PUBLIC (OPENBAAR)

SAP BusinessObjects Business Intelligence-platform

Documentversie: 4.3 Support Package 4 – 2023-12-07

Beheerdershandleiding voor Business Intelligence-platform

© 2024 SAP SE of een aan SAP gelieerde onderneming. Alle rechten voorbehouden.

THE BEST RUN SAP

Inhoud

1 Documentgeschiedenis. 21

2 Aan de slag. 22

2.1 Over deze handleiding. 22

Voor wie is deze handleiding bedoeld?. 22

Het Business Intelligence-platform. 22

Variabelen. 23

Terminologie. 23

2.2 Voordat u begint. 25

Sleutelconcepten. 25

Belangrijkste beheerhulpprogramma's. 28

Belangrijkste taken. 31

3 Architectuur. 34

3.1 Overzicht architectuur. 34

Onderdeeldiagram. 35

Architectuurlagen. 36

Databases. 37

Servers, hosts en clusters. 38

Webtoepassingsservers. 39

Software Development Kits. 44

Gegevensbronnen. 46

Verificatie en eenmalige aanmelding. 46

SAP-integratie. 48

Geïntegreerde versiecontrole. 49

3.2 Servers, services, knooppunten en hosts. 49

Serverwijzigingen sinds XI 3.1. 51

Services. 53

Servicecategorieën. 59

Servertypen. 62

Servers. 65

3.3 Clienttoepassingen. 67

Geïnstalleerd met Clienthulpprogramma's van SAP BusinessObjects Business Intelligence-platform. 68

Geïnstalleerd met SAP BusinessObjects Business Intelligence-platform. 70

Apart verkrijgbaar. 71

Webtoepassingsclients. 72

3.4 Proceswerkstromen. . . . 75
Opstarten en verificatie. . . . 75
Programmaobjecten. . . . 77
Crystal Reports. . . . 78
Web Intelligence. . . . 82
Analyse. . . . 85
3.5 Integratie met launchpad voor SAP Fiori op SAP Enterprise Portal. . . . 86

4 Wizard Systeemconfiguratie. . . . 87
4.1 Inleiding tot de wizard Systeemconfiguratie. . . . 87
4.2 De producten opgeven die u gebruikt. . . . 87
4.3 Een implementatiesjabloon kiezen. . . . 89
4.4 Locaties voor gegevensmappen opgeven. . . . 91
4.5 Uw wijzigingen controleren. . . . 92
4.6 Logboekbestanden en antwoordbestanden. . . . 93
Een antwoordbestand gebruiken. . . . 93

5 Licenties beheren. . . . 97
5.1 Licentiesleutels beheren. . . . 97
Licentiegegevens weergeven. . . . 97
Een licentiesleutel toevoegen. . . . 97
De huidige accountactiviteit weergeven. . . . 98

6 Gebruikers en groepen beheren. . . . 99
6.1 Overzicht van accountbeheer. . . . 99
Gebruikersbeheer. . . . 99
Groepsbeheer. . . . 100
Beschikbare verificatietypen. . . . 101
6.2 Enterprise-accounts en algemene accounts beheren. . . . 102
Een gebruikersaccount maken. . . . 102
Een gebruikersaccount wijzigen. . . . 103
Een gebruikersaccount verwijderen. . . . 104
Een nieuwe groep maken. . . . 104
De eigenschappen van een groep wijzigen. . . . 105
De leden van een groep weergeven. . . . 105
Subgroepen toevoegen. . . . 106
Groepslidmaatschap opgeven. . . . 106
Een groep verwijderen. . . . 107
Gebruikers of gebruikersgroepen bulksgewijs toevoegen. . . . 107
De Guest-account inschakelen. . . . 108
Gebruikers toevoegen aan groepen. . . . 108
Wachtwoordinstellingen wijzigen. . . . 110

Toegang verlenen aan gebruikers en groepen. 112
Toegang verlenen tot het Postvak IN van gebruikers. 112
Fiorified-BI-startpuntopties configureren. 112
Attributen voor systeemgebruikers beheren 116
Prioriteit toekennen aan gebruikersattributen tussen meerdere verificatie-opties. 117
Een nieuw gebruikersattribuut toevoegen. 117
Aangepaste gebruikersattributen bewerken. 119
6.3 Aliassen beheren. 119
Een gebruiker maken en een externe alias toevoegen. 119
Een nieuwe alias maken voor een bestaande gebruiker. 120
Een alias van een andere gebruiker toewijzen. 121
Een alias verwijderen. 121
Een alias uitschakelen. 122

7 Rechten instellen. 123
7.1 Werking van rechten in BI-platform. 123
Toegangsniveaus. 123
Geavanceerde instellingen voor rechten. 124
Overname. 125
Typespecifieke rechten. 130
Effectieve rechten bepalen. 131
7.2 Beveiligingsinstellingen voor objecten beheren in de CMC. 132
De rechten van een principal voor een object weergeven. 132
Principals toewijzen aan de ACL van een object. 133
De beveiliging van een object wijzigen voor een principal. 133
Rechten voor een map op het bovenste niveau instellen in het BI-platform. 134
Beveiligingsinstellingen voor een principal controleren.. 135
7.3 Werken met toegangsniveaus. 137
Kiezen tussen het toegangsniveau *Weergeven* en *Weergeven op aanvraag*. 139
Een bestaand toegangsniveau kopiëren. 140
Een nieuw toegangsniveau maken. 140
De naam van een toegangsniveau wijzigen. 141
Een toegangsniveau verwijderen. 141
De rechten in een toegangsniveau wijzigen. 141
De relatie tussen toegangsniveaus en objecten traceren. 142
Toegangsniveaus beheren op meerdere locaties. 143
7.4 Overname uitschakelen. 144
Overname uitschakelen. 145
7.5 Beheer delegeren met rechten. 146
Kiezen tussen de opties voor “*Rechten van gebruikers voor objecten wijzigen*”. 147
Eigendomsrechten. 149
7.6 Aanbevelingen voor rechtenbeheer. 149

8 Het BI-platform beveiligen. 151
8.1 Overzicht van beveiliging 151
8.2 Veilig gebruik van programmaobjecten. 151
8.3 Planning van herstel na uitval. 152
8.4 Algemene aanbevelingen voor beveiliging van uw implementatie. 153
8.5 Beveiliging configureren voor gebundelde externe servers. 154
8.6 Actieve vertrouwensrelatie. 154
Aanmeldingstokens. 154
Ticketmechanisme voor gedistribueerde beveiliging. 155
8.7 Sessies en het bijhouden van sessies. 155
Sessies bijhouden op de CMS. 156
Sessies beheren. 156
Script voor het wissen van verouderde sessies. 158
8.8 Omgevingsbeveiliging. 158
Webbrowser naar webserver. 158
Webserver naar BI-platform. 159
Bescherming tegen aanmeldingspogingen van kwaadwillende gebruikers. 159
Wachtwoordbeperkingen. 159
Aanmeldingsbeperkingen. 160
Gebruikersbeperkingen. 160
Beperkingen voor de Guest-account. 160
8.9 Wijzigingen in de beveiligingsconfiguratie controleren 161
8.10 Uitbreidingsmodules. 161
8.11 Virusscaninterface. 161
Virusscan inschakelen. 162
8.12 Gegevensbeveiliging op het BI-platform. 163
Beveiligingsmodi voor gegevensverwerking. 163
Beheerdersaccounts. 165
Verbindingsrechten. 165
8.13 Cryptografie in het BI-platform. 166
Met clustersleutels werken. 167
Cryptografie-operators. 169
Cryptografiesleutels beheren in de CMC. 171
8.14 Gegevensbeveiliging en privacy. 175
Woordenlijst. 176
Gebruikerstoestemming. 177
Informatierapport. 178
Verslaglegging van leestoegang. 178
Verwijderen van persoonlijke gegevens. 179
Wijzigingsverslag. 180
8.15 Back-endservers configureren voor SSL. 181

Het standaardconfiguratiebestand maken. 181
Key- en certificaatbestanden maken. 182
SSL instellen wanneer het certificaat wordt beheerd door een certificeringsinstantie. 184
Het SSL-protocol configureren. 186
8.16 Communicatie tussen BI-platformonderdelen begrijpen. 191
Overzicht van BI-platformservers en communicatiepoorten. 191
Communicatie tussen BI-platformonderdelen 193
8.17 Het BI-platform voor firewalls configureren. 204
Het systeem configureren voor firewalls. 204
Fouten opsporen in een implementatie met firewalls. 207
8.18 Voorbeelden van veelvoorkomende scenario's met firewalls. 208
Voorbeeld: de toepassingslaag bevindt zich op een afzonderlijk netwerk.. 209
Voorbeeld: thick client en databaselaag door firewall gescheiden van BI-platformservers. 211
8.19 Firewallinstellingen voor geïntegreerde omgevingen. 213
Specifieke firewallrichtlijnen voor SAP-integratie. 214
Firewall-configuratie voor JD Edwards EnterpriseOne-integratie. 215
Specifieke firewallrichtlijnen voor Oracle EBS. 216
Firewall-configuratie voor PeopleSoft Enterprise-integratie. 217
Firewall-configuratie voor Siebel-integratie. 218
8.20 Het BI-platform en omgekeerde proxyservers 220
Inzicht in de implementatie van webtoepassingen. 220
8.21 Omgekeerde proxyserver configureren voor webtoepassingen van BI-platform. 221
Gedetailleerde instructies voor de configuratie van omgekeerde proxyservers. 221
De omgekeerde proxyserver configureren. 222
De reverse-proxyserver van Apache 2.2 configureren voor het BI-platform 222
De omgekeerde proxyserver van WebSEAL 6.0 configureren voor het BI-platform 223
Microsoft ISA 2006 configureren voor het BI-platform 223
8.22 Speciale configuratie voor het BI-platform in implementaties met omgekeerde proxy's. 225
Omgekeerde proxy voor webservices inschakelen. 225
Het basispad voor sessiecookies inschakelen voor ISA 2006. 228
Omgekeerde proxy inschakelen voor SAP BusinessObjects Live Office. 230

9 Verificatie. 231
9.1 Verificatieopties in het BI-platform. 231
Primaire verificatie. 231
Beveiligingsinvoegtoepassingen. 232
Eenmalige aanmelding bij het BI-platform. 233
9.2 Enterprise-verificatie. 236
Enterprise-verificatie (overzicht). 236
Instellingen voor Enterprise-verificatie. 236
Enterprise-instellingen wijzigen. 238
SAML 2.0-verificatie. 239

Vertrouwde verificatie instellen tussen SAP NetWeaver Java Application Server en BI-platform . . . 252
SAML 2.0-verificatie gebruiken met SAP NetWeaver Java Application Server. . . . 256
Vertrouwde verificatie inschakelen. . . . 256
Vertrouwde verificatie configureren voor de webtoepassing. . . . 259
9.3 LDAP-verificatie. . . . 268
LDAP-verificatie gebruiken. . . . 268
LDAP-verificatie configureren. . . . 270
LDAP-groepen toewijzen. . . . 281
9.4 Windows Active Directory-verificatie. . . . 292
Windows Active Directory-verificatie gebruiken. . . . 292
De domeincontroller voorbereiden. . . . 293
AD-verificatie configureren in de CMC. . . . 294
De BI-platformservice configureren om de SIA uit te voeren. . . . 302
De webtoepassingsserver configureren voor AD-verificatie. . . . 304
Eenmalige aanmelding instellen. . . . 312
Problemen met de Windows AD-verificatie oplossen. . . . 329
9.5 SAP-verificatie. . . . 330
SAP-verificatie configureren . . . 330
Gebruikersaccounts maken voor het BI-platform. . . . 331
Verbinding maken met SAP-machtigingssystemen. . . . 333
Opties voor SAP-verificatie instellen. . . . 335
SAP-rollen importeren. . . . 339
SNC configureren (Secure Network Communication). . . . 342
Eenmalige aanmelding bij het SAP-systeem instellen. . . . 356
SSO configureren voor SAP Crystal Reports en SAP NetWeaver. . . . 360
9.6 PeopleSoft-verificatie. . . . 361
Overzicht. . . . 361
PeopleSoft Enterprise-verificatie inschakelen. . . . 361
PeopleSoft-rollen toewijzen aan het BI-platform. . . . 362
Gebruikersupdates plannen. . . . 365
De PeopleSoft Security Bridge gebruiken. . . . 367
9.7 JD Edwards-verificatie. . . . 376
Overzicht. . . . 376
JD Edwards EnterpriseOne-verificatie inschakelen. . . . 377
JD Edwards EnterpriseOne-rollen toewijzen aan het BI-platform. . . . 377
Gebruikersupdates plannen. . . . 380
9.8 Siebel-verificatie. . . . 382
Siebel-verificatie inschakelen. . . . 382
Rollen toewijzen aan het BI-platform. . . . 382
Gebruikersupdates plannen. . . . 385

9.9 Oracle EBS-verificatie. . . . 387
Oracle EBS-verificatie inschakelen. . . . 387
Oracle E-Business Suite-rollen toewijzen aan het BI-platform. . . . 388
Toewijzing van rollen ongedaan maken . . . 392
Rechten aanpassen voor toegewezen Oracle EBS-groepen en -gebruikers . . . 393
Eenmalige aanmelding configureren voor SAP Crystal Reports en Oracle EBS. . . . 394
9.10 X.509-verificatie. . . . 395
X.509-verificatie voor BI-startpunt. . . . 395
X.509-verificatie voor webservices. . . . 403
X.509-verificatie voor CMC. . . . 406
9.11 OpenID Connect-verificatie. . . . 408
OpenID Connect-verificatie inschakelen. . . . 409

10 Gegevensbronverwijzing. . . . 410
10.1 Verbeterde functie Referentieverwijzingen. . . . 410
Een gegevensbronverwijzing maken. . . . 411
De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in CMC. . . . 412
De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in BI-startpunt. . . . 412
De databasereferenties definiëren voor een gegevensbronverwijzing voor een groep. . . . 413
Een gegevensbronverwijzing koppelen aan een OLAP-verbinding. . . . 413

11 Serverbeheer. . . . 415
11.1 Werken met het beheergebied Servers in de CMC. . . . 415
11.2 Servers beheren via scripts in Windows . . . 418
11.3 Servers beheren op Unix . . . 418
11.4 De status van een server weergeven en wijzigen. . . . 418
De status van de servers weergeven. . . . 418
Servers starten, stoppen en opnieuw starten. . . . 420
Een Central Management Server stoppen. . . . 422
Servers in- en uitschakelen. . . . 423
11.5 Servers toevoegen, klonen of verwijderen. . . . 424
Servers toevoegen, klonen en verwijderen. . . . 424
11.6 Aangepaste internetkopteksten toevoegen. . . . 427
11.7 CMS-servers onderbrengen in clusters. . . . 428
CMS-servers onderbrengen in clusters . . . 428
11.8 Servergroepen beheren. . . . 432
Servergroepen maken. . . . 433
Een exclusieve servergroep naar een niet-exclusieve servergroep converteren en andersom . . . 435
Werken met serversubgroepen. . . . 436
Het groepslidmaatschap van een server wijzigen. . . . 438

Beheerderstoegang tot servers en servergroepen voor gebruikers. 439
Een gebruikersgroep aan een servergroep toewijzen. 440
Een map aan een servergroep toewijzen. 443
Rechtenbeheer servergroep begrijpen. 445
11.9 Adaptive Processing Servers configureren voor productiesystemen. 450
11.10 Systeemprestaties inventariseren. 451
Toezicht op de BI-platformservers. 451
Servergegevens analyseren. 451
Systeemgegevens weergeven. 452
Serveractiviteit registreren. 452
11.11 Serverinstellingen configureren. 453
De eigenschappen van een server wijzigen. 454
Service-instellingen op meerdere servers toepassen. 454
Werken met configuratiesjablonen. 454
11.12 Netwerkinstellingen van servers configureren. 457
Opties voor netwerkomgeving. 457
Opties voor host-id van de server. 458
Een multihomed-computer configureren. 460
Poortnummers configureren. 463
11.13 Knooppunten beheren. 465
Knooppunten gebruiken. 465
Een nieuw knooppunt toevoegen. 468
Een knooppunt opnieuw maken. 472
Een knooppunt verwijderen. 476
De naam van een knooppunt wijzigen. 479
Een knooppunt verplaatsen. 481
Scriptparameters. 485
Windows-serverafhankelijkheden toevoegen. 490
De gebruikersreferenties voor een knooppunt wijzigen. 491
11.14 Namen van computers in BI-platformimplementaties wijzigen. 491
Clusternamen wijzigen 491
IP-adressen wijzigen. 492
Computernamen wijzigen. 493
11.15 32-bits en 64-bits bibliotheken van derden gebruiken in BI-platform. 497
11.16 Tijdelijke aanduidingen voor servers en knooppunten beheren. 497
Tijdelijke plaatsaanduidingen van servers weergeven. 497
De tijdelijke plaatsaanduidingen voor een knooppunt bekijken en bewerken. 498

12 CMS-databases (Central Management Server) beheren. 499
12.1 CMS-systeemdatabaseverbindingen beheren. 499
SQL Anywhere selecteren als CMS-database. 499
SAP HANA kiezen als CMS-database. 500

12.2 Een nieuwe of bestaande CMS-database selecteren. . . . 501
Een nieuwe of bestaande CMS-database selecteren onder Windows. . . . 502
Een nieuwe of bestaande CMS-database selecteren in UNIX. . . . 503
12.3 De CMS-systeemdatabase opnieuw maken. . . . 503
De CMS-systeemdatabase opnieuw maken onder Windows. . . . 504
De CMS-systeemdatabase opnieuw maken in UNIX. . . . 505
12.4 Gegevens kopiëren tussen CMS-systeemdatabases. . . . 506
Kopiëren van CMS-systeemdatabase voorbereiden. . . . 506
Een CMS-systeemdatabase kopiëren in Windows. . . . 507
Gegevens kopiëren vanuit een CMS-systeemdatabase onder UNIX. . . . 507
12.5 Databasestuurprogramma Central Management Server. . . . 508

