>	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.
<i>Nombre de requêtes en attente</i>	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.
<i>Nom de la DLL de l'objet</i>	Nom du plug-in de traitement du serveur. La valeur de cette métrique ne change pas.
<i>Taille de la mémoire cache (Ko)</i>	Volume de données (en kilo-octets) actuellement mises en cache par le serveur sur le disque.
<i>Nombre de connexions ouvertes</i>	Nombre de connexions actuellement ouvertes avec les clients.
<i>Données transférées (Ko)</i>	Total des données (en kilo-octets) transmises aux clients depuis le démarrage du serveur.

## 32 Annexe relative aux espaces réservés de nœuds et de serveurs

### 32.1 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.

Table 249 : Espaces réservés

Espace réservé	Description	Valeurs par défaut
<code>%AuditingDatabaseConnection%</code>	Connexion à la base de données d'audit utilisée par le CMS.	Cette valeur est spécifiée lors de l'installation.
<code>%AuditingDatabaseDriver%</code>	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 <code>sqlserverauditdbss</code> .
<code>%BINDIR%</code>	Le dossier où les fichiers binaires 64 bits de la plateforme SAP BusinessObjects de Business Intelligence sont situés.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;plateforme&gt;/</code>
<code>%BINDIR32%</code>	Le dossier où les fichiers binaires 32 bits de la plateforme SAP BusinessObjects de Business Intelligence sont situés.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;plateforme&gt;/</code>
<code>%CACHESERVER_EXE%</code>	Nom du fichier exécutable du Crystal Reports Cache Server.	Sous Windows, <code>crcache.exe</code> . Sous UNIX, <code>boe_crcached.bin</code>
<code>%CMS_EXE%</code>	Nom du fichier exécutable du serveur Central Management Server.	Sous Windows, <code>cms.exe</code> . Sous UNIX, <code>boe_cmdsd</code> .
<code>%CONNECTIONSERVER32_EXE%</code>	Nom du fichier exécutable du serveur de connexion 32 bits.	Sous Windows, <code>ConnectionServer32.exe</code> . Sous UNIX, <code>ConnectionServer32</code> .
<code>%CONNECTIONSERVER_DIR%</code>	Dossier racine du serveur de connexion.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/dataAccess/connectionServer</code>

Espace réservé	Description	Valeurs par défaut
<code>%CONNECTIONSERVER_EXE%</code>	Nom du fichier exécutable du serveur de connexion 64 bits.	Sous Windows, <code>ConnectionServer.exe</code> . Sous UNIX, <code>ConnectionServer</code> .
<code>%CR2011_BINDIR%</code>	Répertoire dans lequel se trouvent les fichiers binaires du serveur Crystal Reports 2013.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjectsEnterprise XI 4.0\win32_x86</code> . Sous UNIX, le répertoire sera similaire à : <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9</code> .
<code>%CR2011_DefaultWorkingDir%</code>	Répertoire de travail par défaut des serveurs Crystal Reports 2013.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjectsEnterprise XI 4.0\win32_x86</code> . Sous UNIX, le répertoire sera semblable à : <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9</code> .
<code>%CRYSTALRAS_EXE%</code>	Nom du fichier exécutable du serveur Report Application Server.	Sous Windows, <code>crystalras.exe</code> . Sous UNIX, <code>boe_crystalrasd</code> .
<code>%CR_ODBCINI%</code>	Nom et chemin du fichier <code>.odbc.ini</code> .	Sous UNIX, <code>&lt;REPINSTALL&gt;/bobje/odbc.ini</code> . Sous Windows, il s'agit d'une chaîne vide.
<code>%CommonJavaBundlesDir%</code>	Dossier où se trouvent les packages OSGI partagés.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/java/lib/bundles</code> .
<code>%CommonJavaLibDir%</code>	Dossier où se trouvent les bibliothèques communes Java.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\java\lib</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/java/lib</code> .
<code>%DLLEX%</code>	Extension par défaut d'un fichier <code>.dll</code> ou <code>.so</code> .	Sous Windows, <code>.dll</code> . Sous UNIX, <code>.so</code> .
<code>%DLLPATH%</code>	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 ».