13 Containerservers voor webtoepassingen (WACS) beheren. . . . 509
13.1 WACS. . . . 509
Containerserver voor webtoepassingen (WACS). . . . 509
Extra containerserver voor webtoepassingen aan uw implementatie toevoegen of daaruit verwijderen. . . . 512
Services op een WACS toevoegen of verwijderen. . . . 516
HTTPS/SSL configureren. . . . 517
Ondersteunde verificatiemethoden. . . . 521
AD Kerberos configureren voor de WACS 521
Eenmalige AD Kerberos-aanmelding configureren 529
RESTful-webservices configureren. . . . 531
Containerservers voor webtoepassingen en uw IT-omgeving. . . . 541
Eigenschappen van webtoepassing configureren. . . . 544
Problemen oplossen. . . . 545
Eigenschappen van containerserver voor webtoepassingen 549

14 Back-ups van uw systeem maken en het systeem herstellen. . . . 550
14.1 Overzicht van back-up en herstel. . . . 550
14.2 Terminologie. . . . 550
14.3 Cases gebruiken voor back-up en herstel. . . . 551
14.4 Back-ups. . . . 553
Een back-up maken van het volledige systeem. . . . 554
Back-up maken van serverinstellingen. . . . 557
Een back-up maken van BI-inhoud. . . . 560
14.5 Uw systeem herstellen. . . . 560
Uw volledige systeem herstellen. . . . 561
Serverinstellingen herstellen. . . . 568
BI-inhoud herstellen. . . . 571
14.6 De scripts BackupCluster en RestoreCluster. . . . 571

15 Uw BI-platformimplementatie kopiëren. . . . 575

15.1 Overzicht van systeemkopieën. . . . 575
15.2 Terminologie. . . . 575
15.3 Use cases voor systeemkopieën. . . . 575
15.4 Voorbereiding op het kopiëren van uw systeem. . . . 576
15.5 Overwegingen en beperkingen. . . . 577
15.6 Procedure voor het maken van een systeemkopie. . . . 579
Exporteren vanaf een bronsysteem. . . . 579
Importeren naar een doelsysteem. . . . 583

16 Promotiebeheer. . . . 587
16.1 Welkom bij promotiebeheer. . . . 587
Overzicht. . . . 587
Functies. . . . 587
Toegangsrechten voor toepassingen. . . . 588
Ondersteuning voor WinAD in Promotiebeheer. . . . 589
16.2 Aan de slag met het hulpprogramma voor promotiebeheer. . . . 589
Het hulpprogramma voor promotiebeheer openen. . . . 589
Onderdelen van gebruikersinterface. . . . 590
De optie Instellingen gebruiken. . . . 592
16.3 Het hulpprogramma voor promotiebeheer gebruiken. . . . 599
Mappen maken en verwijderen. . . . 600
Een taak maken. . . . 601
Een nieuwe taak maken door een bestaande taak te kopiëren. . . . 604
Een taak zoeken. . . . 604
Een taak bewerken. . . . 605
Een informatieobject toevoegen aan een taak. . . . 606
De afhankelijkheden van een taak beheren. . . . 607
Afhankelijkheden zoeken. . . . 608
Een taak verhogen wanneer gegevensopslagruimten verbonden zijn. . . . 609
Een taak verhogen met een LCMBIAR-bestand. . . . 611
Een taakverhoging plannen. . . . 615
De geschiedenis van een taak weergeven. . . . 616
Een taak terugzetten. . . . 617
16.4 Inhoud van volledige gegevensopslagruimte verhogen met het hulpprogramma voor Promotiebeheer. . . . 619
Bron- en doelsystemen voorbereiden. . . . 620
Migratiestrategieën. . . . 621
16.5 Stappen volledige systeemverhoging. . . . 622
Gebruikers en gebruikersgroepen (taak 1). . . . 623
Afhankelijke objecten verhogen (taak 2). . . . 623
Primaire objecten verhogen (taak 3). . . . 625
Na verhoging. . . . 626

16.6 De optie Opdrachtregel gebruiken. . . . 626
Het hulpprogramma voor opdrachtregels in Windows uitvoeren. . . . 626
Het hulpprogramma voor opdrachtregels in Unix uitvoeren. . . . 627
Parameters van opdrachtregelprogramma. . . . 628
Voorbeeld van eigenschappenbestand. . . . 653
16.7 Het Enhanced Change and Transport System gebruiken. . . . 654
Vereisten. . . . 655
Integratie van het BI-platform en CTS+ configureren. . . . 655
Een taak verhogen met CTS. . . . 662
16.8 De wizard Doorgiftebeheer gebruiken 665
Objecten uitsluiten van doorgifte. . . . 666
Wanneer moet u de wizard Doorgiftebeheer gebruiken. . . . 666
Scenario. . . . 668
Objecten. . . . 669
Afhankelijkheden. . . . 673
Samenvatting. . . . 674
(Optioneel) eigenschappenbestand. . . . 675
De wizard Doorgiftebeheer in Linux. . . . 678

17 Versiebeheer. . . . 679
17.1 Verschillende versies van een informatieobject beheren. . . . 679
Toegangsrechten voor Versiebeheer. . . . 679
Back-ups van Subversion-bestanden maken en herstellen. . . . 680
17.2 Verschillende versies van BI-bronnen beheren. . . . 681
17.3 Subversion handmatig starten en stoppen in Unix. . . . 683
17.4 Vereiste bestanden voor Subversion in Solaris 10 en RedHat Linux 5. . . . 683
17.5 Apache SubVersion gebruiken als Versiebeheersysteem. . . . 683
17.6 Git gebruiken als versiebeheersysteem. . . . 684
17.7 Standaardinstellingen van Versiebeheersysteem. . . . 685
17.8 Verschillende versies van dezelfde taak vergelijken. . . . 686
17.9 Upgrade van Subversion-inhoud uitvoeren. . . . 686
17.10 Subversion configureren voor geclusterde Job Servers voor verwerking. . . . 687
Optie A: De Subversion-hoofdcomputer vóór eventuele bewerkingen in het versiebeheersysteem configureren. . . . 687
Optie B: Subversion configureren nadat het versiebeheersysteem een werkkopiemap heeft gemaakt. . . . 688
Andere SubVersion-computers configureren. . . . 688

18 Toepassingen beheren. . . . 690
18.1 GDPR-pop-upbericht uitschakelen. . . . 690
18.2 Toepassingen beheren via de CMC. . . . 692
Overzicht. . . . 692

Algemene instellingen voor toepassingen. . . . 693
Toepassingsspecifieke instellingen. . . . 694
18.3 Toepassingen beheren via Semantic Layer-eigenschappen. . . . 752
18.4 Toepassingen beheren via BOE.war-eigenschappen. . . . 754
Het BOE.war-bestand. . . . 754
18.5 Ingangspunten voor aanmelding bij BI-startpunt en OpenDocument aanpassen. . . . 772
Bestandslocaties van het BI-startpunt en OpenDocument. . . . 773
Een aangepaste aanmeldingspagina definiëren. . . . 774
Vertrouwde verificatie toevoegen bij aanmelding. . . . 774
18.6 Gebruikersinterfaces toepassing aanpassen. . . . 775
Web Intelligence. . . . 776
BI-startpunt. . . . 782
18.7 BI-platform RESTful-webservices configureren op webserver. . . . 783
18.8 Hybride gebruikersbeheer. . . . 786
18.9 Uw On-Premises gebruikers toewijzen aan SAP Analytics Cloud. . . . 787
Een verbinding tot stand brengen tussen het On-Premises-systeem en de cloud. . . . 787
18.10 OAuth-clientreferenties maken in SAP Analytics Cloud. . . . 788
18.11 Het bronsysteem configureren. . . . 789
18.12 Het doelsysteem configureren. . . . 790
18.13 Gebruikers en gebruikersgroepen toewijzen aan SAP Analytics Cloud. . . . 791
18.14 Toegewezen gebruikers weergeven in SAP Analytics Cloud. . . . 791
18.15 Voorbeeldsjablonen. . . . 792

19 Verbindingen en universes beheren. . . . 796
19.1 Verbindingen beheren. . . . 796
Een universe-verbinding verwijderen. . . . 796
19.2 Universes beheren. . . . 797
Universes verwijderen. . . . 798

20 BI-beheerderstudio. . . . 799
20.1 Beheercockpit. . . . 800
Beheercockpit. . . . 800
BI voor servers. . . . 801
BI in documentexemplaren. . . . 802
BI voor gebruikers en sessies. . . . 803
BI voor inhoudsgebruik. . . . 803
BI op toepassingen. . . . 804
20.2 Toezicht. . . . 804
Termen met betrekking tot toezicht. . . . 805
Databaseondersteuning configureren voor de Toezichtfunctie. . . . 809
Configuratie-eigenschappen. . . . 817
Integratie met andere toepassingen. . . . 824

Clusterondersteuning voor toezichtserver. . . . 824
Problemen oplossen. . . . 825
20.3 Visueel verschil. . . . 828
Objecten of bestanden vergelijken met Visueel verschil. . . . 829
Objecten of bestanden vergelijken met het Versiebeheersysteem. . . . 830
20.4 HTML-elementen autoriseren. . . . 831
De lijst met geautoriseerde HTML-elementen wijzigen. . . . 833

21 CMS-rapportage. . . . 834
21.1 CMS-rapportage. . . . 834
De architectuur van het SAP BusinessObjects-platform. . . . 834
De structuur van de CMS-systeemdatabase. . . . 835
Info InfoObjects. . . . 837
21.2 Overzicht van CMS-rapportage. . . . 840
21.3 CMS-databaseverbinding. . . . 840
21.4 Voorbeeldkit CMS-rapportage. . . . 842
De voorbeeldkit voor CMS-rapportage met promotiebeheer importeren. . . . 842
De CMS-voorbeelduniverse . . . 843
De CMS-voorbeelduniverse uitbreiden. . . . 843
21.5 Een rapport op CMS maken. . . . 844

22 Workflowassistent. . . . 845
22.1 Doelgroep. . . . 846
22.2 De architectuur. . . . 846
22.3 Woordenlijst. . . . 847
22.4 Informatie over installeren en bijwerken. . . . 850
22.5 De Workflowassistent configureren. . . . 851
Basisconfiguratie. . . . 851
22.6 Workflowassistent-rechten beheren via de Central Management Console. . . . 853
22.7 Werken met de Workflowassistent. . . . 858
Standaardtaaksjablonen. . . . 858
Informatie over standaardworkflowsjablonen. . . . 868
Informatie over aangepaste taaksjablonen. . . . 869
Workflowsjablonen beheren. . . . 869
Scenario's beheren en resultaten weergeven. . . . 871
De statuswaarden van taaksjablonen, workflowsjablonen en scenario's. . . . 876
Werken met Systemen. . . . 878
Volledige processtroom van de Worklowassistent. . . . 881
22.8 Logboekbestanden controleren. . . . 881

23 Prullenbak. . . . 883
23.1 Prullenmand. . . . 883

Item uit prullenmand herstellen. 883
Items uit de prullenmand permanent verwijderen. 884
Automatisch opschonen voor prullenmand inschakelen. 884

24 Controle. 886
24.1 Overzicht. 886
24.2 CMC-controlepagina. 893
Controlestatus. 893
Controlegebeurtenissen configureren. 895
Configuratie-instellingen van ADS (Auditing Data Store). 899
24.3 Controlegebeurtenissen. 900
Audit events and details. 909

25 Gebeurtenissen. 932
25.1 Over gebeurtenissen. 932
Gebruikersberichten. 933

26 Platform zoeken. 937
26.1 Hoe Platform zoeken werkt. 937
SDK van Platform zoeken. 937
Geclusterde omgeving. 938
26.2 Platform zoeken instellen. 938
OpenSearch implementeren. 938
Reverse proxy configureren. 940
Toepassingseigenschappen configureren in de CMC. 940
26.3 Werken met Platform zoeken. 948
Inhoud indexeren in de CMS-gegevensopslagruimte. 948
Lijst met fouten bij indexering. 949
Door resultaten zoeken. 950
26.4 Platform zoeken integreren met SAP NetWeaver Enterprise Search. 956
Een connector maken in SAP NetWeaver Enterprise Search 956
De rol van een gebruiker in het BI-platform importeren. 957
26.5 Zoeken in resultaten uit SAP NetWeaver Enterprise Search. 958
26.6 Controle. 958
26.7 Problemen oplossen. 959
Zelfherstel. 959
Scenario's van problemen. 960

27 Federatie. 962
27.1 Federatie. 962
27.2 Federatieterminologie. 963
27.3 Beveiligingsrechten beheren. 965
Vereiste rechten op de oorspronkelijke locatie. 965

Vereiste rechten op de doellocatie. . . . 966
Rechten specifiek voor Federatie. . . . 967
Beveiliging voor een object herhalen. . . . 968
Beveiliging herhalen met toegangsniveaus. . . . 969
27.4 Opties voor herhalingstype en herhalingsmodus. . . . 969
Herhaling in één richting 969
Herhaling in beide richtingen 970
Vernieuwen vanaf oorsprong of Vernieuwen vanaf doel. . . . 970
27.5 Externe gebruikers en groepen herhalen. . . . 972
27.6 Universes en universeverbindingen herhalen. . . . 973
27.7 Herhalingslijsten beheren. . . . 974
Herhalingslijsten maken. . . . 975
Herhalingslijsten wijzigen. . . . 977
27.8 Externe verbindingen beheren. . . . 978
Externe verbindingen maken. . . . 978
Externe verbindingen wijzigen. . . . 980
27.9 Herhalingstaken beheren. . . . 981
Herhalingstaken maken. . . . 981
Herhalingstaken plannen. . . . 983
Herhalingstaken wijzigen. . . . 983
Een logboek weergeven na uitvoering van een herhalingstaak. . . . 984
27.10 Opschoning van objecten beheren. . . . 985
Een object opschonen. . . . 985
Limieten voor het opschonen van objecten. . . . 986
Frequentie voor het opschonen van objecten. . . . 986
27.11 Conflictopsporing en -oplossing beheren. . . . 987
Conflicten als gevolg van herhaling in één richting oplossen. . . . 988
Conflicten als gevolg van replicatie in twee richtingen oplossen. . . . 990
27.12 Webservices gebruiken in Federatie. . . . 993
Sessievariabelen 993
Bestandencache 994
Aangepaste implementatie 994
27.13 Externe planning en lokaal uitgevoerde exemplaren. . . . 995
Externe planning. . . . 995
Lokaal uitgevoerde exemplaren. . . . 997
Exemplaren delen. . . . 997
27.14 Herhaalde inhoud importeren en overbrengen. . . . 998
Herhaalde inhoud importeren. . . . 999
Herhaalde inhoud importeren en herhaling voortzetten 999
Inhoud overbrengen vanuit een testomgeving. . . . 1000
Opnieuw verwijzen naar een doellocatie. . . . 1001

27.15 Gebruiksadviezen. 1001
Beperkingen van de huidige release. 1004
Probleemoplossing bij foutberichten. 1005

28 Aanvullende configuraties voor ERP-omgevingen. 1010
28.1 Configuraties voor SAP NetWeaver-integratie. 1010
Integreren met SAP Business Warehouse (BW). 1010
28.2 Configureren voor JD Edwards-integratie. 1055
Eenmalige aanmelding configureren voor SAP Crystal Reports. 1055
Secure Sockets Layer configureren voor JD Edwards-integraties. 1056
28.3 Configureren voor PeopleSoft Enterprise-integratie. 1058
Eenmalige aanmelding configureren voor SAP Crystal Reports en PeopleSoft Enterprise. 1058
Secure Sockets Layer-communicatie configureren. 1059
Prestatie-afstemming voor PeopleSoft-systemen. 1060
28.4 Configureren voor Siebel-integratie. 1062
Siebel configureren voor integratie met SAP BI-platform. 1062
Het menu-item Crystal Reports aanmaken. 1063
Contextgebonden regels. 1064
Eenmalige aanmelding configureren voor SAP Crystal Reports en Siebel. 1066
Configureren voor Secure Sockets Layer-communicatie. 1067

29 Logboeken beheren en configureren. 1069
29.1 Tracering voor onderdelen registreren. 1069
29.2 Niveaus voor traceringslogboeken. 1069
29.3 Tracering voor servers configureren. 1070
Het logboekniveau instellen in de CMC. 1071
Het logboekniveau voor meerdere servers instellen in de CMC. 1071
Servertracering configureren via het bestand BO_trace.ini. 1072
29.4 Tracering configureren voor webtoepassingen. 1074
Het niveau voor het traceringslogboek voor webtoepassingen instellen in de CMC. 1075
Traceringsinstellingen configureren via het bestand `BO_trace.ini`. 1076
29.5 Tracering configureren voor clienttoepassingen van BI-platform. 1081
29.6 Uitgebreide tracering van foutmeldingen configureren.. 1081
29.7 Logboekbestanden uitgebreide informatie van foutmelding inschakelen. 1081

30 Integratie in SAP Solution Manager. 1083
30.1 Integratieoverzicht. 1083
30.2 Controlelijst voor SAP Solution Manager-integratie. 1083
30.3 Registratie van systeemlandschapsmap beheren. 1084
Registratie van het BI-platform in het systeemlandschap. 1084
Wanneer wordt SLD-registratie geactiveerd?. 1086
Opschoning SLD vóór patchinstallaties. 1086

SLD-verbindingen registreren . . . 1087
Virtuele hostnaam. . . . 1087
30.4 Solution Manager Diagnostics-agenten beheren. . . . 1088
Overzicht van Solution Manager Diagnostics. . . . 1088
Met SMD-agents werken. . . . 1088
SMAdmin-gebruikersaccount. . . . 1089
30.5 Prestatie-instrumentatie beheren. . . . 1090
Prestatie-instrumentatie voor het BI-platform. . . . 1090
Prestatie-instrumentatie instellen voor het BI-platform. . . . 1090
Prestatie-instrumentatie voor de weblaag. . . . 1091
Logboekbestanden van instrumentatie . . . 1092
30.6 Tracering met SAP Passport. . . . 1092