Espace réservé	Description	Valeurs par défaut
<a href="#">%DLLPATH32%</a>	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.
<a href="#">%DLLPATH64%</a>	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.
<a href="#">%DLLPREFIX%</a>	Préfixe par défaut d'un fichier .dll or .so.	Sous UNIX, « lib ». Cet espace réservé est une chaîne vide sur les ordinateurs Windows.
<a href="#">%DLLPRELOAD%</a>	Nom de la variable d'environnement LD_PRELOAD pour la plateforme.	Sous UNIX <a href="#">LD_PRELOAD</a> . Cet espace réservé est une chaîne vide sur les ordinateurs Windows.
<a href="#">%DLLPRELOAD32%</a>	Nom de la variable d'environnement LD_PRELOAD sur les systèmes AIX 32 bits.	Sous AIX, <a href="#">LDR_PRELOAD</a> . Cet espace réservé est une chaîne vide sur d'autres ordinateurs.
<a href="#">%DLLPRELOAD64%</a>	Nom de la variable d'environnement LD_PRELOAD sur les systèmes AIX 64 bits.	Sous AIX, <a href="#">LDR_PRELOAD64</a> . Cet espace réservé est une chaîne vide sur d'autres ordinateurs.
<a href="#">%DP%</a>	Délimiteur de chemin.	Sous Windows, « ; ». Sous UNIX, « : ».
<a href="#">%DefaultAuditingDir%</a>	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, <a href="#">&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\Auditing</a> . Sous UNIX, <a href="#">&lt;REPINSTALL&gt;/sap_bobj/data/Auditing/</a> .
<a href="#">%DefaultDataDir%</a>	Répertoire temporaire utilisé par le Job Server.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\Data</a> . Sous UNIX, <a href="#">&lt;REPINSTALL&gt;/sap_bobj/data</a> .
<a href="#">%DefaultInputFRSDir%</a>	Dossier racine du serveur Input File Repository Server.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input</a> . Sous UNIX, <a href="#">&lt;REPINSTALL&gt;/sap_bobj/data/frsinput</a> .

Espace réservé	Description	Valeurs par défaut
<code>%DefaultLoggingDir%</code>	Emplacement de stockage des fichiers journaux.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\logging</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/logging</code> .
<code>%DefaultOutputFRSDir%</code>	Dossier racine du serveur Output File Repository Server.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/data/frsoutput</code> .
<code>%DefaultWorkingDir%</code>	Répertoire de travail des serveurs 64 bits	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;plateforme&gt;</code> .
<code>%DefaultWorkingDir32%</code>	Répertoire de travail des serveurs 32 bits	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;plateforme&gt;</code> .
<code>%EPM_LD_PRELOAD_ONCE%</code>	Nom de la variable d'environnement LD_PRELOAD_ONCE pour la plateforme.	<code>\$LD_PRELOAD_ONCE\$</code>
<code>%EVENTSERVER_EXE%</code>	Nom du fichier exécutable du serveur Event Server.	Sous Windows, <code>EventServer.exe</code> . Sous UNIX, <code>boe_eventsd</code> .
<code>%EXEEXT%</code>	Extension par défaut des fichiers exécutables.	Sous Windows, <code>.exe</code> . Cet espace réservé n'est pas disponible sous UNIX.
<code>%EXEPATH%</code>	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 ».
<code>%EnterpriseDir%</code>	L'emplacement où la plateforme SAP BusinessObjects de Business Intelligence 64 bit est installée.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\.</code> Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/.</code>
<code>%EnterpriseDir32%</code>	L'emplacement où la plateforme SAP BusinessObjects de Business Intelligence 32 bits est installée.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\.</code> Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/.</code>

Espace réservé	Description	Valeurs par défaut
<code>%ExternalJavaLibDir%</code>	Dossier où se trouvent les bibliothèques Java tierces.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\java\lib\external</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/java/lib/external</code> .
<code>%FILESERVER_EXE%</code>	Nom du fichier exécutable du serveur de fichiers.	Sous Windows, <code>fileserv.exe</code> . Sous UNIX, <code>boe_filesd</code> .
<code>%HOARD_PATH%</code>	Emplacement du gestionnaire de mémoire.	Par défaut, cette valeur est vide.
<code>%HOARD_PRELOAD%</code>	Indique s'il faut précharger le gestionnaire de mémoire.	Par défaut, cette valeur est vide.
<code>%INSTALLROOTDIR%</code>	Dossier où est installée la plateforme SAP BusinessObjects Business Intelligence 64 bits.	Cette valeur est spécifiée lors de l'installation.
<code>%INSTALLROOTDIR32%</code>	Le dossier où la plateforme SAP BusinessObjects de Business Intelligence 32 bits est installée.	Cette valeur est spécifiée lors de l'installation.
<code>%IntroscopeAgentEnableInstrumentation%</code>	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.
<code>%IntroscopeAgentEnterpriseManagerHost%</code>	Nom d'hôte d'Introscope Agent Enterprise Manager vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
<code>%IntroscopeAgentEnterpriseManagerPort%</code>	Port d'Introscope Agent Enterprise Manager vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
<code>%IntroscopeAgentEnterpriseManagerTransport%</code>	Transport utilisé pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager. Les valeurs possibles sont : <ul style="list-style-type: none"> <li>• TCP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• SSL</li> </ul>	TCP
<code>%IntroscopeAgentEnterpriseManagerTransportHTTP%</code>	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via HTTP.	<code>com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory</code>
<code>%IntroscopeAgentEnterpriseManagerTransportHTTPS%</code>	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via HTTPS.	<code>com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory</code>