31 Beheer van opdrachtregels. . . . 1094
31.1 Unix-scripts. . . . 1094
Scriptprogramma's. . . . 1094
Scriptsjablonen. . . . 1099
Scripts die door het BI-platform worden gebruikt. . . . 1100
31.2 Windows-scripts. . . . 1101
ccm.exe. . . . 1101
31.3 Opdrachtregels voor servers. . . . 1104
Overzicht van opdrachtregels. . . . 1104
Standaardopties voor alle servers. . . . 1105
Central Management Server. . . . 1106
Crystal Reports Processing Server en Crystal Reports Cache Server. . . . 1107
Job Servers. . . . 1108
Adaptive Processing Server. . . . 1109
Report Application Server. . . . 1109
Web Intelligence-verwerkingsserver. . . . 1111
Input en Output File Repository Server. . . . 1112
Event Server. . . . 1114

32 Diagnostisch hulpprogramma voor gegevensopslagruimten. . . . 1116
32.1 Overzicht van het diagnostisch hulpprogramma voor gegevensopslagruimte. . . . 1116
32.2 Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken. . . . 1117
Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken. . . . 1117
Parameters voor het diagnostische hulpprogramma voor gegevensopslagruimten. . . . 1119
32.3 Inconsistenties tussen de CMS en de FRS. . . . 1127
32.4 Inconsistenties in de CMS-metagegevens. . . . 1128
32.5 Restful-SDK beheren in BOE WebApp. . . . 1131

33 HSTS (HTTP Strict Transport Security). . . . 1132

33.1 HSTS (HTTP Strict Transport Security) configureren. . . . 1132

34 Bijlage Rechten. . . . 1133

34.1 De rechtenbijlage. . . . 1133

34.2 Algemene rechten. . . . 1133

Doelrechten. . . . 1137

34.3 Rechten voor specifieke objecttypen. . . . 1138

Maprechten. . . . 1138

Categorieën. . . . 1138

Crystal Reports-rapporten. . . . 1139

Web Intelligence-documenten. . . . 1139

Gebruikers en groepen. . . . 1140

Toegangsniveaus. . . . 1142

Universe-rechten (.unv). . . . 1142

Universe-rechten (.unx). . . . 1144

Toegangsniveaus voor universe-objecten. . . . 1145

Verbindingsrechten. . . . 1146

Toepassingen. . . . 1148

35 Bijlage Servereigenschappen. . . . 1157

35.1 Over de bijlage Servereigenschappen. . . . 1157

Algemene servereigenschappen. . . . 1157

Eigenschappen van kernservices. . . . 1159

Eigenschappen van Connectivity-services. . . . 1170

Eigenschappen van Crystal Reports-services. . . . 1175

Eigenschappen van Analysis Services. . . . 1183

Eigenschappen van Data Federator-services. . . . 1184

Eigenschappen van Web Intelligence Services. . . . 1185

36 Bijlage Servergegevens. . . . 1193

36.1 Informatie over de bijlage Servergegevens. . . . 1193

Algemene servergegevens. . . . 1193

Gegevens van Central Management Server. . . . 1195

Gegevens van verbindingsserver. . . . 1198

Gegevens van Event Server. . . . 1199

Gegevens van File Repository Server. . . . 1199

Gegevens van Adaptive Processing Server. . . . 1200

Gegevens van containerserver voor webtoepassingen. . . . 1205

Gegevens van Adaptive Job Server. . . . 1205

Crystal Reports Server-gegevens. . . . 1207

Gegevens van Web Intelligence Server. . . . 1209

37 Appendix met tijdelijke aanduidingen voor servers en knooppunten. . . . 1211

37.1 Tijdelijke plaatsaanduidingen voor server en knooppunt. 1211

38 Appendix met schema voor controle van gegevensopslag. 1221

38.1 Overzicht. 1221

38.2 Schemadiagram. 1221

38.3 Auditing Data Store Tables. 1221

39 Appendix met schema voor controle van database. 1229

39.1 Schema van trending-database. 1229

40 Bijlage met werkblad Systeemkopie. 1232

40.1 Werkblad Systeemkopie. 1232

1 Documentgeschiedenis

De volgende tabel geeft een overzicht van de belangrijkste documentwijzigingen.

Versie	Datum	Beschrijving
SAP BusinessObjects Business Intelligence-platform 4.3 SP3	December 2022	De volgende onderwerpen zijn bijgewerkt met het nieuwe veld met een maximale wachtwoordlengte voor Enterprise-verificatie: • Instellingen voor Enterprise-verificatie [pagina 236] • Een gebruikersaccount maken [pagina 102] • Algemene wachtwoordinstellingen wijzigen [pagina 111] • Algemene wachtwoordinstellingen wijzigen [pagina 238] • De optie voor het inschakelen van het gebruik van een pad naar een relatieve URL is geïntroduceerd om de relatieve URL van de browser te gebruiken.
SAP BusinessObjects Business Intelligence-platform 4.3 SP2	December 2021	Configuratie verificatieserver [pagina 748] toegevoegd. Interface-elementen van Web Intelligence aanpassen per gebruikersgroepen en mappen [pagina 776] bijgewerkt.

SAP BusinessObjects Business Intelligence-platform 4.3 SP1	December 2020	• De volgende nieuwe onderwerpen zijn toegevoegd:
		  • Een onderwerp over aanpassing van de Web Intelligence-gebruikersinterface. Zie Interface-elementen van Web Intelligence aanpassen per gebruikersgroepen en mappen [pagina 776].
		  • Script voor het wissen van verouderde sessies [pagina 158].
		  • De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in BI-startpunt [pagina 412]
		  • JMX SSL-configuratie [pagina 821]
		• Er zijn twee onderwerpen bijgewerkt:
		  • Upgradepaden [pagina 30].
		  • Doelrechten [pagina 1137] voor *Doelopties* en *Eigenschappen van het e-maildoel* met het nieuw toegevoegde veld *Antwoord aan* voor alle publicatiescenario's.

SAP BusinessObjects Business Intelligence-platform 4.3	Juni 2020	• SAP BusinessObjects Explorer, SAP BusinessObjects-dashboards, het hulpprogramma voor rapportconversie, het hulpprogramma voor upgradebeheer en BI Widgets zijn verwijderd in release 4.3. • Een nieuw onderwerp Workflowassistent [pagina 845] toegevoegd.

2 Aan de slag

2.1 Over deze handleiding

Deze handleiding biedt u informatie over en procedures voor de implementatie en configuratie van het SAP BusinessObjects Business Intelligence-platform (het "BI platform"). Veelvoorkomende taken worden toegelicht aan de hand van procedures. Alle geavanceerde onderwerpen worden eerst algemeen beschreven, waarna technische details worden gegeven.

Zie de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence Platform* voor meer informatie over de installatie van dit product.

2.1.1 Voor wie is deze handleiding bedoeld?

Deze handleiding gaat over de implementatie en configuratie van het BI-platform. Het is raadzaam deze handleiding te raadplegen wanneer u een van de volgende taken uitvoert:

- Planning van uw eerste implementatie
- Configuratie van uw eerste implementatie
- Ingrijpende wijzigingen aanbrengen in de architectuur van een bestaande implementatie
- De systeemprestaties verbeteren

Deze handleiding is bedoeld voor systeembeheerders die verantwoordelijk zijn voor het configureren, beheren en onderhouden van een BI-platforminstallatie. Kennis van het besturingssysteem en de netwerkomgeving is gewenst, evenals algemene kennis van webserverbeheer en scripttechnologieën. Aangezien deze handleiding bedoeld is voor beheerders op alle niveaus, wordt er voldoende achtergrondinformatie geboden en worden de beginselen van alle beheerderstaken en -functies toegelicht.

2.1.2 Het Business Intelligence-platform

Het Business Intelligence-platform (BI-platform) is een flexibele en schaalbare oplossing voor het leveren van informatie aan eindgebruikers in verschillende vormen, zoals dashboards en interactieve rapporten, via elke webtoepassing: intranet, extranet, internet of bedrijfsportal.

Het platform is een geïntegreerde suite voor rapportage, analyse en levering van informatie en biedt concrete voordelen voor de hele organisatie en daarbuiten.

Het zorgt ook voor een hogere productiviteit van de eindgebruiker en een afname van de administratieve werkzaamheden.

Het wordt bijvoorbeeld gebruikt om wekelijkse verkooprapporten te verspreiden, om klanten een persoonlijk serviceaanbod te leveren of om essentiële informatie op te nemen in bedrijfsportalen.

2.1.3 Variabelen

In deze handleiding worden de volgende variabelen gebruikt.

Variabele	Beschrijving
`<INSTALLDIR>`	De map waarin BI-platform is geïnstalleerd. Onder Windows is de standaardmap: `C:\Program Files (x86)\SAP BusinessObjects`
`<PLATFORM64DIR>`	De naam van uw Unix-besturingssysteem. Geldige waarden zijn: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
`<SCRIPTDIR>`	De map waarin de scripts voor het beheer van het BI-platform zijn opgeslagen. In Windows is de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`. In Unix is de map `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM64MAP>/scripts`.

2.1.4 Terminologie

De volgende termen worden gebruikt in de documentatie van het BI-platform:

Begrip	Definitie
Invoegproducten	Producten die met het BI-platform werken maar hun eigen installatieprogramma hebben.
ADS (Auditing Data Store)	De database die wordt gebruikt om controlegegevens op te slaan.
BI-platform	Een afkorting voor het SAP BusinessObjects Business Intelligence-platform
Gebundelde database, gebundelde webtoepassingsserver	De database of webtoepassingsserver die bij het BI-platform wordt geleverd.
Cluster	Een cluster bestaat uit twee of meer CMS'en (Central Management Servers) die samenwerken en één CMS-database gebruiken.

Begrip	Definitie
Clusteren	Ga als volgt te werk om een cluster te maken: 1. Installeer een CMS en CMS-database op computer A. 2. Installeer een CMS op computer B. 3. Zorg dat de CMS op computer B naar de CMS-database op computer A verwijst.
Clustersleutel	Wordt gebruikt om de sleutels in de CMS-database te decoderen. U kunt de clustersleutel wijzigen met de CCM, maar u kunt deze sleutel niet opnieuw instellen zoals met een wachtwoord. De sleutel bevat gecodeerde inhoud. Daarom is het belangrijk dat u deze niet kwijtraakt
CMS	Een afkorting voor de Central Management Server
CMS-database	De database die door de CMS wordt gebruikt om informatie over het BI-platform op te slaan.
Implementatie	De software van het BI-platform die op een of meer computers is geïnstalleerd, geconfigureerd en wordt uitgevoerd.
Installatie	Een exemplaar van bestanden van het BI-platform dat door het installatieprogramma op een computer gemaakt is.
Computer	De computer waar de BI platform-software is geïnstalleerd
Hoofdversie	Een volledige versie van de software
Subversie	Een versie van enkele componenten van de software
Knooppunt	Een groep BI-platformservers die op dezelfde computer worden uitgevoerd en door dezelfde SIA (Server Intelligence Agent) worden beheerd.
patch	Kleine update voor een specifieke ondersteuningspakketversie.
Doorgifte	Het proces van het overdragen van Business Intelligence-inhoud tussen implementaties met dezelfde hoofdversie (bijv. 4.3 naar 4.3) met de toepassing voor doorgiftebeheer.
Server	Een BI-platformproces. Een server host een of meer services
SIA (Server Intelligence Agent)	Proces voor het beheer, inclusief stoppen, starten en herstarten, van een groep servers.
ondersteuningspakket	Software-update voor een sub- of hoofdversie.

Begrip	Definitie
Webtoepassingsserver	Een server die dynamische inhoud verwerkt
Upgrade	Alle planning, voorbereiding, migratie en postprocessen die zijn vereist om een migratieproces te voltooien.
ONE Installer	ONE Installer is een afzonderlijk installatiepakket dat ondersteuning biedt voor meerdere BI-installatiescenario's zoals een nieuwe installatie van een servicepakket of Support Package, een update van de Support Package-versie of een update van een servicepakket naar een Support Package.

2.2 Voordat u begint

2.2.1 Sleutelconcepten

2.2.1.1 Server Intelligence

Server Intelligence is een kerncomponent van het BI-platform. Wijzigingen in serverprocessen die in de CMC (Central Management Console) worden aangebracht, worden doorgevoerd in de desbetreffende serverobjecten door de CMS (Central Management Server). De SIA (Server Intelligence Agent) wordt gebruikt om een server automatisch opnieuw op te starten of af te sluiten als aan een onverwachte voorwaarde wordt voldaan, en wordt door de beheerder gebruikt om een knooppunt te beheren.

De CMS slaat informatie over servers op in de CMS-systeemdatabase, zodat u standaardserverinstellingen gemakkelijk kunt herstellen. Omdat de SIA periodiek gegevens ophaalt uit de CMS over beheerde servers, is in de SIA bekend wat de status van die servers is en wanneer actie moet worden ondernomen.

> ⓘ Opmerking
>
> Een BI-platforminstallatie is een uniek exemplaar van de BI-platformbestanden die door het installatieprogramma op een computer zijn gemaakt. Een exemplaar van een BI-platforminstallatie kan alleen in één cluster worden gebruikt. Knooppunten die tot verschillende clusters behoren met dezelfde BI-platforminstallatie, worden niet ondersteund, omdat er geen patch of update op dit type implementatie kan worden toegepast. Alleen UNIX-platforms ondersteunen meerdere installaties van de software op dezelfde computer. Als elke installatie wordt uitgevoerd onder een unieke gebruikersaccount en in een aparte map, delen de installaties geen bestanden. Alle computers in het cluster moeten dezelfde versie en hetzelfde patchniveau hebben.

Verwante informatie

Servers, hosts en clusters [pagina 38]

2.2.1.2 Servers, services, knooppunten en hosts

In het BI-platform worden de termen server en service gebruikt om te verwijzen naar de twee typen software die op een computer met het BI-platform worden uitgevoerd.

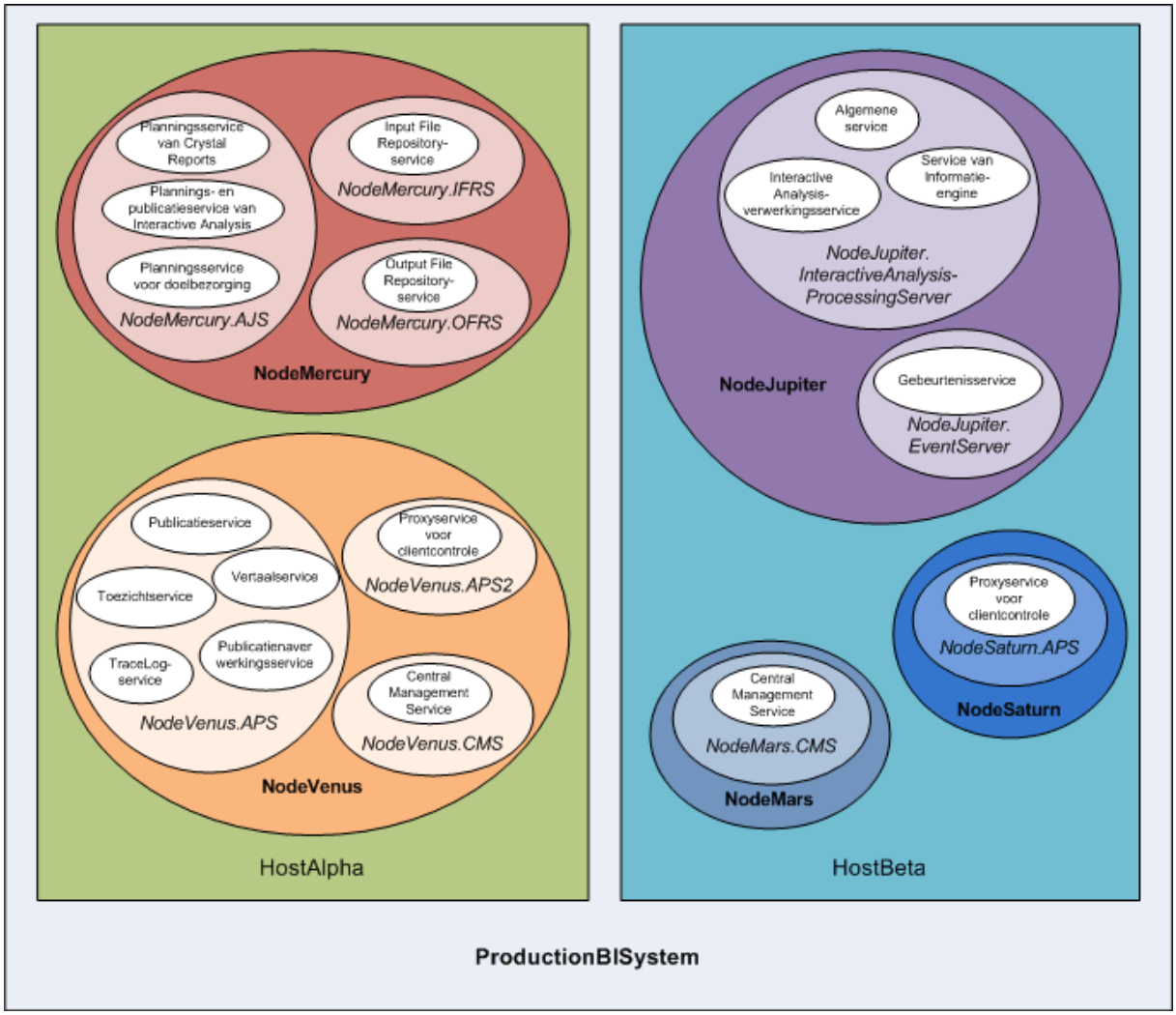
De term “server” wordt gebruikt om een proces op besturingssysteemniveau te beschrijven (op sommige systemen heet dit een daemon), dat een of meer services host. De CMS (Central Management Server) en de Adaptive Processing Server bijvoorbeeld, zijn servers. Servers worden uitgevoerd onder een bepaald besturingssysteemaccount en hebben een eigen PID (proces-id).

Een service is een serversubsysteem dat een specifieke functie heeft. De service wordt uitgevoerd in de geheugenruimte van de bijbehorende server, onder de proces-id van de bovenliggende container (server). De plannings- en publicatieservice van Web Intelligence is bijvoorbeeld een subsysteem dat op de Adaptive Job Server wordt uitgevoerd.

Een knooppunt is een verzameling BI-platformservers die worden uitgevoerd op dezelfde host en worden beheerd via dezelfde SIA (Server Intelligence Agent). Een host kan meerdere knooppunten bevatten.

Het BI-platform kan op één computer worden geïnstalleerd, op een aantal computers in een intranet of in een WAN (Wide Area Network).

In het volgende diagram wordt een hypothetische installatie van het BI-platform weergegeven. Het aantal hosts, knooppunten, servers en services, evenals het type servers en services, zal verschillen in daadwerkelijke installaties.



Twee hosts vormen het cluster met de naam ProductionBISystem:

- Op de host genaamd HostAlpha is het BI-platform geïnstalleerd en geconfigureerd voor twee knooppunten:
  - NodeMercuy bevat een Adaptive Job Server (`NodeMercury.AJS`) met services voor het plannen en publiceren van rapporten, een Input File Repository Server (`NodeMercury.IFRS`) met een service voor het opslaan van invoerrapporten, en een Output File Repository Server (`NodeMercury.OFRS`) met een service voor het opslaan van rapportuitvoer.
  - NodeVenus bevat een Adaptive Processing Server (`NodeVenus.APS`) met functies voor publiceren, controleren en vertalen, een Adaptive Processing Server (`NodeVenus.APS`) met een service voor clientcontrole, en een Central Management Server (`NodeVenus.CMS`) met een service voor de CMS-services.
- Op de host genaamd HostBeta is het BI-platform geïnstalleerd en geconfigureerd voor drie knooppunten:
  - `NodeMars` bevat een Central Management Server (NodeMars.CMS) met een service voor de CMS-services. Als u de CMS op twee computers installeert, beschikt u over mogelijkheden voor taakverdeling, risicobeperking en failover.
  - NodeJupiter bevat een Web Intelligence-verwerkingsserver (`NodeJupiter.Web Intelligence`) met een service voor Web Intelligence-rapportage en een gebeurtenisserver (`NodeJupiter.EventServer`) voor rapportcontrole van bestanden.

- NodeSaturn bevat een Adaptive Processing Server (`NodeSaturn.APS`) met een service voor clientcontrole.

2.2.2 Belangrijkste beheerhulpprogramma's

2.2.2.1 Wizard Systeemconfiguratie

De wizard Systeemconfiguratie is een hulpprogramma waarmee u uw BI-platformimplementatie snel en eenvoudig kunt configureren. De wizard begeleidt u bij de basisopties van de configuratie met als resultaat een actieve implementatie met algemene instellingen zoals:

- de producten waarvan de servers automatisch moeten worden gestart met het BI-platform
- of u uw implementatie wilt optimaliseren voor maximumprestaties of voor beperkte hardwareresources
- de locaties van systeemmappen

De wizard is standaard ingesteld om automatisch te worden uitgevoerd wanneer u zich aanmeldt bij de CMC (Central Management Console), maar u kunt deze instelling in de wizard wijzigen. U kunt de wizard ook op elk moment in het gebied *Beheren* in de CMC starten.

> ⓘ Opmerking
>
> In productiesystemen is het raadzaam in te stellen dat de wizard niet automatisch wordt uitgevoerd, om te voorkomen dat er onbedoeld een herconfiguratie plaatsvindt.

> ⓘ Opmerking
>
> Maak een volledige back-up voordat u de wizard gebruikt voor het aanbrengen van wijzigingen in een bestaand systeem.

2.2.2.2 Central Management Console (CMC)

De Central Management Console (CMC) is een webtoepassing waarmee u beheertaken kunt uitvoeren (bijvoorbeeld gebruikers-, inhoud- en serverbeheer) en beveiligingsopties kunt instellen. Omdat de CMC een webtoepassing is, kunt u de gewenste beheertaken uitvoeren in een webbrowser op elke computer met een verbinding met de webtoepassingsserver.

Alleen leden van de groep Administrators kunnen beheerinstellingen wijzigen, tenzij aan andere gebruikers expliciet de rechten hiertoe zijn verleend. In CMC kunnen aan gebruikers rollen worden toegekend waarmee zij beperkte beheertaken kunnen uitvoeren, zoals het beheren van gebruikers in uw groep en het beheren van rapporten in teammappen.

2.2.2.3 Central Configuration Manager (CCM)

De CCM (Central Configuration Manager) is een serverprogramma voor probleemoplossing en knooppuntbeheer dat beschikbaar is in twee vormen. In een Microsoft Windows-omgeving kunt u met de CCM lokale en externe servers beheren. U gebruikt daartoe de grafische gebruikersinterface (GUI) van het programma of een opdrachtregel. In een Unix-omgeving kunt u servers met behulp van het CCM-shellscript (`ccm.sh`) via de opdrachtregel beheren.

U gebruikt de CCM voor het maken en configureren van knooppunten of het starten en stoppen van de webtoepassingsserver, als dit de standaard gebundelde Tomcat-webtoepassingsserver is. In Windows kunt u de CCM ook gebruiken om netwerkparameters te configureren, bijvoorbeeld SSL-codering (Secure Sockets Layer). Deze parameters zijn van toepassing op alle servers binnen een knooppunt.

> **Opmerking**
>
> De meeste serverbeheertaken worden nu via de CMC verwerkt, niet via de CCM. De CCM wordt nu voor probleemoplossing en knooppuntconfiguratie gebruikt.

2.2.2.4 Diagnostisch hulpprogramma voor gegevensopslagruimten

Met het diagnostische hulpprogramma voor gegevensopslagruimten kunt u inconsistenties die zich voordoen tussen de CMS-systeemdatabase (Central Management Server) en de FRS's (File Repository Servers), scannen, diagnosticeren en herstellen. U kunt een limiet instellen voor het aantal fouten dat het RDT per sessie kan detecteren en herstellen.

Het RDT moet worden gebruikt nadat u uw BI-platformsysteem hebt hersteld.

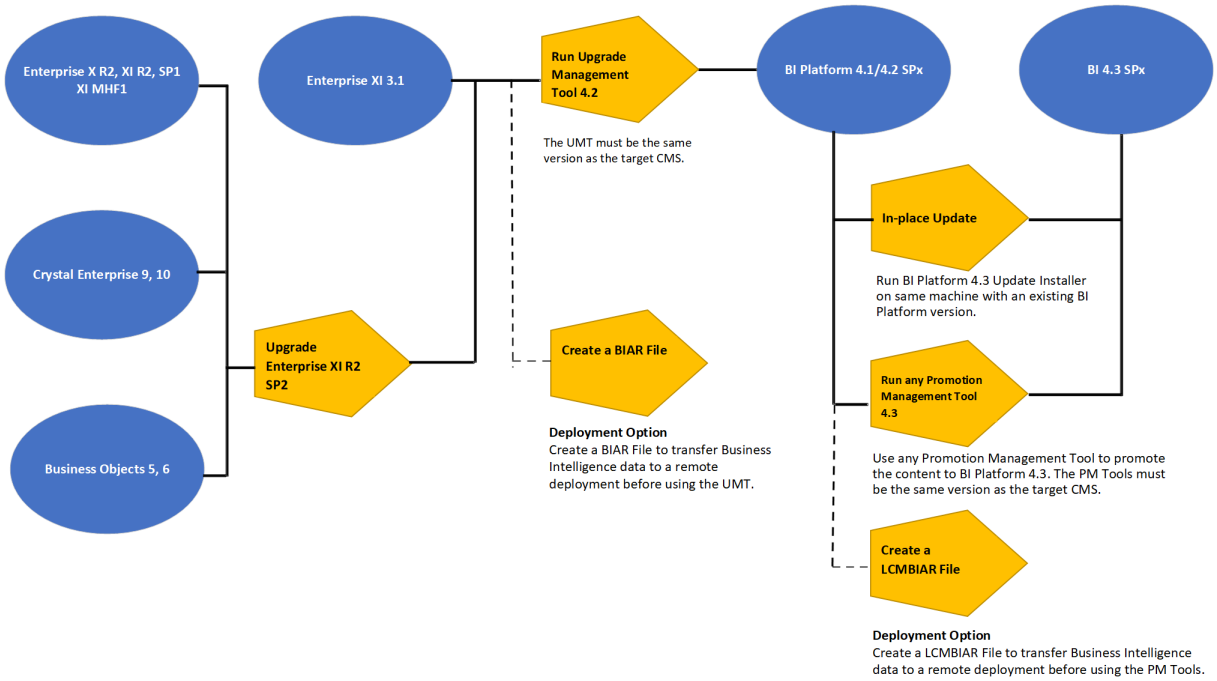
> **Opmerking**
>
> In productiesystemen is het raadzaam om het diagnostische hulpprogramma voor gegevensopslagruimten regelmatig uit te voeren (schakel dan wel de optie “Repareren” uit) om te controleren of er sprake is van onderliggende problemen met de systeemstatus. Schakel de optie Repareren bij het uitvoeren van het diagnostische hulpprogramma voor gegevensopslagruimten alleen in als u wilt dat het systeem door het programma wordt gerepareerd.

2.2.2.5 Hulpprogramma voor upgradebeheer

Het hulpprogramma UMT is uit gebruik genomen in de BI 4.3-release. Zie 2801797 voor meer informatie.

2.2.2.6 Upgradepaden

U kunt uw systeemgegevens en BI-inhoud migreren van de vorige BI 4.x versies naar SAP BusinessObjects Business Intelligence-platform 4.3.



Het hulpprogramma voor upgradebeheer is uit gebruik genomen in SAP BusinessObjects Business Intelligence-platform 4.3, maar u kunt de hierna genoemde upgradepaden gebruiken voor de migratie naar 4.3.

Voor een oudere implementatie volgt u deze richtlijnen om uw bestaande implementatie te upgraden naar BI-platform 4.3:

1. Als uw bestaande implementatie XI R2, XI MHF1, XI R2 SP1, BusinessObjects 5/6 of Crystal Enterprise 9/10 is, moet u eerst upgraden naar XI R2 SP2 (of hoger) en dan verdergaan bij stap 3.
2. Als uw bestaande implementatie XI 3.x is, kunt u direct bij stap 3 van de upgrade beginnen.
3. Installeer BI 4.1/4.2 SPx op een aparte computer en voer het hulpprogramma voor upgradebeheer uit vanuit 4.1/4.2 SPx om de inhoud te migreren van de bovengenoemde versies naar het BI 4.1/4.2 SPx-niveau.
4. Wanneer uw inhoud op het BI 4.1/4.2 SPx-niveau is, kiest u een van beide volgende methoden om over te stappen naar 4.3.
   1. Voer de installatiesoftware voor de update van BI 4.3.x uit op de computer op 4.1/4.2 SPx-niveau, of
   2. Installeer BI 4.3 op een aparte computer en gebruik het hulpprogramma voor doorgiftebeheer van BI 4.3.x om de inhoud te migreren van het BI 4.1/4.2 SPx-niveau naar het BI 4.3.x-niveau.

> **Opmerking**
>
> 1. Voor de migratie van de inhoud van het BI 4.1/4.2 SPx-niveau naar het BI 4.3.x-niveau, moet het hulpprogramma voor doorgiftebeheer van dezelfde versie zijn als die van het doel-CMS.
> 2. Zie de Migratiehandleiding en de Installatiehandleiding voor BI-platform voor uw versie op https://help.sap.com/viewer/product/

SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US voor meer informatie over de migratie van BusinessObjects 5/6 naar XI 3.1.

3. Met het hulpprogramma voor upgradebeheer (UMT) wordt alleen een upgrade van de server- en weblaagfuncties in uw implementatie uitgevoerd. Zie voor meer informatie over UMT de Upgradehandleiding voor Business Intelligence-platform voor uw versie, die beschikbaar is op https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US.

2.2.3 Belangrijkste taken

Afhankelijk van uw situatie kunt u specifieke secties in deze handleiding raadplegen en mogelijk zijn er nog andere bronnen die u kunt gebruiken. Voor elk van de volgende situaties worden er taken gesuggereerd die u kunt uitvoeren en informatie die u kunt lezen.

Verwante informatie

Voor het eerst een implementatie plannen of uitvoeren [pagina 31]
De implementatie configureren [pagina 32]
De systeemprestaties verbeteren [pagina 32]
Central Management Console (CMC) [pagina 28]

2.2.3.1 Voor het eerst een implementatie plannen of uitvoeren

Als u uw eerste implementatie van het BI-platform plant of uitvoert, is het raadzaam de volgende secties van deze handleiding te lezen:

- Teneinde vertrouwd te raken met de onderdelen van het BI-platform leest u “Overzicht van de architectuur”.
- “Communicatie tussen BI-platformonderdelen begrijpen”
- “Overzicht van beveiliging”
- Als u van plan bent om gebruik te maken van externe verificatie, leest u “Verificatieopties in het BI-platform”.
- Na de installatie leest u “Werken met het beheergebied Servers in de CMC”.

Zie de *Installatiehandleiding voor* SAP BusinessObjects Business Intelligence-platform voor meer informatie over het installeren van het BI-platform. Raadpleeg de *Planningshandleiding voor SAP BusinessObjects Business Intelligence-platform* als u wilt inventariseren wat nodig is en een implementatiearchitectuur wilt ontwerpen die daarbij past.

Verwante informatie

Overzicht architectuur [pagina 34]
Communicatie tussen BI-platformonderdelen [pagina 193]
Overzicht van beveiliging [pagina 151]
Verificatieopties in het BI-platform [pagina 231]
Werken met het beheergebied Servers in de CMC [pagina 415]

2.2.3.2 De implementatie configureren

Als u de installatie van BI-platform zojuist hebt voltooid en de eerste configuratietaken gaat uitvoeren, bijvoorbeeld de firewall en gebruikersbeheer configureren, is het raadzaam de volgende secties door te nemen.

Verwante informatie

Inleiding tot de wizard Systeemconfiguratie [pagina 87]
Communicatie tussen BI-platformonderdelen [pagina 193]
Overzicht van beveiliging [pagina 151]
Toezicht [pagina 804]

2.2.3.3 De systeemprestaties verbeteren

Als u de efficiëntie van uw implementatie wilt testen en de implementatie nauwkeurig wilt afstellen om resources te optimaliseren, leest u de volgende secties:

- Als u een implementatiesjabloon wilt gebruiken om uw systeem te configureren, leest u “Inleiding tot de wizard Systeemconfiguratie”.
- Als u toezicht wilt houden op het bestaande systeem, leest u “Toezicht”.
- Voor dagelijkse onderhoudstaken en procedures voor het werken met servers in de CMC leest u “Werken met het beheergebied Servers in de CMC”.

Verwante informatie

Inleiding tot de wizard Systeemconfiguratie [pagina 87]
Toezicht [pagina 804]
Werken met het beheergebied Servers in de CMC [pagina 415]

2.2.3.4 Werken met objecten in de CMC

Een object is een document of bestand dat wordt gemaakt in het BI-platform of andere software, en vervolgens in de gegevensopslagruimte van BI-platform wordt opgeslagen en beheerd. Als u werkt met objecten in de CMC, raadpleegt u de volgende secties:

- Zie "Overzicht van accountbeheer" voor informatie over het instellen van gebruikers en groepen in de CMC.
- Zie "De werking van rechten in het BI-platform" om beveiliging voor objecten in te stellen.
- Zie de *Gebruikershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor algemene informatie over het werken met objecten.

Verwante informatie

Overzicht van accountbeheer [pagina 99]
Werking van rechten in BI-platform [pagina 123]

3 Architectuur

3.1 Overzicht architectuur

Deze sectie biedt een overzicht van de platformarchitectuur, het systeem en de serviceonderdelen die samen het SAP BusinessObjects Business Intelligence-platform vormen. De informatie helpt beheerders inzicht te verkrijgen in essentiële systeeminstellingen en een plan op te stellen voor de implementatie, het beheer en het onderhoud van het systeem.

> **Opmerking**
>
> Voor een lijst met ondersteunde platforms, talen, databases, webtoepassingsservers, webservers en andere systemen die door deze release worden ondersteund, raadpleegt u de *Product Availability Matrix* (PAM) die beschikbaar is op http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540.

> **Opmerking**
>
> Omdat de PAM continue wordt bijgewerkt, raadpleegt u altijd de online versie van de PAM in plaats van de kopie uit de download.

Business Intelligence (BI) -platform is ontworpen voor optimale prestaties in vele verschillende gebruiks- en implementatiescenario's. U kunt plannings- en verwerkingstaken die veel van de processor vereisen, delegeren door specifieke servers te maken die specifieke services hosten. De architectuur voldoet in vrijwel elke BI-implementatie en is voldoende flexibel om te worden uitgebreid van een aantal gebruikers met één hulpprogramma tot tienduizenden gebruikers met meerdere hulpprogramma's en interfaces.

Ontwikkelaars kunnen het BI-platform in de andere technologiesystemen van hun organisatie integreren door middel van webservices, Java of .NET API's (Application Programming Interfaces).