Espace réservé	Description	Valeurs par défaut
<code>%IntroscopeAgentEnterpriseManagerTransportSSL%</code>	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via SSL.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
<code>%IntroscopeAgentEnterpriseManagerTransportTCP%</code>	Classe utilisée pour envoyer les données d'instrumentation à Introscope Agent Enterprise Manager via TCP.	com.wily.isengard.postoffice-hub.link.net.DefaultSocketFactory
<code>%IntroscopeDir%</code>	Dossier où est installé Introscope Agent Enterprise Manager.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\java\wily.</code> Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/java/wily.</code>
<code>%JAWAW_EXE%</code>	Nom du fichier exécutable de la JVM sans fenêtre de console.	Sous Windows, <code>javaw.exe</code> . Sous UNIX, <code>java</code> .
<code>%JAVA_EXE%</code>	Nom du fichier exécutable de la JVM.	Sous Windows, <code>java.exe</code> . Sous UNIX, <code>java</code> .
<code>%JOBSEVERCHILD_EXE%</code>	Nom du fichier exécutable du serveur Adaptive Job Server Child.	Sous Windows, <code>JobServerChild.exe</code> . Sous UNIX, <code>boe_jobcd</code> .
<code>%JOBSEVER_EXE%</code>	Nom du fichier exécutable du serveur Adaptive Job Server.	Sous Windows, <code>JobServer.exe</code> . Sous UNIX, <code>boe_jobcd</code> .
<code>%JdkBinDir%</code>	Dossier où se trouvent les fichiers binaires JDK.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapvm\bin</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/&lt;PLATEFORME&gt;/sapvm/bin</code> .
<code>%JreBinDir%</code>	Dossier où se trouvent les fichiers binaires JRE.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapvm\jre\bin</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/&lt;PLATEFORME&gt;/sapvm/jre/bin</code> .
<code>%JVM_ARCH_ENVIRONMENT%</code>	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.
<code>%JVM_HEADLESS_MODE%</code>	Argument de la ligne de commande qui spécifie si la JVM travaille en mode headless (sans tête).	Sous Windows, <code>-Djava.awt.headless=false</code> . Sous UNIX, <code>-Djava.awt.headless=true</code>
<code>%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%</code>	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=%Default-LoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"

Espace réservé	Description	Valeurs par défaut
<a href="#">%JVM_SHARED_MEMORY_SEGMENT%</a>	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.
<a href="#">%LANGUAGEPACKSDIR%</a>	Dossier où sont installés les packs linguistiques du déploiement.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;</a> \SAP BusinessObjects Enterprise XI 4.0\Languages. Sous UNIX, <a href="#">&lt;REPINSTALL&gt;</a> /sap_bobj/enterprise_xi40/Languages/.
<a href="#">%LANGUAGEPACKSDIR32%</a>	Dossier où sont installés les packs linguistiques du déploiement sur des systèmes 32 bits.	. Sous Windows, <a href="#">&lt;REPINSTALL&gt;</a> \SAP BusinessObjects Enterprise XI 4.0\Languages. Sous UNIX, <a href="#">&lt;REPINSTALL&gt;</a> /sap_bobj/enterprise_xi40/Languages/.
<a href="#">%LSTDir%</a>	Dossier où sont stockés les fichiers de configuration LST.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;</a> \SAP BusinessObjects Enterprise XI 4.0\conf\lst. Sous UNIX, <a href="#">&lt;REPINSTALL&gt;</a> /sap_bobj/enterprise_xi40/conf/lst.
<a href="#">%MDAS_JVM_OS_STACK_SIZE%</a>	Spécifie la taille de pile de la JVM pour le service d'analyse multidimensionnelle.	Par défaut, cet espace réservé est vide.
<a href="#">%NCSInstrumentLevelThreshold%</a>	Niveau de seuil de la journalisation d'événements de la bibliothèque NCS.	La valeur par défaut est 0.
<a href="#">%PAGESERVER_EXE%</a>	Nom du fichier exécutable du serveur de traitement Crystal Reports 2013.	Sous Windows, crproc.exe. Sous UNIX, boe_crprocd.bin.
<a href="#">%PJSContainerDir%</a>	Dossier où se trouvent les fichiers JAR de conteneur de serveur de traitement adaptatif.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;</a> \SAP BusinessObjects Enterprise XI 4.0\java\pjs\container. Sous UNIX, <a href="#">&lt;REPINSTALL&gt;</a> /sap_bobj/enterprise_xi40/java/pjs/container.
<a href="#">%PJSServicesDir%</a>	Dossier où se trouvent les fichiers JAR de service de serveur de traitement adaptatif.	Sous Windows, <a href="#">&lt;REPINSTALL&gt;</a> \SAP BusinessObjects Enterprise XI 4.0\java\pjs\services. Sous UNIX, <a href="#">&lt;REPINSTALL&gt;</a> /sap_bobj/enterprise_xi40/java/pjs/services.
<a href="#">%Platform%</a>	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.