Eindgebruikers kunnen rapporten weergeven, maken, bewerken en gebruiken met behulp van gespecialiseerde hulpprogramma's en toepassingen, waaronder:

- Clients die worden geïnstalleerd door het installatieprogramma van Clienthulpprogramma's voor het BI-platform:
  - Web Intelligence Rich Client
  - Business Views-beheer
  - Hulpprogramma voor universe-ontwerp
  - Query als een webservice
  - Hulpprogramma voor informatieontwerp (voorheen Information Designer)
  - Hulpprogramma voor vertaalbeheer (voorheen Translation Manager)
- Clients die afzonderlijk verkrijgbaar zijn:
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (voorheen Voyager)
  - BI-werkruimten (voorheen Dashboard Builder)

IT-afdelingen hebben hulpprogramma's voor gegevensbeheer en systeembeheer tot hun beschikking, waaronder:

- Rapportviewers
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Diagnostisch hulpprogramma voor gegevensopslagruimten (RDT)
- Data Federator-beheerprogramma
- Hulpprogramma voor universe-ontwerp (voorheen Universe Designer)
- SAP BusinessObjects Mobile

BI-platform-onderdelen kunnen op één computer of op vele computers worden geïnstalleerd, wat flexibiliteit, betrouwbaarheid en schaalbaarheid biedt. U kunt in bepaalde gevallen zelfs twee verschillende versies van het BI-platform gelijktijdig op dezelfde computer installeren, hoewel deze configuratie uitsluitend wordt aanbevolen als onderdeel van het upgradeproces of om tests uit te voeren.

Serverprocessen kunt u verticaal schalen (een aantal of alle serverprocessen worden op één computer uitgevoerd) om kosten te besparen of horizontaal schalen (serverprocessen worden verdeeld over twee of meer netwerkcomputers) om de prestaties te verbeteren. Het is ook mogelijk om meerdere, redundante versies van hetzelfde serverproces op meerdere computers uit te voeren, zodat de verwerking kan worden voortgezet als het primaire proces op een probleem stuit.

> **Opmerking**
>
> Hoewel het mogelijk is om Windows- en Unix- of Linux-platforms tegelijk te gebruiken, wordt het afgeraden om besturingssystemen door elkaar te gebruiken voor CMS-processen (Central Management Server).

3.1.1 Onderdeeldiagram

SAP BusinessObjects Business Intelligence-platform is een BI-platform (Business Intelligence) dat analyse- en rapportagehulpprogramma's op bedrijfsniveau biedt om informatieverstrekking te vergemakkelijken. Gegevens kunnen vanuit een groot aantal ondersteunde databasesystemen worden geanalyseerd (inclusief tekstsystemen of multidimensionale OLAP-systemen) en BI-rapporten kunnen in vele verschillende indelingen worden gepubliceerd naar vele verschillende publicatiesystemen.

In dit architectuurdiagram vindt u de BI-platformonderdelen, waaronder servers en clienthulpprogramma's, evenals aanvullende analyseproducten, webtoepassingsonderdelen en databases die deel uit kunnen maken van een BI-platformlandschap. Architectuurdiagram van BI 4.3.

Het BI-platform rapporteert via een alleen-lezenverbinding aan de databases van uw organisatie en gebruikt eigen databases voor het opslaan van configuratie- en controlegegevens en andere verwerkingsinformatie. De BI-rapporten die door het systeem worden gemaakt, kunnen naar een scala aan bestemmingen worden gestuurd, waaronder bestandssystemen en e-mailprogramma's, of worden geopend via websites of portals.

Het BI-platform is een zelfstandig systeem dat op één computer kan worden gebruikt (bijvoorbeeld als kleinschalige omgeving voor ontwikkelingen of preproductietests), of kan worden uitgebreid naar een cluster van vele computers die verschillende onderdelen uitvoeren (bijvoorbeeld als grootschalige productieomgeving).

3.1.2 Architectuurlagen

SAP BusinessObjects Business Intelligence-platform kan worden gezien als een reeks conceptuele lagen:

Clientlaag

De clientlaag bevat alle clienttoepassingen die in samenwerking met het BI-platform een groot aantal functies voor rapportage, analyse, en beheer bieden. Voorbeelden hiervan zijn de Central Configuration Manager (installatieprogramma van BI-platform), het hulpprogramma voor informatieontwerp (installatieprogramma voor clienthulpprogramma's van BI-platform) en SAP Crystal Reports (afzonderlijk verkrijgbaar en geïnstalleerd).

Vanaf SAP BI 4.3 zijn desktopclienttoepassingen (waaronder Web Intelligence Rich Client, het hulpprogramma voor informatieontwerp en het hulpprogramma voor universe-ontwerp) 64-bits toepassingen. Ze zijn niet langer 32-bits.

Weblaag

De weblaag bevat webtoepassingen die geïmplementeerd zijn op een Java-webtoepassingsserver. Webtoepassingen bieden BI-platformfunctionaliteit aan eindgebruikers via een webbrowser. Voorbeelden van webtoepassingen zijn de webinterface voor beheer van de CMC (Central Management Server), en BI-startpunt.

De weblaag bevat ook webservices. De webservices bieden BI-platformfunctionaliteit aan softwareprogramma's via de webtoepassingsserver, zoals sessieverificatie, beheer van gebruikersrechten, planning, zoeken, beheer, rapportage en querybeheer. LiveOffice is bijvoorbeeld een product dat gebruikmaakt van webservices om rapportagefunctionaliteit van het BI-platform te integreren in bepaalde Microsoft Office-producten.

Beheerlaag

Op de beheerlaag (ook wel Intelligence-laag genoemd) worden alle onderdelen van BI-platform gecoördineerd en aangestuurd. Deze laag bestaat uit de CMS (Central Management Server), de gebeurtenisserver en aanverwante services. De CMS onderhoudt beveiligings- en configuratiegegevens, verstuurt serviceaanvragen naar servers, beheert de controle en onderhoudt de CMS-systeemdatabase. De Event Server beheert bestandsgebeurtenissen, die plaatsvinden op een gedefinieerde opslaglaag.

Opslaglaag

De opslaglaag is verantwoordelijk voor de verwerking van bestanden, zoals documenten en rapporten.

De Input File Repository Server beheert bestanden met informatie die in rapporten moet worden gebruikt, zoals de volgende bestandstypen: `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, `.unv`, `.unx`.

> **Opmerking**
>
> De gegevensopslagruimte van het Input Repository Server-bestand wordt niet beheerd door het systeem. Een beheerder moet het controle- en beheerplan beheren.

De Output File Repository Server beheert rapporten die door het systeem gemaakt zijn, zoals de volgende bestandstypen: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

De opslaglaag is ook verantwoordelijk voor het in cache plaatsen van rapporten om systeembronnen te besparen wanneer gebruikers rapporten openen.

Verwerkingslaag

Op de verwerkingslaag worden gegevens geanalyseerd en rapporten en andere uitvoertypen gemaakt. Dit is de enige laag die toegang heeft tot de databases die rapportgegevens bevatten. Deze laag bestaat uit de Adaptive Job Server, de verbindingsserver (64-bits) en verwerkingsservers zoals de Adaptive Processing Server en de Crystal Reports-verwerkingsserver.

Gegevenslaag

De gegevenslaag bestaat uit de databaseservers die de CMS-systeemdatabase en de Controlegegevensopslag hosten. De laag bestaat ook uit databaseservers die relationele, OLAP- of andere gegevenstypen bevatten voor rapportage- en analysetoepassingen.

3.1.3 Databases

Het BI-platform gebruikt meerdere verschillende databases.

- Rapportagedatabases
  Dit verwijst naar de gegevens van uw organisatie. Het zijn de brongegevens die door SAP BusinessObjects Business Intelligence Suite-producten zijn geanalyseerd en gerapporteerd. De gegevens worden doorgaans opgeslagen in een relationele database, maar kunnen zich ook in tekstbestanden, Microsoft Office-documenten of OLAP-systemen bevinden.
- CMS-systeemdatabase
  De CMS-systeemdatabase wordt gebruikt om BI-platforminformatie op te slaan, zoals gegevens over gebruikers, servers, mappen, documenten, configuraties en verificatie. Deze informatie wordt beheerd door de CMS (Central Management Server) en hiernaar wordt soms verwezen als de *systeemgegevensopslagruimte*.
- Controlegegevensopslag
  De Controlegegevensopslag wordt gebruikt om informatie op te slaan over gebeurtenissen in het BI-platform die kunnen worden bijgehouden. Met behulp van deze informatie kunnen het gebruik

van systeemonderdelen, gebruikersactiviteit of andere aspecten van de dagelijkse werking worden gecontroleerd.

- Controledatabase
  Voor controle wordt de Controlegegevensopslagdatabase gebruikt om gegevens over systeemconfiguratie en onderdelen op te slaan voor SAP-ondersteuning.
- Commentaardatabase
  BI Commentary is een toepassing die is geïntroduceerd in de CMC. Hiermee kunnen gebruikers samenwerken door opmerkingen te plaatsen bij beschikbare gegevens/statistieken in een bepaald document.
  De commentaardatabase wordt in dezelfde database geconfigureerd als de controledatabase. Deze wordt standaard in de controledatabase gemaakt.

Als u geen databaseserver beschikbaar hebt om met de database van het CMS-systeem of Gegevensopslag controleren te gebruiken, kan het installatieprogramma van het BI-platform een database voor u installeren en configureren. Het verdient aanbeveling uw behoeften te evalueren op basis van de informatie die de leverancier van uw databaseserver biedt om te bepalen welke database hebt beste aansluit op de behoeften van uw onderneming.

> **Opmerking**
>
> De standaard-SQL Anywhere-database wordt niet aanbevolen voor productiesystemen. Deze is gebundeld met de BI-platformserverpakketten waarmee u het BI-platform onmiddellijk kunt implementeren en testen, maar heeft beperkte mogelijkheden voor het beheren van een database. Het wordt aanbevolen om SQL Anywhere in zijn volledige vorm of een bestaand ondersteund database-exemplaar te gebruiken voor een productiesysteem. Het is namelijk cruciaal dat uw CSM-systeem zich in uw datacenter bevindt. Het wordt beheerd door databasebeheerders die de juiste processen voor gegevensbeveiliging en beschikbaarheid van servers hebben ingesteld.

3.1.4 Servers, hosts en clusters

Het BI-platform bestaat uit serververzamelingen die op een of meer hosts worden uitgevoerd. Kleine installaties (zoals test- of ontwikkelingssystemen) kunnen één host gebruiken voor een webtoepassingsserver, een databaseserver en alle BI-platformservers.

Bij installaties van normale en grote omvang kunnen servers op meerdere hosts worden uitgevoerd. De host van een webtoepassingsserver kan bijvoorbeeld in combinatie met een BI-platformserverhost worden gebruikt. Dit maakt bronnen vrij op de BI-platformserverhost, zodat er meer informatie kan worden verwerkt dan wanneer er ook de webtoepassingsserver op wordt gehost.

Bij grote installaties kunnen er meerdere BI-platformserverhosts in een cluster samenwerken. Als een organisatie bijvoorbeeld een groot aantal SAP Crystal Reports-gebruikers heeft, kunnen verschillende Crystal Reports-verwerkingsservers op verschillende BI-platformserverhosts worden gemaakt. Op deze manier zijn er voldoende bronnen beschikbaar voor het verwerken van clientaanvragen.

Het gebruik van meerdere servers biedt de volgende voordelen:

- Verbeterde prestaties
  Meerdere BI-platformserverhosts kunnen een wachtrij met rapportagegegevens sneller verwerken dan één BI-platformserverhost.

- Taakverdeling
  Als een server zwaar wordt belast, stuurt de CMS nieuwe aanvragen automatisch naar andere servers in het cluster.
- Verbeterde beschikbaarheid
  Als er een onverwachte fout op een server optreedt, stuurt de CMS aanvragen automatisch naar andere servers tot de fout is verholpen.

3.1.5 Webtoepassingsservers

Een webtoepassingsserver fungeert als de vertaallaag tussen een webbrowser of rijke toepassing en het BI-platform. Er wordt ondersteuning geboden voor webtoepassingsservers die in Windows, Unix of Linux worden uitgevoerd.

Raadpleeg de *Supported Platforms/PARs* voor een uitgebreide lijst met ondersteunde webtoepassingsservers. Deze is beschikbaar op: https://support.sap.com/home.html.

Als u geen webtoepassingsserver hebt voor gebruik met het BI-platform, kan het installatieprogramma een Tomcat-webtoepassingsserver voor u installeren en configureren. Het verdient aanbeveling uw behoeften te evalueren op basis van de informatie die de leverancier van uw webtoepassingsserver biedt, om te bepalen welke webtoepassingsserver het beste aansluit op de behoeften van uw onderneming.

> **Opmerking**
>
> Wanneer u een productieomgeving configureert, is het raadzaam om de webtoepassingsserver op een apart systeem te hosten. Wanneer het BI-platform en een webtoepassingsserver op dezelfde host worden uitgevoerd in een productieomgeving, kan dit een nadelige invloed hebben op de prestaties.

3.1.5.1 Clustering inschakelen in de webtoepassing BI-startpunt om sessiefailover en schaalbaarheid te ondersteunen

In deze sectie wordt uitgelegd hoe clustering kan worden ingeschakeld in de webtoepassing BI-startpunt om sessiefailover en schaalbaarheid te ondersteunen. In deze sectie wordt ook uitgelegd wat de stappen zijn voor de configuratie van toepassingsservers van Apache Tomcat en WebSphere met hetzelfde doel.

Om clustering in te schakelen voor een toepassingsserver, zoals Tomcat of WebSphere, hebt u de volgende componenten nodig:

- Een HTTP-server
- Een compatibele taakverdeler
- Twee of meer toepassingsservers waarop de vereiste webtoepassing al is geïnstalleerd
- Een voltooide BOE-installatie (opslagruimte)

> **Opmerking**
>
> De stappen die in deze sectie worden beschreven zijn algemeen en kunnen worden gebruikt om clustering in te schakelen voor elke andere toepassing. De enige verschillen zijn de wijzigingen die zijn gemaakt in

de implementatie-descriptor van de webtoepassing (web.xml). Het is raadzaam de leverancier van uw webtoepassingsserver te raadplegen voor informatie over de configuratie van de taakverdeling van de weblaag.

3.1.5.1.1 Apache Tomcat installeren

Voer de volgende stappen uit om de Apache Tomcat-server te installeren:

1. Installeer de Apache HTTP-server.
2. Installeer de Apache Tomcat-server op de computers.
3. Download mod_jk (taakverdeler) en sla deze op in de opslagruimte "modules" op de Apache HTTPD-server van http://tomcat.apache.org/download-connectors.cgi .
4. Voer SI-agent uit op een computer met een volledige installatie van BOE al geïnstalleerd.

> **Opmerking**
>
> Start uw HTTP-server om de compatibiliteit voor mod_jk te controleren. Er verschijnt een foutmelding op de console als de gedownloade versie van mod_jk niet compatibel is met uw versie van de HTTP-server.

Apache Tomcat configureren

Voer de volgende stappen uit om Apache Tomcat te configureren:

1. Configureer de Apache HTTP-server.
   a. Configureer httpd.conf (taakverdeler, webtoepassing laden, toezicht, pad naar bestand worker.properties).
   b. Configureer het bestand workers.properties en sla het op in de Apache\Conf-bibliotheek.

C:\Server\Apache2\Apache2\conf\httpd.conf - Notepad++

File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?

httpd.conf | httpd.default.conf

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

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

Load Tomcat Connector (mod_jk)

2. Configureer server.xml in Tomcat (voeg clusteringcodes toe).
   a. In server.xml, het jvmRoute-attribuut moet overeenkomen met de naam die u hebt gebruikt in het bestand workers.properties.
   b. Als u Tomcat 8 of hoger gebruikt, verwijder dan JvmRouteSessionIDBinderListener (afgekeurd).
3. Voeg een distribueerbare code toe aan het bestand web.xml (implementatie-descriptor) van de webtoepassing waarvan u wilt dat clustering wordt ondersteund.

De aangepaste waarde die de standaardwaarde aanroept voor elke aanvraag wordt hieronder weergegeven. Als u Tomcat 8 gebruikt, vervangt u in alle server.xml-bestanden van Tomcat:

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

door

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

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

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

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

4. Exporteer de jar voor de aangepaste waarde (als wijzigingen nodig zijn) van de code. Kopieer het bestand `forcereplicationvalve.jar` in `<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` en plak dit in `<TomcatInstallDir>/tomcat/lib` (in alle Tomcat-knooppunten).
5. Sla deze jar op in de map `tomcat/lib` van elk exemplaar.
6. Start alle servers opnieuw.

> **Opmerking**
>
> - We bevelen aan om de servers één voor één te starten; wacht totdat een server volledig is gestart voordat u de volgende server start.
> - Gebruik localhost:6400 niet als systeemnaam in het aanmeldscherm voor het startpunt. Geef de naam (of IP) op van de specifieke BOE-installatiecomputer. Zorg dat er een SI-agent wordt uitgevoerd op deze installatie.
> - Verken het attribuut channelSendOptions voor de meest geschikte optie. Het wordt gebruikt om opties in te stellen voor synchrone respons, asynchrone respons enzovoort.
> - Als u de jar exporteert voor de standaardwaarde van de code, maak dan ook een geldige pakkethiërarchie voor de jar en voeg deze hiërarchie toe aan server.xml.

3.1.5.1.2 WebSphere installeren

WebSphere configureren

Voer de volgende stappen uit om WebSphere te configureren:

1. Voeg een distribueerbare tag toe in web.xml of BOE-webapp voor beide exemplaren van de WebSphere-toepassingsserver.
2. Ga in de IBM-console naar *Alle servers* > *lid1* > *Sessiebeheer*.
   a. Controleer cookies en schakel ze in.
   b. Schakel *Seriële toegang toestaan* in en wijzig de time-out naar 10 seconden.
3. Navigeer naar *Instellingen distributie-omgeving* > *Herhalingsproces geheugen-naar-geheugen*.
   a. Maak een herhalingsdomein en selecteer het.
   b. Selecteer de herhalingsmodus – zowel de client als de server.
4. Selecteer van elk exemplaar in *Alle servers* hetzelfde herhalingsdomein als dat u hebt geselecteerd in de vorige stap.
5. Navigeer naar *Instellingen distributie-omgeving* > *Aangepaste tuningparameters*.
   a. Selecteer voor failover *Laag* als het tuningniveau.
6. Start alle servers opnieuw.

3.1.5.2 Containerserver voor webtoepassingen (WACS)

Er is een webtoepassingsserver vereist om webtoepassingen van het BI-platform te hosten.

Als u een geavanceerde beheerder van Java-webtoepassingsservers bent met geavanceerde beheervereisten, is het aan te raden om een ondersteunde Java-webtoepassingsserver te gebruiken om BI-platformwebtoepassingen te hosten. Als u een ondersteund Windows-besturingssysteem gebruikt om het BI-platform te hosten en de voorkeur geeft aan een eenvoudig installatieproces voor de webtoepassingsserver, of als u geen rechten hebt om een Java-webtoepassingsserver te beheren, kunt u de Containerservice voor webtoepassingen installeren wanneer u het BI-platform installeert.

De Containerserver voor webtoepassingen is een BI-platformserver waarmee BI-platformwebtoepassingen, zoals de CMC (Central Management Console), BI-startpunt en webservices, uitgevoerd kunnen worden zonder eerst de Java-webtoepassingsserver te installeren.

Het gebruik van de WACS biedt een aantal voordelen:

- U kunt de WACS zeer eenvoudig installeren, onderhouden en configureren. De installatie en configuratie worden uitgevoerd door het installatieprogramma van het BI-platform en er zijn geen verdere stappen nodig om ermee aan de slag te gaan.
- Met de WACS zijn serverbeheer en onderhoudstaken voor Java-toepassingen niet nodig.
- De Containerserver voor webtoepassingen bevat een beheerinterface die consistent is met andere BI-platformservers.
- Net als andere BI-platformservers kan de Containerserver voor webtoepassingen op een specifieke host geïnstalleerd worden.

> **Opmerking**
>
> Het gebruik van een WACS in plaats van een specifieke Java-webtoepassingsserver kent een aantal beperkingen:

- WACS is alleen beschikbaar op ondersteunde Windows-besturingssystemen.
- Aangepaste webtoepassingen kunnen niet op de Containerserver voor webtoepassingen worden geïmplementeerd, aangezien alleen de webtoepassingen worden ondersteund die bij het BI-platform worden geïnstalleerd.
- WACS kan niet worden gebruikt met Apache-taakverdeling.

Het is mogelijk om naast WACS een specifieke webtoepassingsserver te gebruiken. Deze specifieke webtoepassingsserver kan dan aangepaste webtoepassingen hosten, terwijl de CMC en andere webtoepassingen van het BI-platform door de Containerserver voor webtoepassingen worden gehost.

3.1.6 Software Development Kits

Met een Software Development Kit (SDK) kan een ontwikkelaar aspecten van SAP BusinessObjects Business Intelligence-platform opnemen in de eigen toepassingen en systemen van een organisatie.

Het BI-platform heeft SDK's voor softwareontwikkeling op Java- en .NET-platforms.

> **Opmerking**
>
> De BI-platform .NET SDK's zijn niet standaard geïnstalleerd en moeten worden gedownload van de SAP Service Marketplace.

De volgende SDK's worden ondersteund door het BI-platform:

- Java SDK en .NET SDK van Business Intelligence -platform
  Met de SDK's van BI-platform kunnen toepassingen taken uitvoeren zoals verificatie, sessiebeheer, werken met gegevensopslagobjecten, rapportplanning en -publicatie, en serverbeheer.

  > **Opmerking**
  >
  > Gebruik de Java SDK voor volledige toegang tot functies voor beveiliging, serverbeheer en controle.

- Business Intelligence-platform RESTful webservice SDK
  Met de BI-platform RESTful-webservices SDK hebt u toegang tot het BI-platform via het HTTP-protocol. U kunt deze SDK gebruiken om u aan te melden bij het BI-platform, door de gegevensopslagruimte van het BI-platform te navigeren, bronnen op te roepen en eenvoudige planningstaken voor bronnen uit te voeren. U krijgt toegang tot deze SDK door toepassingen te schrijven die een programmeertaal gebruiken die het HTTP-protocol ondersteunt, of door een hulpprogramma te gebruiken dat HTTP-verzoeken ondersteunt.
- Java Consumer SDK en .NET Consumer SDK van Business Intelligence-platform
  Een implementatie van SOAP-webservices waarmee u gebruikersverificatie en -beveiliging, toegang tot documenten en rapporten, planning, publicaties en serverbeheer kunt verwerken.
  BI-platformwebservices maken gebruik van standaarden als XML, SOAP, AXIS 2.0 en WSDL. Het platform voldoet aan de webservicesspecificatie WS-Interoperability Basic Profile 1.0.

  > **Opmerking**
  >
  > Webservicetoepassingen worden momenteel alleen ondersteund met de volgende configuraties voor de taakverdeler:
  > 1. Persistentie van bron-IP-adres.
  > 2. Persistentie van bron-IP en doelpoort (alleen beschikbaar op een Cisco Content Services Switch).

3. SSL-persistentie.
4. Sessiebehoud door cookies.

> **Opmerking**
>
> SSL-persistentie leidt mogelijk tot problemen met de beveiliging en betrouwbaarheid in bepaalde webbrowsers. Vraag uw netwerkbeheerder of SSL-persistentie van toepassing is op uw organisatie.

- Data Access Driver en Connection Java SDK's
  Met behulp van deze SDK's kunt u databasestuurprogramma's voor de Verbindingsserver maken en databaseverbindingen beheren.
- Java SDK met semantische laag
  Met de Semantic Layer Java SDK kunt u een Java-toepassing ontwikkelen die beheer- en beveiligingstaken voor universes en verbindingen uitvoert. U kunt bijvoorbeeld services implementeren om een universe naar een gegevensopslagruimte te implementeren of om een beveiligde verbinding vanuit de gegevensopslagruimte op te halen naar uw werkruimte. Deze toepassing kan worden ingesloten in BI-platformoplossingen die het BI-platform als OEM integreren.
- Report Application Server Java SDK en .NET SDK
  Met de Report Application Server SDK's kunnen toepassingen bestaande Crystal Reports-rapporten openen, maken en wijzigen, waaronder parameterwaarden instellen, gegevensbronnen wijzigen en exporteren naar andere indelingen, zoals XML, PDF, Microsoft Word en Microsoft Excel.
- Java en .NET Crystal Reports-rapportviewers
  Met de viewers kunnen toepassingen Crystal Reports-rapporten weergeven en exporteren. De volgende viewers zijn beschikbaar:
  - DHTML-rapportpaginaviewer: hiermee worden gegevens weergegeven en kunt u analyses op lager niveau uitvoeren, door pagina's navigeren, zoomen, vragen stellen, zoeken, markeren, exporteren en afdrukken.
  - Rapportonderdeelviewer: hiermee wordt de mogelijkheid geboden individuele onderdelen van een rapport weer te geven, waaronder diagrammen, tekst en velden.
- Report Engine Java SDK en .NET SDK
  Via de Report Engine SDK's kunnen toepassingen communiceren met rapporten die gemaakt zijn met SAP BusinessObjects Web Intelligence.
  De Report Engine SDK's bevatten bibliotheken die u kunt gebruiken om een hulpprogramma voor het ontwerpen van webrapporten te bouwen. Met de toepassingen die met deze SDK's zijn gebouwd, kunt u verschillende Web Intelligence-documenten weergeven, maken of wijzigen. Gebruikers kunnen documenten wijzigen door objecten zoals tabellen, diagrammen, voorwaarden en filters toe te voegen, te verwijderen en aan te passen.
- SDK van Platform zoeken: De SDK van Platform zoeken is de interface tussen de clienttoepassing en de service van Platform zoeken. Platform zoeken biedt ondersteuning voor Openbare SDK die wordt geleverd als onderdeel van de SDK van Platform zoeken.
  Wanneer een zoekopdrachtparameter via de clienttoepassing naar de SDK-laag wordt verzonden, wordt de opdrachtparameter door de SDK-laag naar een XML-gecodeerde indeling geconverteerd en vervolgens doorgestuurd naar de service voor Platform zoeken.

De SDK's kunnen samen worden gebruikt voor een breed aanbod aan BI-functies voor uw toepassingen. Zie de productpagina van SAP BusinessObjects Business Intelligence-platform voor meer informatie over deze SDK's, waaronder handleidingen voor ontwikkelaars en API-verwijzingen.

3.1.7 Gegevensbronnen

3.1.7.1 Universes

De universe is een semantische laag die de complexiteit van gegevens vereenvoudigt, door het gebruik van begrijpelijke taal voor de toegang, bewerking en indeling van gegevens. Deze taal wordt opgeslagen in de vorm van objecten in een universebestand. Web Intelligence, Crystal Reports-rapporten en andere toepassingen gebruiken universes om het maken van eenvoudige tot complexe eindgebruikersquery's en -analyses te vereenvoudigen.

Universes zijn een kernonderdeel van het BI-platform. Alle universeobjecten en de bijbehorende verbindingen worden door de verbindingsserver opgeslagen en beveiligd in de centrale gegevensopslagruimte. Clienthulpprogramma's voor het ontwerpen van universes moeten zich bij het BI-platform aanmelden om toegang te krijgen tot het systeem en universes te maken. Universetoegang en beveiliging op rij-/kolomniveau kunnen ook in de ontwerpomgeving worden beheerd op groepsniveau of op het niveau van afzonderlijke gebruikers.

De semantische laag stelt Web Intelligence in staat documenten beschikbaar te maken, door meerdere gesynchroniseerde gegevensbronnen te gebruiken, zoals OLAP- (online analytical processing) en CWM-gegevensbronnen (Common Warehousing Metamodel).

3.1.7.2 Business Views

Business Views heft voor rapportontwikkelaars de complexiteit van gegevens op, waardoor het maken van rapporten en interactie eenvoudiger worden. Met Business Views-weergaven kunnen gegevensverbindingen, gegevenstoegang, bedrijfsonderdelen en toegangscontrole gescheiden worden.

Business Views-weergaven kunnen alleen worden gebruikt door Crystal Reports en zijn bedoeld voor vereenvoudiging van de gegevenstoegang en de weergavebeveiliging die vereist zijn bij het maken van Crystal Reports-rapporten. U kunt in Business Views meerdere gegevensbronnen in één weergave gebruiken. Business Views-weergaven worden volledig ondersteund in het BI-platform.

3.1.8 Verificatie en eenmalige aanmelding

Systeembeveiliging wordt uitgevoerd door de CMS (Central Management Server), door beveiligingsinvoegtoepassingen en verificatieprogramma's van derden, zoals SiteMinder en Kerberos. Deze onderdelen zorgen voor de verificatie en autorisatie van gebruikers die toegang willen tot het BI-platform en de bijbehorende mappen, en andere objecten.

De volgende beveiligingsinvoegtoepassingen voor verificatie bij eenmalige aanmelding van gebruikers zijn beschikbaar:

- Enterprise (standaard), inclusief ondersteuning voor vertrouwde verificatie voor gebruik met verificatiemethoden zoals SAML, X.509, SAP NW SSO en andere methoden die door uw toepassingsserver worden ondersteund.
- LDAP

- AD (Windows Active Directory)

Op een ERP-systeem (Enterprise Resource Planning) wordt eenmalige aanmelding gebruikt om gebruikerstoegang tot het ERP-systeem te verifiëren, zodat rapporten kunnen worden vergeleken met ERP-gegevens. De volgende verificatie voor eenmalige aanmelding van gebruikers bij ERP-systemen wordt ondersteund:

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

3.1.8.1 Beveiligingsinvoegtoepassingen

Beveiligingsinvoegtoepassingen automatiseren de aanmaak en het beheer van accounts doordat u gebruikersaccounts en groepen van externe systemen kunt toewijzen in het BI-platform. U kunt gebruikersaccounts van derden toewijzen aan bestaande Enterprise-gebruikersaccounts, of u kunt nieuwe Enterprise-gebruikersaccounts maken die overeenkomen met elke toegewezen vermelding in het externe systeem.

De externe gebruikers en groepen worden door de beveiligingsinvoegtoepassingen dynamisch onderhouden. Wanneer u een LDAP-groep (Lightweight Directory Access Protocol) of in Windows een AD-groep (Active Directory) aan het BI-platform hebt toegewezen, kunnen alle gebruikers binnen deze groep zich aanmelden bij het BI-platform. Wijzigingen die hierna in het groepslidmaatschap van derden worden aangebracht, worden automatisch doorgevoerd.

In het BI-platform worden de volgende beveiligingsinvoegtoepassingen ondersteund:

- Enterprise-beveiligingsinvoegtoepassing
  De CMS (Central Management Server) beheert beveiligingsgegevens, zoals gebruikersaccounts, groepslidmaatschappen en objectrechten, waarmee de rechten voor gebruikers en groepen worden gedefinieerd. Dit wordt ook wel Enterprise-verificatie genoemd.
  Enterprise-verificatie is altijd ingeschakeld en kan niet worden uitgeschakeld. Gebruik de standaard Enterprise-verificatie als u afzonderlijke accounts en groepen voor het BI-platform wilt maken of als u nog geen hiërarchie van gebruikers en groepen hebt gemaakt op een LDAP- of Windows AD-server.
  Vertrouwde verificatie is een onderdeel van Enterprise-verificatie die oplossingen voor eenmalige aanmelding van derden integreert, zoals JAAS (Java Authentication and Authorization Service). Bij toepassingen die vertrouwd zijn voor de Central Management Server, kunnen gebruikers zich met Vertrouwde verificatie aanmelden zonder hun wachtwoord op te geven.
- LDAP-beveiligingsinvoegtoepassing
- Windows AD

> **Opmerking**
>
> Hoewel gebruikers Windows AD-verificatie voor het BI-platform en aangepaste toepassingen via de CMC kunnen configureren, bieden de CMC en BI-startpunt zelf geen ondersteuning voor Windows AD-verificatie met NTLM. De enige verificatiemethoden die door de CMC en BI-startpunt worden ondersteund, zijn Windows AD met Kerberos, LDAP, Enterprise en Vertrouwde verificatie.

3.1.8.2 Integratie met ERP (Enterprise Resource Planning)

Een ERP-toepassing (Enterprise Resource Planning) biedt ondersteuning voor de essentiële functies van de processen in een organisatie, doordat in realtime informatie wordt verzameld over de dagelijkse bewerkingen. Het BI-platform ondersteunt eenmalige aanmelding en rapportage op de volgende ERP-systemen:

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

> ⓘ Opmerking
>
> - Ondersteuning voor SAP ERP en BW wordt standaard geïnstalleerd. Gebruik de installatieoptie *Aangepast / Uitgebreid* om de ondersteuning voor SAP-integratie te deselecteren als u geen ondersteuning wilt voor SAP ERP of BW.
> - Ondersteuning voor Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne of PeopleSoft wordt niet standaard geïnstalleerd. Gebruik de installatieoptie *Aangepast / Uitgebreid* als u de integratie voor niet-SAP ERP-systemen wilt selecteren en installeren.

Voor meer informatie over de specifieke versies die door het BI-platform worden ondersteund, raadpleegt u de *Supported Platforms/PARs* op https://support.sap.com/home.html.

Als u ERP-integratie wilt configureren, raadpleegt u het hoofdstuk *Aanvullende configuraties voor ERP-omgevingen* van deze handleiding.

3.1.9 SAP-integratie

Het BI-platform kan met uw bestaande SAP-infrastructuur worden geïntegreerd met de volgende SAP-hulpprogramma's:

- SAP System Landscape Directory (SLD)
  De System Landscape Directory (SLD) van SAP NetWeaver is de centrale bron van systeemlandschapsgegevens voor het beheer van de softwarelevenscyclus. Wanneer u een map verstrekt met informatie over alle software die geïnstalleerd kan worden en verkrijgbaar is bij SAP, evenals automatisch bijgewerkte gegevens over systemen die al in een landschap geïnstalleerd zijn, legt u de grondslag voor hulpprogramma-ondersteuning om taken voor de softwarelevenscyclus in uw systeemlandschap te plannen.
  Het installatieprogramma van het BI-platform registreert de leveranciers- en productnamen en -versies bij het systeemlandschap, evenals namen, versies en locaties van server- en front-end-onderdelen.
- SAP Solution Manager
  SAP Solution Manager is een platform dat de geïntegreerde inhoud, hulpprogramma's en methodes biedt waarmee de SAP- en niet-SAP-oplossingen in een organisatie kunnen worden geïmplementeerd, bediend, ondersteund en gecontroleerd.
  Software die niet van SAP is met een SAP-gecertificeerde integratie wordt in een centrale gegevensopslagruimte geplaatst en automatisch naar uw SAP-SLD's (System Landscape Directories) overgedragen. SAP-klanten kunnen vervolgens eenvoudig aangeven welke versie van productintegratie van

derden door SAP is gecertificeerd in hun SAP-systeemomgeving. Deze service biedt nog meer herkenning voor producten van derden, naast de online catalogi voor producten van derden.
SAP Solution Manager is gratis beschikbaar voor SAP-klanten en omvat directe toegang tot SAP-ondersteuning en informatie over paden voor SAP-productupgrades. Voor meer informatie over SLD leest u "Registratie van het BI-platform in het systeemlandschap".