Espace réservé	Description	Valeurs par défaut
<code>%Platform32%</code>	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.
<code>%RasBinDir%</code>	Dossier racine du serveur Report Application Server.	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/&lt;PLATFEORME&gt;/ras</code> .
<code>%NOM_CONVIVIAL_SERVEUR%</code>	Nom complet du serveur.	Nom complet du serveur.
<code>%NOM_SERVEUR%</code>	Nom complet du serveur.	Nom complet du serveur.
<code>%SMDAgentHost%</code>	Nom d'hôte SMD Agent vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
<code>%SMDAgentPort%</code>	Port SMD Agent vers lequel les données d'instrumentation sont envoyées.	Cette valeur est spécifiée lors de l'installation.
<code>%TRACE_CONFIGFILE_INI%</code>	Nom et chemin d'accès au fichier <code>BO_Trace.ini</code> .	Sous Windows, <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/conf/BO-trace.ini</code> .
<code>%WarFilesDir%</code>	L'emplacement des fichiers d'applications Web.	Sous Windows <code>&lt;REPINSTALL&gt;\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps</code> . Sous UNIX, <code>&lt;REPINSTALL&gt;/sap_bobj/enterprise_xi40/warfiles/webapps</code> .
<code>%WEBI_LD_PRELOAD%</code>	Nom de la variable d'environnement <code>LD_PRELOAD</code> pour la plateforme.	<code>\$LD_PRELOAD\$</code>
<code>%WEBISERVER_EXE%</code>	Nom du fichier exécutable du Web Intelligence Processing Server.	Sous Windows, <code>wireportserver.exe</code> . Sous UNIX, <code>WIReportServer</code> .
<code>%WEBI_LD_PRELOAD_ONCE%</code>	Nom de la variable d'environnement <code>LD_PRELOAD_ONCE</code> pour la plateforme.	<code>\$LD_PRELOAD_ONCE\$</code>
<code>%XCCACHE_EXE%</code>	Nom du fichier exécutable du serveur Cache Server des tableaux de bord.	Sous Windows, <code>xccache.exe</code> . Sous UNIX, <code>boe_xccached</code> .
<code>%XCPROC_EXE%</code>	Nom du fichier exécutable du serveur de traitement Dashboards.	Sous Windows, <code>xcproc.exe</code> . Sous UNIX, <code>boe_xcprocd</code> .

## **i** 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%`

## Informations associées

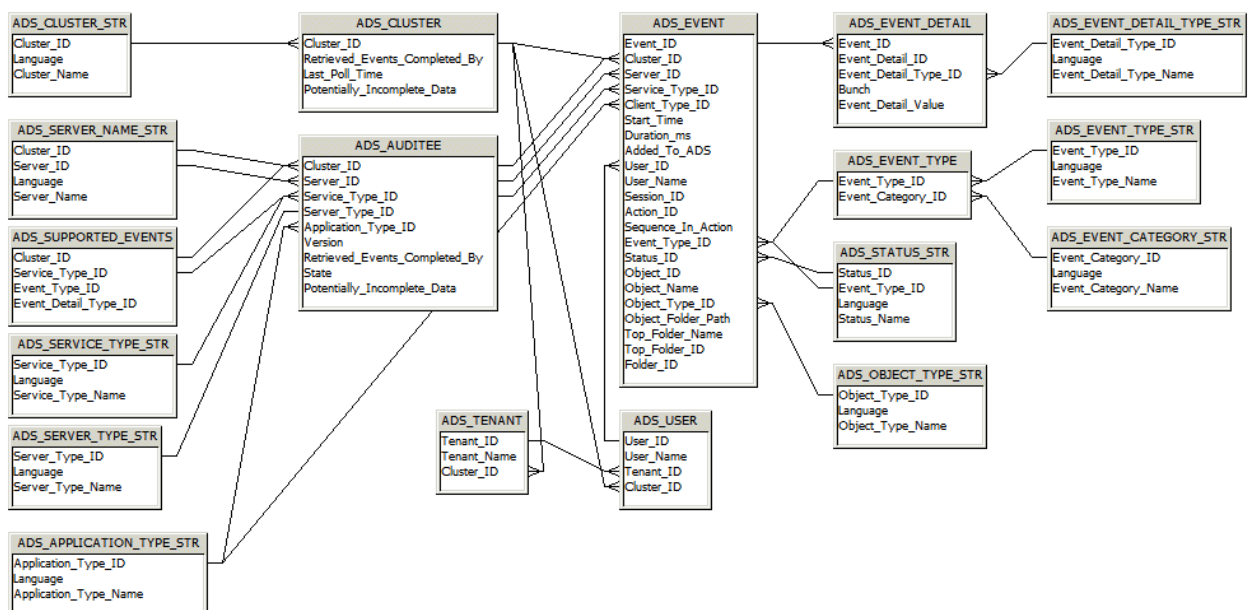
[Visualisation et modification des espaces réservés d'un nœud \[page 435\]](#)