- Change and Transport System (CTS+)
  Het CTS helpt u om ontwikkelingsprojecten in ABAP Workbench en in Customizing te organiseren, en de wijzigingen vervolgens tussen de SAP-systemen in uw systeemlandschap over te dragen. Naast ABAP-objecten kunt u ook Java-objecten (J2EE, JEE) en SAP-specifieke niet-ABAP-technologieën (zoals Web Dynpro Java of SAP NetWeaver Portal) in uw landschap overdragen.
- Toezicht houden met CA Wily Introscope
  CA Wily Introscope is een product voor webtoepassingsbeheer voor controle en diagnose van prestatieproblemen die kunnen optreden binnen op Java gebaseerde SAP-modules in de productieomgeving. Zo kunt u inzicht verkrijgen in aangepaste Java-toepassingen en verbindingen met back-end-systemen. Met behulp van het product kunt u knelpunten identificeren in NetWeaver-modules, waaronder afzonderlijke servlets, JSP's, EJB's, JCO's, klassen, methodes en meer. Het programma biedt controle in real time met lage overheads, end-to-end transactiezichtbaarheid, historische gegevens voor analyse- of capaciteitsplanning, aanpasbare dashboards, geautomatiseerde drempelsignalen en een open architectuur om controle uit te breiden tot buiten NetWeaver-omgevingen.

3.1.10 Geïntegreerde versiecontrole

De bestanden van het BI-platform in een serversysteem worden beheerd door versiecontrole. Het Subversion-versiecontrolesysteem wordt door het installatieprogramma geïnstalleerd en geconfigureerd. U kunt ook gegevens invoeren om een bestaand Subversion- of Clearcase-versiecontrolesysteem te gebruiken.

Met een versiecontrolesysteem kunt u verschillende versies van configuratie- en andere bestanden bewaren en herstellen, waardoor het altijd mogelijk is om het systeem terug te zetten naar een bekende status op een willekeurige tijd in het verleden.

3.2 Servers, services, knooppunten en hosts

In het BI-platform worden de termen server en service gebruikt om te verwijzen naar de twee typen software die op een computer met het BI-platform worden uitgevoerd.

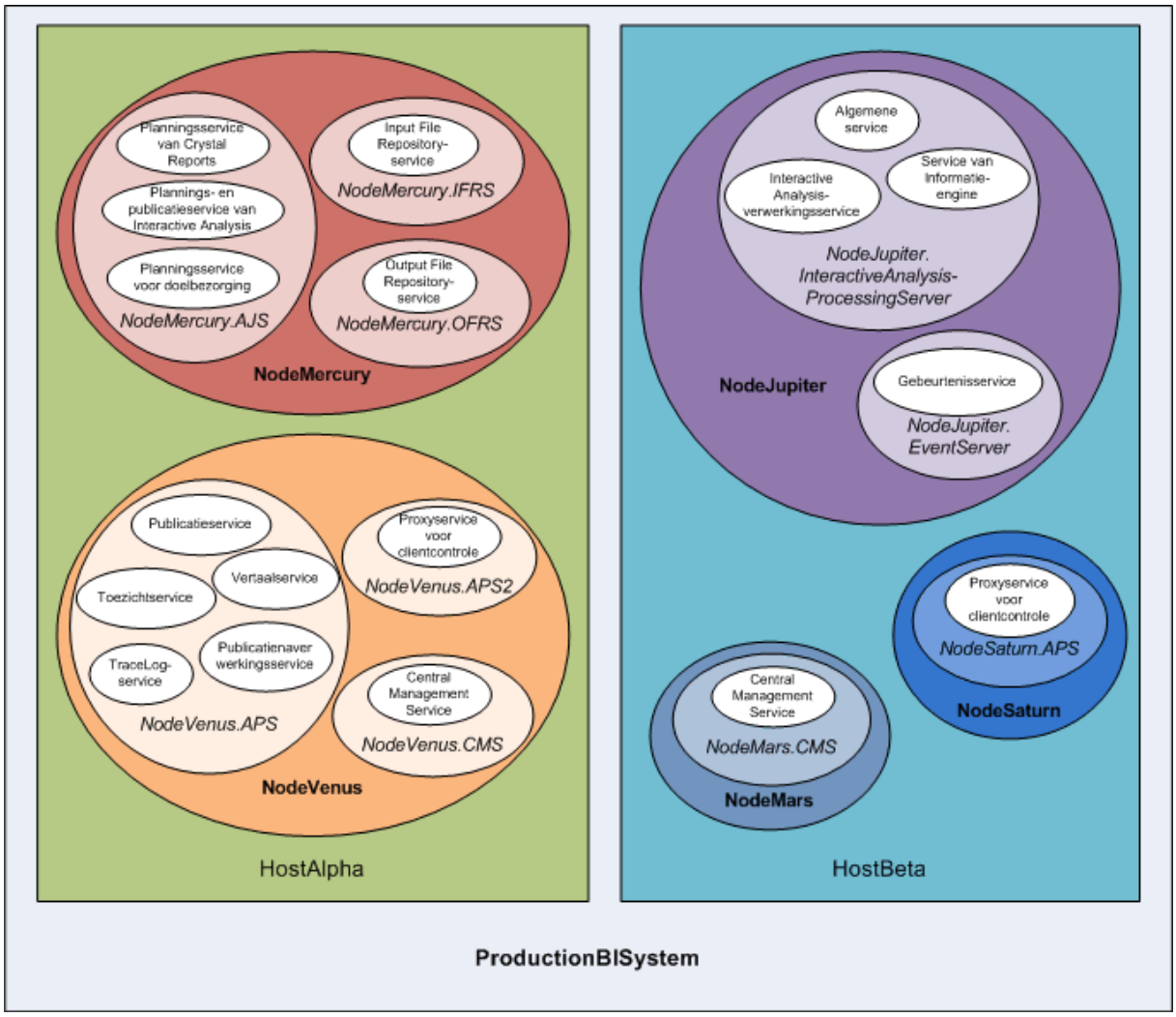
De term "server" wordt gebruikt om een proces op besturingssysteemniveau te beschrijven (op sommige systemen heet dit een daemon), dat een of meer services host. De CMS (Central Management Server) en de Adaptive Processing Server bijvoorbeeld, zijn servers. Servers worden uitgevoerd onder een bepaald besturingssysteemaccount en hebben een eigen PID (proces-id).

Een service is een serversubsysteem dat een specifieke functie heeft. De service wordt uitgevoerd in de geheugenruimte van de bijbehorende server, onder de proces-id van de bovenliggende container (server). De plannings- en publicatieservice van Web Intelligence is bijvoorbeeld een subsysteem dat op de Adaptive Job Server wordt uitgevoerd.

Een knooppunt is een verzameling BI-platformservers die worden uitgevoerd op dezelfde host en worden beheerd via dezelfde SIA (Server Intelligence Agent). Een host kan meerdere knooppunten bevatten.

Het BI-platform kan op één computer worden geïnstalleerd, op een aantal computers in een intranet of in een WAN (Wide Area Network).

In het volgende diagram wordt een hypothetische installatie van het BI-platform weergegeven. Het aantal hosts, knooppunten, servers en services, evenals het type servers en services, zal verschillen in daadwerkelijke installaties.



Twee hosts vormen het cluster met de naam ProductionBISystem:

- Op de host genaamd HostAlpha is het BI-platform geïnstalleerd en geconfigureerd voor twee knooppunten:
  - NodeMercuy bevat een Adaptive Job Server (`NodeMercury.AJS`) met services voor het plannen en publiceren van rapporten, een Input File Repository Server (`NodeMercury.IFRS`) met een service voor het opslaan van invoerrapporten, en een Output File Repository Server (`NodeMercury.OFRS`) met een service voor het opslaan van rapportuitvoer.
  - NodeVenus bevat een Adaptive Processing Server (`NodeVenus.APS`) met functies voor publiceren, controleren en vertalen, een Adaptive Processing Server (`NodeVenus.APS`) met een service voor

clientcontrole, en een Central Management Server (`NodeVenus.CMS`) met een service voor de CMS-services.

- Op de host genaamd HostBeta is het BI-platform geïnstalleerd en geconfigureerd voor drie knooppunten:
  - `NodeMars` bevat een Central Management Server (NodeMars.CMS) met een service voor de CMS-services. Als u de CMS op twee computers installeert, beschikt u over mogelijkheden voor taakverdeling, risicobeperking en failover.
  - NodeJupiter bevat een Web Intelligence-verwerkingsserver (`NodeJupiter.Web Intelligence`) met een service voor Web Intelligence-rapportage en een gebeurtenisserver (`NodeJupiter.EventServer`) voor rapportcontrole van bestanden.
  - NodeSaturn bevat een Adaptive Processing Server (`NodeSaturn.APS`) met een service voor clientcontrole.

3.2.1 Serverwijzigingen sinds XI 3.1

In de onderstaande tabel worden de belangrijkste wijzigingen in de BI-platformservers na XI 3.1 beschreven. Soorten wijzigingen zijn onder meer:

- Servers die een andere naam hebben gekregen, maar wat betreft functionaliteit niet of nauwelijks zijn veranderd.
- Servers die niet meer zijn opgenomen in nieuwere versies.
- Gemeenschappelijke of aan elkaar gerelateerde services die zijn samengevoegd in de Adaptive Servers. Bijvoorbeeld: de planningsservices die in XI 3.1 door afzonderlijke Job Servers werden uitgevoerd, zijn vanaf versie 4.0 verplaatst naar de Adaptive Job Server.
- Nieuwe servers die zijn geïntroduceerd.

Serverwijzigingen

XI 3.1	4.0	4.0 Functiepakket 3	4.1	4,2	4,3
Verbindingsserver [1]	Verbindingsserver Verbindingsserver 32	Verbindingsserver Verbindingsserver 32	Verbindingsserver Verbindingsserver 32	Verbindingsserver Verbindingsserver 32	Verbindingsserver Verbindingsserver 32
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports-verwerkingsserver	Crystal Reports 2011-verwerkingsserver Crystal Reports-verwerkingsserver (voor SAP Crystal Reports for Enterprise-rapporten)	Crystal Reports 2011-verwerkingsserver Crystal Reports-verwerkingsserver (voor SAP Crystal Reports for Enterprise-rapporten)	Crystal Reports 2013-verwerkingsserver Crystal Reports-verwerkingsserver (voor SAP Crystal Reports for Enterprise-rapporten)	Crystal Reports 2016-verwerkingsserver Crystal Reports-verwerkingsserver (voor SAP Crystal Reports for Enterprise-rapporten)	Crystal Reports 2020-verwerkingsserver Crystal Reports-verwerkingsserver (voor SAP Crystal Reports for Enterprise-rapporten)

XI 3.1	4.0	4.0 Functiepakket 3	4.1	4,2	4,3
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (BI-werkruimten)	Niet meer beschikbaar vanaf versie 4.0 Functiepakket 3	Niet beschikbaar in 4.1	Niet beschikbaar in 4.2	Niet beschikbaar in 4.3
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (BI-werkruimten)	Niet meer beschikbaar vanaf versie 4.0 Functiepakket 3	Niet beschikbaar in 4.1	Niet beschikbaar in 4.2	Niet beschikbaar in 4.3
Desktop Intelligence Cache Server [3]	Niet meer beschikbaar vanaf versie 4.0	Niet meer beschikbaar vanaf versie 4.0	Niet beschikbaar in 4.1 [3]	Niet beschikbaar in 4.2 [3]	Niet beschikbaar in 4.3 [3]
Desktop Intelligence Job Server [3]	Niet meer beschikbaar vanaf versie 4.0	Niet meer beschikbaar vanaf versie 4.0	Niet beschikbaar in 4.1 [3]	Niet beschikbaar in 4.2 [3]	Niet beschikbaar in 4.3 [3]
Desktop Intelligence-verwerkingsserver [3]	Niet meer beschikbaar vanaf versie 4.0	Niet meer beschikbaar vanaf versie 4.0	Niet beschikbaar in 4.1 [3]	Niet beschikbaar in 4.2 [3]	Niet beschikbaar in 4.3 [3]
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Multi-Dimensional Analysis Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2013 Report Application Server (RAS)	Crystal Reports 2016 Report Application Server (RAS)	Crystal Reports 2020 Report Application Server (RAS)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius-cacheserver [4]	Dashboard Design-cacheserver (Xcelsius) [5]	Dashboards-cacheserver (Xcelsius) [5]	Dashboards-cacheserver (Xcelsius) [5]	Dashboards-cacheserver (Xcelsius) [5]	Niet beschikbaar in 4.3 [7]
Xcelsius-verwerkingsserver [4]	Dashboard Design-verwerkingsserver (Xcelsius) [5]	Dashboards-verwerkingsserver (Xcelsius)	Dashboards-verwerkingsserver (Xcelsius)	Dashboards-verwerkingsserver (Xcelsius)	Niet beschikbaar in 4.3 [7]
Inhoudspecifieke webonderdelen [6]	Crystal Reports-rapportviewer, Xcelsius-viewer en Analytische rapportviewer	Crystal Reports-rapportviewer, Xcelsius-viewer en Analytische rapportviewer	Crystal Reports-rapportviewer, Xcelsius-viewer en Analytische rapportviewer	Crystal Reports-rapportviewer, Xcelsius-viewer en Analytische rapportviewer	Inhoudspecifieke webonderdelen worden verwijderd in 4.3

- [1] In versie 4.0 is Verbindingsserver 32 32-bits en verzorgt deze de verbindingen met gegevensbronnen die 64-bits middleware niet ondersteunen. Verbindingsserver is 64-bits en verzorgt verbindingen met alle andere gegevensbronnen. Zie de *Handleiding voor gegevenstoegang* voor meer informatie.
- [2] De Dashboard Server en Dashboard Analytics Server zijn verwijderd in versie 4.0 Functiepakket 3. De serverconfiguratie is niet meer nodig voor BI-werkruimtefunctionaliteit (voorheen Dashboard Builder in XI 3.1).
- [3] Desktop Intelligence was niet beschikbaar in 4.0 en 4.0-onderhoudspakketten. De Desktop Intelligence-clienttoepassing is beschikbaar in versie 4.1, maar Desktop Intelligence-servers zijn niet beschikbaar in 4.1. Desktop Intelligence-rapporten kunnen worden geconverteerd naar Web Intelligence-documenten via het hulpprogramma Rapportconversie.
- [4] De cache- en verwerkingsservices van Xcelsius zijn geïntroduceerd in XI 3.1 Service Pack 3 om Query als een webservice-aanvragen op relationele gegevensbronnen van Xcelsius te optimaliseren. Equivalente cache- en verwerkingsservices zijn beschikbaar in de Dashboards-cacheserver en de Dashboards-verwerkingsserver die in versie 4.0 Functiepakket 3 zijn geïntroduceerd.
- [5] De naam Dashboard Design-servers in versie 4.0 is gewijzigd in "Dashboards" in versie 4.0 Functiepakket 3 in overeenstemming met de wijziging van de productnaam naar SAP BusinessObjects Dashboards.
- [6] De volgende inhoudspecifieke webonderdelen worden verwijderd in 4.3:
  - Crystal Reports-rapportviewer
  - Xcelsius-viewer
  - Analytische rapportviewer
- [7] Dashboards-verwerkingsserver (Xcelsius) en Dashboards-cacheserver (Xcelsius) worden beide verwijderd.

3.2.2 Services

Wanneer u servers toevoegt, moet u ook enkele services toevoegen op de Adaptive Job Server. Bijvoorbeeld de planningsservice voor doelbezorging.

> ⓘ Opmerking
>
> - In toekomstige onderhoudsversies kunnen nieuwe services of servertypen worden opgenomen.
> - De Sample Java Scheduling Service wordt alleen verbruikt voor interne ontwikkeldoelen en is niet beschikbaar voor verbruik door externe belanghebbenden.

Service	Servicecategorie	Servertype	Servicebeschrijving
Adaptive Connectivity-service	Connectivity-services	Adaptive Processing Server	Biedt verbindingsservices voor Java-stuurprogramma's

Service	Servicecategorie	Servertype	Servicebeschrijving
Analytics Hub-service	Kernservices	Adaptive Processing Server	Deze service wordt uitgevoerd op de Adaptive Processing Server en communiceert met SAP Analytics Cloud en het SAP Analytics Hub-systeem.
Planningsservice voor verificatie-update	Kernservices	Adaptive Job Server	Biedt synchronisatie van updates voor beveiligingsinvoegtoepassingen van derden.
BEx-webtoepassingsservice	Analysis Services	Adaptive Processing Server	Biedt integratie van SAP BW (Business Warehouse) BEx-webtoepassingen (Business Explorer) met het BI-startpunt.
BIMobileService(OCA)	Kernservices	Adaptive Processing Server	Schakelt pushberichtgeving op mobiele apparaten in.
Containerservice voor webtoepassingen	Kernservices	Containerserver voor webtoepassingen	Biedt webtoepassingen voor de containerserver voor webtoepassingen: de CMC (Central Management Console), het BI-startpunt en OpenDocument.
Central Management-service	Kernservices	Central Management Server	Hiermee wordt server-, gebruikers-, sessie- en beveiligingsbeheer (rechten en verificatie) geboden. Er moet ten minste één Central Management Service beschikbaar zijn in een cluster voor een goede werking van het cluster.
Proxyservice voor clientcontrole	Kernservices	Adaptive Processing Server	Hiermee worden controlegebeurtenissen die vanaf clients verzonden zijn, verzameld en doorgestuurd naar de CMS-server.
Commentaarservice	Kernservices	Adaptive Processing Server	Hiermee worden commentaarbewerkingen in documenten toegestaan.
Crystal Reports 2020-verwerkingsservice	Crystal Reports-services	Crystal Reports-verwerkingsserver	Accepteert en verwerkt Crystal Reports 2020-rapporten; kan gegevens met andere rapporten delen om het aantal keren dat de databases worden geopend te beperken.