## 33 Annexe relative au schéma de magasin de données d'audit

### 33.1 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.

### 33.2 Diagramme de schéma



### 33.3 Tables du magasin de données d'audit

#### Table ADS\_APPLICATION\_TYPE\_STR

Cette table fournit un dictionnaire multilingue des noms de types d'application client.

Table 250 :

Nom de colonne	Type	Description
Application_Type_ID	Caractère (64)	CUID du type d'application de l'application.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le type d'application ; par exemple, <EN> ou <DE>.
Application_Type_Name	Caractère (255)	Nom du texte du type d'application ; Crystal Reports ou Web Intelligence, par exemple.

## Table ADS\_AUDITEE

Cette table enregistre des informations de propriétés pour tous les serveurs de candidats à l'audit dans le cadre du déploiement.

Table 251 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster auquel appartient le candidat à l'audit.
Server_ID	Caractère (64)	CUID du serveur ayant déclenché l'événement. Si l'événement est déclenché par le client, il enregistre le CUID du serveur de traitement adaptatif ayant traité l'événement.
Service_Type_ID	Caractère (64)	CUID de type de service du service ayant déclenché l'événement. Les événements déclenchés par le client enregistrent un CUID de type d'application.
Server_Type_ID	Caractère (64)	CUID de type de serveur du serveur ayant déclenché l'événement.
Application_Type_ID	Caractère (64)	CUID de type d'application du client ayant déclenché l'événement. Dans le cas des événements de serveur, l'ID du type de service est enregistré.
Version	Caractère (64)	Version du serveur ou du client ayant déclenché l'événement au moment où il était enregistré.
Retrieved_Events_Completed_By	Datetime	Dernière interrogation du CMS de l'auditeur par le candidat quant à ses fichiers temporaires. Cela indique que tous les événements de ce candidat à l'audit terminés avant cette date ou heure se trouvent dans le magasin de données d'audit.
Etat	INTEGER	Etat (En cours d'exécution, Non exécuté, Supprimé) dans lequel se trouvait le candidat à l'audit.
Potentially_Incomplete_Data	INTEGER	Indique si le candidat à l'audit peut avoir des événements qui n'auraient pas été transférés au magasin de données d'audit.

## Table ADS\_CLUSTER

Cette table enregistre les informations relatives aux clusters contenant les candidats à l'audit.

Table 252 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster.
Retrieved_Events_Completed_By	Datetime	Indique dans quelle mesure les informations d'audit de la base de données concernant ce cluster sont actuelles. Enregistre le plus ancien horodatage d'audit extrait pour tous les serveurs de candidats à l'audit en cours d'exécution à tout moment. Cela indique que tous les événements terminés avant cette date se trouvent dans le magasin de données d'audit.
Last_Poll_Time	Datetime	Dernière interrogation du CMS de l'auditeur par les candidats à l'audit de ce cluster.
Potentially_Incomplete_Data	INTEGER	Indique les informations d'audit potentiellement incomplètes dans le cluster : "0" = tous les serveurs ont transmis les données normalement ; "1" = au moins un serveur en cours d'exécution ou non exécuté dans le cluster a un indicateur défini sur <a href="#">Potentially_Incomplete_Data</a> , signifiant que des événements d'un candidat à l'audit n'ont pas été transférés au magasin de données d'audit.

## Table ADS\_CLUSTER\_STR

Cette table fournit un enregistrement de référence des différents clusters dans votre déploiement.

Table 253 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	ID unique du cluster.
Langue	Caractère (10)	Code du paramètre de langue du cluster ; par exemple, <EN> ou <DE>.
Cluster_Name	Caractère (255)	Nom du cluster.

## Table ADS\_EVENT

Cette table enregistre les propriétés de base de chaque événement, elle représente le point de liaison central pour d'autres tables du schéma.

Table 254 :

Nom de colonne	Type	Description
Event_ID	Caractère (64)	ID unique généré pour l'événement.
Cluster_ID	Caractère (64)	GUID du cluster du candidat à l'audit. Il est enregistré car plusieurs clusters peuvent utiliser le même magasin de données d'audit.
Server_ID	Caractère (64)	CUID du serveur ayant déclenché l'événement.

Nom de colonne	Type	Description
Service_Type_ID	Caractère (64)	<ul style="list-style-type: none"> <li>• CUID du type de serveur ayant déclenché l'événement. Les services d'un serveur enregistreront leur CUID de type de service.</li> <li>• Les applications client (zone de lancement BI ou Web Intelligence, par exemple) enregistreront leur CUID de type d'application.</li> </ul>
Client_Type_ID	Caractère (64)	Enregistre l'ID du type de client du client qui a établi la session.
Start_Time	Datetime	Date et heure (UTC) auxquelles l'opération a débuté (y compris les millisecondes).
Duration_ms	INTEGER	Durée de l'opération en millisecondes.
Added_to_ADS	Datetime	Date et heure (UTC) auxquelles l'événement a été enregistré dans le magasin de données d'audit.
User_ID	Caractère (64)	CUID de la personne qui a effectué l'action.
User_Name	Caractère (255)	Nom associé à l'ID de la personne qui a effectué l'action. Enregistré dans la langue par défaut du CMS de l'auditeur.
Session_ID	Caractère (64)	GUID de la session durant laquelle l'événement a été déclenché. En l'absence de session associée, le champ est nul.
Action_ID	Caractère (64)	ID de l'action utilisateur ayant déclenché l'événement. Utilisé pour grouper les événements résultant d'une unique action utilisateur.
Sequence_In_Action	INTEGER	Serveur ou application client dans la séquence ayant déclenché l'événement dans le cas d'événements multi-serveurs (ou client et multi-serveur). Dans tous les workflows de planification, l'ID de séquence sera toujours 0.
Event_Type_ID	INTEGER	Type d'événement (Visualiser ou Enregistrer, par exemple).
Status_ID	INTEGER	Statut de l'opération (par exemple, "0" = réussite, "1" = échec).
Object_ID	Caractère (64)	CUID de l'objet sur lequel a été effectuée l'opération.
Object_Name	Caractère (255)	Nom de l'objet sur lequel a été effectuée l'opération. Enregistré dans la langue par défaut du CMS de l'auditeur.
Object_Type_ID	Caractère (64)	CUID du type d'objet sur lequel a été effectuée l'opération.
Object_Folder_Path	Caractère (255)	Chemin complet du dossier (par exemple Pays/Région/Ville) de l'objet sur lequel a été effectuée l'opération. Enregistré dans la langue par défaut du CMS de l'auditeur. Si le chemin du dossier ne peut pas être déterminé, cette valeur sera nulle.
Folder_ID	Caractère (64)	CUID du dossier de l'objet sur lequel a été effectuée l'opération.
Top_Folder_Name	Caractère (255)	Nom du dossier de niveau supérieur de l'objet. Par exemple, si l'objet est situé dans Pays/Région/Ville, Pays sera enregistré.
Top_Folder_ID	Caractère (64)	CUID du dossier de niveau supérieur où se trouve l'objet. Par exemple, si l'objet est situé dans Pays/Région/Ville, le CUID du dossier Pays sera alors enregistré.

## Table ADS\_EVENT\_CATEGORY\_STR

Cette table fournit un dictionnaire multilingue des noms de catégories d'événement.

Table 255 :

Nom de colonne	Type	Description
Event_Category_ID	INTEGER	ID de catégorie d'événement.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le nom de catégorie d'événement ; par exemple, <EN> ou <DE>.
Event_Category_Name	Caractère (255)	Nom de la catégorie d'événement.

## ADS\_EVENT\_DELETES

N'utilisez pas cette table et ne créez pas de rapport à partir de celle-ci. Elle est destinée à être utilisée par le système et pourrait être supprimée lors de versions futures.

## Table ADS\_EVENT\_DETAIL

Cette table enregistre les propriétés de détail d'événement.

Table 256 :

Nom de colonne	Type	Description
Event_Detail_ID	INTEGER	GUID du détail d'événement.
Event_ID	Caractère (64)	GUID d'événement parent.
Event_Detail_Type_ID	INTEGER	Type de détail d'événement.
Tas	INTEGER	<p>Si le détail fait partie d'une série, il est utilisé pour les lier ensemble.</p> <p>Par exemple, si un rapport comporte des invites pour Etat et Pays, un utilisateur peut saisir "Etats-Unis" pour l'invite Pays et "Californie" et "Nevada" pour l'invite Etat. Cela produirait des détails d'événement avec deux tas. Le tas 1 consisterait en :</p> <ul style="list-style-type: none"><li>• Nom de l'invite : Pays</li><li>• Valeur de l'invite . Etats-Unis</li></ul> <p>Le tas 2 consisterait en :</p> <ul style="list-style-type: none"><li>• Nom de l'invite : Etat</li><li>• Valeur de l'invite . Californie</li><li>• Valeur de l'invite . Nevada</li></ul>
Event_Detail_Value	Caractère (texte long)	Valeur du détail d'événement.

## Table ADS\_EVENT\_DETAIL\_TYPE\_STR

Cette table fournit un dictionnaire multilingue des noms de types de détail.

Table 257 :

Nom de colonne	Type	Description
Event_Detail_ID	INTEGER	ID du type de détail d'événement du détail d'événement.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le nom de détail d'événement ; par exemple, <EN> ou <DE>.
Event_Detail_Type_Name	Caractère (255)	Nom du texte du type de détail de l'événement.

## Table ADS\_EVENT\_TYPE

Cette table fournit un enregistrement de référence des différentes catégories d'événement.

Table 258 :

Nom de colonne	Type	Description
Event_Type_ID	INTEGER	Identifiant unique du type d'événement.
Event_Category_ID	INTEGER	Catégorie d'événement. Par exemple, commun, Web Intelligence ou Gestion du cycle de vie.

## Table ADS\_EVENT\_TYPE\_STR

Cette table fournit un dictionnaire multilingue des noms de types d'événement.

Table 259 :

Nom de colonne	Type	Description
Event_Type_ID	INTEGER	ID du type d'événement de l'événement.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le nom de catégorie d'événement ; par exemple, <EN> ou <DE>.
Event_Type_Name	Caractère (255)	Nom du texte du type d'événement ; Visualiser ou Se connecter, par exemple.

## Table ADS\_OBJECT\_TYPE\_STR

Cette table fournit un dictionnaire multilingue des noms d'objets d'événement.



Table 260 :

Nom de colonne	Type	Description
Object_Type_ID	Caractère (64)	CUID du type d'objet de l'objet.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le nom du type d'objet ; par exemple, <EN> ou <DE>.
Object_Type_Name	Caractère (255)	Nom du type d'objet.

## Table ADS\_SERVER\_NAME\_STR

Cette table fournit un dictionnaire multilingue des noms de serveurs. Les valeurs seront mises à jour lorsque seront renommés les serveurs.

Table 261 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster auquel appartient le serveur.
Server_ID	Caractère (64)	CUID du serveur.
Langue	Caractère (10)	Code de la langue du nom de serveur ; par exemple, <EN> ou <DE>.
Server_Name	Caractère (255)	Nom du serveur.

## Table ADS\_SERVICE\_TYPE\_STR

Cette table fournit un dictionnaire multilingue des noms de types de service.

Table 262 :

Nom de colonne	Type	Description
Service_Type_ID	Caractère (64)	CUID du type de service ou de la catégorie de service du service.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le nom du type de service ; par exemple, <EN> ou <DE>.
Service_Type_Name	Caractère (255)	Nom du type de service.

## Table ADS\_STATUS\_STR

Cette table fournit un dictionnaire multilingue des noms de statuts d'événement.

Table 263 :

Nom de colonne	Type	Description
Status_ID	INTEGER	Représentation numérique du statut de l'opération.
Event_Type_ID	INTEGER	ID du type d'événement de l'événement. Par exemple, 1002 pour Visualiser.
Langue	Caractère (10)	Code de la langue dans laquelle est enregistré le statut de l'événement ; par exemple, <EN> ou <DE>.
Status_Name	Caractère (255)	Une description de texte du statut de l'événement ; Succès ou Echec, par exemple.

## Table ADS\_SUPPORTED\_EVENTS

Ce tableau enregistre une liste des événements pris en charge et des détails d'événement associés pour chaque type de service ou d'application client.

Table 264 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster auquel appartient le service.
Service_Type_ID	Caractère (64)	CUID de type de service du service ayant déclenché l'événement. Si l'événement est déclenché par une application client, un CUID de type d'application est alors enregistré.
Event_Type_ID	INTEGER	ID du type d'événement enregistré (ID de Enregistrer, par exemple).
Event_Detail_Type_ID	INTEGER	CUID identifiant le type de détail d'événement capturé pour cet événement (Chemin de fichier, par exemple).

## Table ADS\_TENANT

Cette table enregistre les relations entre les noms et les ID de client

Table 265 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster.
Tenant_ID	Caractère (64)	CUID du client.
Tenant_Name	Caractère (255)	Nom du client

## Table ADS\_USER

Cette table enregistre les relations entre les utilisateurs et les clients.

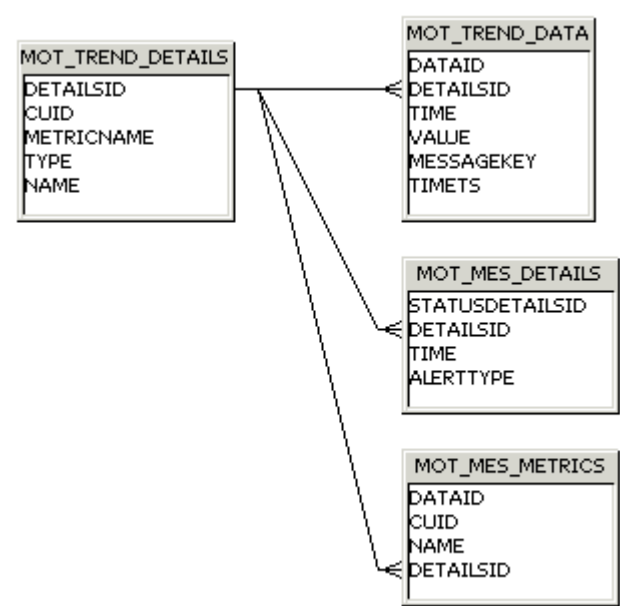
Table 266 :

Nom de colonne	Type	Description
Cluster_ID	Caractère (64)	GUID du cluster.
User_ID	Caractère (64)	CUID de l'utilisateur.
User_Name	Caractère (255)	Nom de l'utilisateur.
Tenant_ID	Caractère (64)	CUID du client.

# 34 Annexe relative au schéma de la base de données de surveillance

## 34.1 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.

Table 267 :

Nom de colonne	Type	Clé	Description
DetailsId	INTEGER	Clé primaire Générée automati- quement	
CUID	VARCHAR(64)	NA	CUID de l'InfoObject qui expose la métrique ou y est associé
MetricName	VARCHAR(255)	NA	Nom de la métrique

Nom de colonne	Type	Clé	Description
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.

Table 268 :

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 TIMESTAMPTZ	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.

Table 269 :

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.

Table 270 :

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

## 35 Annexe relative à la feuille de calcul Copie du système

### 35.1 Feuille de calcul Copie du système

Table 271 :

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

## Exemples de code source

Le code et les lignes ou chaînes de code ("Code") inclus dans la présente documentation ne sont que des exemples et ne doivent en aucun cas être utilisés dans un environnement productif. Le Code est utilisé uniquement pour mieux expliquer et visualiser les règles de syntaxe de certains codages. SAP ne sera pas tenu responsable des erreurs ou dommages causés par l'utilisation de ce Code, sauf si de tels dommages étaient causés par SAP intentionnellement ou par négligence grave.

## Accessibilité

Les informations contenues dans la documentation SAP représentent la vision actuelle de SAP concernant les critères d'accessibilité, à la date de publication de ladite documentation, et ne peuvent en aucun cas être considérées comme juridiquement contraignantes pour garantir l'accessibilité aux produits logiciels. SAP décline toute responsabilité pour le présent document. Cette clause de non-responsabilité ne s'applique toutefois pas à des cas de faute intentionnelle ou lourde de la part de SAP. En outre, ce document n'entraîne pas des obligations contractuelles directes ou indirectes pour SAP.

## Langage non discriminatoire

Dans la mesure du possible, la documentation SAP est non discriminatoire au titre du genre féminin ou masculin. Selon le contexte, le texte s'adresse au lecteur en utilisant le pronom "vous" ou un substantif neutre (tel que "commercial" ou "jour ouvrable"). Lorsque le texte se réfère à des hommes et des femmes, que la troisième personne du singulier ne peut pas être évitée ou qu'un substantif neutre n'existe pas, SAP se réserve le droit d'utiliser la forme masculine du nom ou du pronom. Ceci permet d'assurer la bonne compréhension de la documentation.

## Hyperliens Internet

La documentation SAP peut contenir des hyperliens vers Internet. Lesdits hyperliens sont utilisés pour indiquer où trouver l'information. SAP ne garantit pas la disponibilité et l'exactitude des informations ou leur capacité à répondre à un but précis. SAP ne saurait être tenu responsable des dommages causés par l'utilisation desdites informations sauf si de tels dommages étaient causés par une négligence grave ou une faute intentionnelle de SAP. Tous les liens sont catégorisés pour transparence (voir : <http://help.sap.com/disclaimer>).





[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2015 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.

Pour plus d'informations sur les marques déposées, voir <http://www.sap.com/corporate-en/legal/copyright/index.epx>.