Service	Servicecategorie	Servertype	Servicebeschrijving
Planningsservice van Crystal Reports 2020	Crystal Reports-services	Adaptive Job Server	Hiermee worden geplande oude Crystal Reports-taken uitgevoerd en de resultaten daarvan naar de opgegeven uitvoerlocatie gepubliceerd.
Service voor weergave en wijziging van Crystal Reports 2020	Crystal Reports-services	Report Application Server (RAS)	Verwerkt weergave- en wijzigingsverzoeken voor Crystal Reports 2020-rapporten.
Crystal Reports-service voor opslaan in cache	Crystal Reports-services	Crystal Reports Cache Server	Hiermee wordt de toegang tot databases die is gegenereerd vanuit Crystal Reports-rapporten beperkt en wordt de rapportage versneld door het beheer van een cache met rapporten.
Crystal Reports-verwerkingsservice	Crystal Reports-services	Crystal Reports-verwerkingsserver	Accepteert en verwerkt Crystal Reports-rapporten; kan gegevens tussen rapporten delen om het aantal keren dat de databases worden geopend, te reduceren.
Planningsservice van Crystal Reports	Crystal Reports-services	Adaptive Job Server	Hiermee worden geplande nieuwe Crystal Reports-taken uitgevoerd en de resultaten daarvan naar de opgegeven uitvoerlocatie gepubliceerd.
Service voor aangepaste gegevenstoegang	Web Intelligence-services	Adaptive Processing Server	Biedt dynamische verbindingen met gegevensbronnen die geen verbindingsserver vereisen. Met deze service krijgt u toegang tot rapporten die zijn gemaakt op basis van persoonlijke gegevensbronnen, zoals CSV-bestanden, en kunt u deze rapporten vernieuwen. Raadpleeg de *Gebruikershandleiding voor SAP BusinessObjects Web Intelligence* voor meer informatie over het maken van query's of het vernieuwen van documenten die op een tekstbestand zijn gebaseerd.

Service	Servicecategorie	Servertype	Servicebeschrijving
Data Federator-service	Data Federator-services	Adaptive Processing Server	Voert query's uit en verwerkt de onderliggende gegevensbronnen voor een universe met meerderen bronnen.
Planningsservice voor doelbezorging	Kernservices	Adaptive Job Server	Hiermee worden geplande taken uitgevoerd en worden de resultaten naar een opgegeven uitvoerlocatie gepubliceerd, zoals een bestandsysteem, FTP-server, SFTP-server, e-mail of het Postvak IN van een gebruiker. **Opmerking** Wanneer u servers toevoegt, moet u ook enkele Adaptive Job Server-services toevoegen, waaronder deze service.
Service voor documentherstel	Web Intelligence-services	Adaptive Processing Server	Web Intelligence-documenten automatisch opslaan en herstellen
DSL Bridge-service	Web Intelligence-services	Adaptive Processing Server	Ondersteuning voor DSL-sessie (Dimensional Semantic Layer).
Gebeurtenisservice	Kernservices	Event Server	Hiermee worden bestandsgebeurtenissen op een FRS (File Repository Server) gecontroleerd en worden rapporten indien nodig uitgevoerd.
Service voor Excel-gegevenstoegang	Web Intelligence-services	Adaptive Processing Server	Hiermee worden Excel-bestanden ondersteund die als gegevensbronnen naar het BI-platform worden geüpload. Raadpleeg de *Gebruikershandleiding voor SAP BusinessObjects Web Intelligence* voor meer informatie over het maken van query's of het vernieuwen van documenten die zijn gebaseerd op een Excel-bestand.

Service	Servicecategorie	Servertype	Servicebeschrijving
Service van Informatie-engine	Web Intelligence-services	Web Intelligence-verwerkingsserver	Service die vereist is voor het verwerken van Web Intelligence-documenten
Input Filestore-service	Kernservices	Input File Repository Server	Onderhoudt gepubliceerde rapport- en programmaobjecten die kunnen worden gebruikt bij het genereren van nieuwe rapporten wanneer een invoerbestand wordt ontvangen.
Insight to Action Service	Kernservices	Adaptive Processing Server	Hiermee kunnen acties worden opgeroepen en kan ondersteuning voor RRI worden geboden.
ClearCase-service promotiebeheer	Services voor promotiebeheer	Adaptive Processing Server	Biedt ClearCase-ondersteuning voor LCM.
Planningsservice promotiebeheer	Services voor promotiebeheer	Adaptive Job Server	Hiermee worden geplande taken van promotiebeheer uitgevoerd.
Service voor promotiebeheer	Services voor promotiebeheer	Adaptive Processing Server	Kernservice voor promotiebeheer
Toezichtservice.	Kernservices	Adaptive Processing Server	Biedt controlefuncties
Multi-Dimensional Analysis-service	Analysis Services	Adaptive Processing Server	Biedt toegang tot multidimensionale OLAP-gegevens (Online Analytical Processing), converteert de onbewerkte gegevens naar XML voor weergave in kruistabellen en diagrammen in Excel, PDF of Analysis (voorheen Voyager).
Eigen Connectivity-service	Connectivity-services	Verbindingsserver	Biedt eigen Connectivity-services voor een 64-bits architectuur.
Eigen Connectivity-service (32 bits)	Connectivity-services	Verbindingsserver	Biedt eigen Connectivity-services voor een 32-bits architectuur.
Output Filestore-service	Kernservices	Output File Repository Server	Onderhoudt een verzameling van voltooide documenten.
Planningsservice voor Platform zoeken	Kernservices	Adaptive Job Server	Voert geplande zoekopdracht uit om alle inhoud van de CMS-gegevensopslagruimte (Central Management Server) te indexeren.

Service	Servicecategorie	Servertype	Servicebeschrijving
Service Platform zoeken	Kernservices	Adaptive Processing Server	Biedt zoekfunctionaliteit voor het BI-platform.
Planningsservice van test	Kernservices	Adaptive Job Server	Hiermee worden geplande testtaken uitgevoerd en worden de resultaten naar een uitvoerlocatie gepubliceerd.
Programmaplanningsservice	Kernservices	Adaptive Job Server	Hiermee worden programma's uitgevoerd die gepland zijn voor uitvoer.
Planningsservice voor publicatie	Kernservices	Adaptive Job Server	Hiermee worden geplande publicatietaken uitgevoerd en worden de resultaten naar de opgegeven uitvoerlocatie gepubliceerd.
Publicatienaverwerkingsservice	Kernservices	Adaptive Processing Server	Hiermee worden acties uitgevoerd op rapporten nadat deze zijn voltooid, zoals het verzenden van een rapport naar een uitvoerlocatie.
Publicatieservice	Kernservices	Adaptive Processing Server	Coördineert met de publicatienaverwerkingsservice en Destination Job Service om de rapporten naar een uitvoerlocatie te publiceren, zoals een bestandssysteem, FTP-server, SFTP-server, e-mail of het postvak IN van een gebruiker.
Rebean-service	Web Intelligence-services	Adaptive Processing Server	SDK gebruikt door Web Intelligence en Explorer
Herhalingsservice	Kernservices	Adaptive Job Server	Voert geplande federatietaken uit om inhoud tussen federatiesites te synchroniseren.
RESTful Web Service	Kernservices	Containerserver voor webtoepassingen (WACS)	Biedt sessieverwerking voor RESTful Web Service-aanvragen.
Planningsservice voor beveiligingsquery	Kernservices	Adaptive Job Server	Voert geplande taken van Beveiligingsquery uit.
Service voor beveiligingstokens	Kernservices	Adaptive Processing Server	Ondersteuning voor eenmalige SAP-aanmelding
Setmaterialiseringsservice	Kernservices	Adaptive Processing Server	Werkt aan materialiseriing van sets en setgroepen.

Service	Servicecategorie	Servertype	Servicebeschrijving
Planningsservice setmaterialisering	Kernservices	Adaptive Job Server	Hiermee kunt u sets en setgroepen voor materialisering plannen.
Vertaalservice	Kernservices	Adaptive Processing Server	Vertaalt InfoObjects met invoer vanuit de Translation Manager-client.
Planningsservice voor importeren van gebruikers en groepen	Kernservices	Adaptive Job Server	Staat de planning van imports van principal-bestanden toe
Planningsservice voor Visueel verschil	Services voor promotiebeheer	Adaptive Job Server	Voert geplande taken voor Visueel verschil (promotiebeheer) uit en publiceert de resultaten naar een uitvoerlocatie.
Service voor Visueel verschil	Services voor promotiebeheer	Adaptive Processing Server	Bepaalt of documenten zichtbaar identiek zijn voor het verhogen van documenten en promotiebeheer.
Visualisatieservice	Web Intelligence-services	Adaptive Processing Server	Gemeenschappelijke service voor visualisatie van objectmodel, gebruikt door Web Intelligence.
Algemene service van Web Intelligence	Web Intelligence-services	Web Intelligence-verwerkingsserver	Ondersteunt verwerking van Web Intelligence-documenten
Web Intelligence-kernservice	Web Intelligence-services	Web Intelligence-verwerkingsserver	Ondersteunt verwerking van Web Intelligence-documenten
Web Intelligence-verwerkingsservice	Web Intelligence-services	Web Intelligence-verwerkingsserver	Accepteert en verwerkt Web Intelligence-documenten
Planningsservice voor Web Intelligence	Web Intelligence-services	Adaptive Job Server	Maakt ondersteuning voor geplande Web Intelligence-taken mogelijk
Versiebeheerservice	Services voor promotiebeheer	Adaptive Processing Server	Beheert meerdere versies van BI-bronnen die IBM Rational ClearCase of Apache SubVersion gebruiken.

3.2.3 Servicecategorieën

> ⓘ Opmerking
>
> In toekomstige onderhoudsversies kunnen nieuwe services of servertypen worden opgenomen.

Servicecategorie	Service	Servertype
Analysis Services	BEx-webtoepassingsservice	Adaptive Processing Server
Analysis Services	Multi-Dimensional Analysis-service	Adaptive Processing Server
Connectivity-services	Adaptive Connectivity-service	Adaptive Processing Server
Connectivity-services	Eigen Connectivity-service	Verbindingsserver
Connectivity-services	Eigen Connectivity-service (32 bits)	Verbindingsserver
Kernservices	Analytics Hub-service	Adaptive Processing Server
Kernservices	Planningsservice voor verificatie-update	Adaptive Job Server
Kernservices	BIMobileService(OCA)	Adaptive Processing Server
Kernservices	Central Management-service	Central Management Server
Kernservices	Proxyservice voor clientcontrole	Adaptive Processing Server
Kernservices	Commentaarservice	Adaptive Processing Server
Kernservices	Doelconfiguratieservice*	Adaptive Job Server
Kernservices	Planningsservice voor doelbezorging	Adaptive Job Server
Kernservices	Gebeurtenisservice	Event Server
Kernservices	Insight to Action Service	Adaptive Processing Server
Kernservices	Input Filestore-service	Input File Repository Server
Kernservices	Toezichtservice	Adaptive Processing Server
Kernservices	Output Filestore-service	Output File Repository Server
Kernservices	Planningsservice voor Platform zoeken	Adaptive Job Server
Kernservices	Service Platform zoeken	Adaptive Processing Server
Kernservices	Planningsservice van test	Adaptive Job Server
Kernservices	Programmaplanningsservice	Adaptive Job Server
Kernservices	Planningsservice voor publicatie	Adaptive Job Server
Kernservices	Publicatienaverwerkingsservice	Adaptive Processing Server
Kernservices	Publicatieservice	Adaptive Processing Server
Kernservices	RESTful-webservice	Containerserver voor webtoepassingen
Kernservices	Herhalingsservice	Adaptive Job Server
Kernservices	Planningsservice voor beveiligings-query	Adaptive Job Server
Kernservices	Service voor beveiligingstokens	Adaptive Processing Server
Kernservices	Setmaterialiseringsservice	Adaptive Processing Server
Kernservices	Planningsservice setmaterialisering	Adaptive Processing Server
Kernservices	Service voor enkelvoudige aanmelding*	Central Management Server, Verbindingsserver, Crystal Reports-verwerkingsserver, RAS en Web Intelligence-verwerkingsserver

Servicecategorie	Service	Servertype
Kernservices	TraceLog-service*	Elke server
Kernservices	Vertaalservice	Adaptive Processing Server
Kernservices	Planningsservice voor importeren gebruikers en groepen*	Adaptive Job Server
Kernservices	Containerservice voor webtoepassingen*	Containerserver voor webtoepassingen
Crystal Reports-services	Crystal Reports 2020-verwerkingsservice	Crystal Reports-verwerkingsserver
Crystal Reports-services	Planningsservice van Crystal Reports 2020	Adaptive Job Server
Crystal Reports-services	Service voor weergave en wijziging van Crystal Reports 2020	Report Application Server (RAS)
Crystal Reports-services	Crystal Reports-service voor opslaan in cache	Crystal Reports-cacheserver
Crystal Reports-services	Crystal Reports-verwerkingsservice	Crystal Reports-verwerkingsserver
Crystal Reports-services	Planningsservice van Crystal Reports	Adaptive Job Server
Data Federator-services	Data Federator-service	Adaptive Processing Server
Services voor beheer van levenscyclus	ClearCase-service promotiebeheer	Adaptive Processing Server
Services voor beheer van levenscyclus	Planningsservice promotiebeheer	Adaptive Job Server
Services voor beheer van levenscyclus	Service voor promotiebeheer	Adaptive Processing Server
Services voor beheer van levenscyclus	Planningsservice voor Visueel verschil	Adaptive Job Server
Services voor beheer van levenscyclus	Service voor Visueel verschil	Adaptive Processing Server
Web Intelligence-services	Service voor aangepaste gegevenstoegang	Adaptive Processing Server
Web Intelligence-services	Service voor documentherstel	Adaptive Processing Server
Web Intelligence-services	DSL Bridge-service	Adaptive Processing Server
Web Intelligence-services	Service voor Excel-gegevenstoegang	Adaptive Processing Server
Web Intelligence-services	Service van Informatie-engine	Web Intelligence-verwerkingsserver
Web Intelligence-services	Rebean-service	Adaptive Processing Server
Web Intelligence-services	Visualisatieservice	Adaptive Processing Server
Web Intelligence-services	Algemene service van Web Intelligence	Web Intelligence-verwerkingsserver
Web Intelligence-services	Web Intelligence-kernservice	Web Intelligence-verwerkingsserver
Web Intelligence-services	Toezichtservice van Web Intelligence*	Adaptive Processing Server
Web Intelligence-services	Web Intelligence-verwerkingsservice	Web Intelligence-verwerkingsserver
Web Intelligence-services	Planningsservice voor Web Intelligence	Adaptive Job Server
Services voor doorgiftebeheer	Versiebeheerservice	Adaptive Processing Server

3.2.4 Servertypen

Een sterretje naast de naam van een service geeft aan dat het om een secondaire service gaat. Sommige secondaire services worden automatisch gemaakt, maar u moet kiezen om andere secondaire services op te nemen wanneer u de primaire service selecteert waarvan een secondaire service afhankelijk is.

> **Opmerking**
>
> In toekomstige onderhoudsversies kunnen nieuwe services of servertypen worden opgenomen.

Servertype	Service	Servicecategorie
Elke server	TraceLog-service	Kernservices
Adaptive Job Server	Planningsservice voor verificatie-update	Kernservices
Adaptive Job Server	Planningsservice van Crystal Reports 2020	Crystal Reports-services
Adaptive Job Server	Planningsservice van Crystal Reports	Crystal Reports-services
Adaptive Job Server	Doelconfiguratieservice	Kernservices
Adaptive Job Server	Planningsservice voor doelbezorging	Kernservices
Adaptive Job Server	Planningsservice promotiebeheer	Services voor promotiebeheer
Adaptive Job Server	Planningsservice voor Platform zoeken	Kernservices
Adaptive Job Server	Planningsservice van test	Kernservices
Adaptive Job Server	Programmaplanningsservice	Kernservices
Adaptive Job Server	Planningsservice voor publicatie	Kernservices
Adaptive Job Server	Herhalingsservice	Kernservices
Adaptive Job Server	Planningsservice voor beveiligingsquery	Kernservices
Adaptive Job Server	Planningsservice setmaterialisering	Kernservices
Adaptive Job Server	Planningsservice voor importeren gebruikers en groepen	Kernservices
Adaptive Job Server	Planningsservice voor Visueel verschil	Services voor promotiebeheer
Adaptive Job Server	Planningsservice voor Web Intelligence	Web Intelligence-services
Adaptive Processing Server	Adaptive Connectivity-service	Connectivity-services
Adaptive Processing Server	Analytical Hub-services	Kernservices
Adaptive Processing Server	BEx-webtoepassingsservice	Analysis Services
Adaptive Processing Server	Proxyservice voor clientcontrole	Kernservices
Adaptive Processing Server	Service voor aangepaste gegevenstoegang	Web Intelligence-services
Adaptive Processing Server	Data Federator-service	Data Federator-services
Adaptive Processing Server	Service voor document herstellen	Web Intelligence-services

Servertype	Service	Servicecategorie
Adaptive Processing Server	DSL Bridge-service	Web Intelligence-services
Adaptive Processing Server	Service voor Excel-gegevenstoegang	Web Intelligence-services
Adaptive Processing Server	Insight to Action Service	Kernservices
Adaptive Processing Server	ClearCase-service promotiebeheer	Services voor promotiebeheer
Adaptive Processing Server	Service voor promotiebeheer	Services voor promotiebeheer
Adaptive Processing Server	Toezichtservice.	Kernservices
Adaptive Processing Server	Multi-Dimensional Analysis-service	Analysis Services
Adaptive Processing Server	Service Platform zoeken	Kernservices
Adaptive Processing Server	Publicatienaverwerkingsservice	Kernservices
Adaptive Processing Server	Publicatieservice	Kernservices
Adaptive Processing Server	Rebean-service	Web Intelligence-services
Adaptive Processing Server	Service voor beveiligingstokens	Kernservices
Adaptive Processing Server	Setmaterialiseringsservice	Kernservices
Adaptive Processing Server	Vertaalservice	Kernservices
Adaptive Processing Server	Service voor Visueel verschil	Services voor promotiebeheer
Adaptive Processing Server	Visualisatieservice	Web Intelligence-services
Adaptive Processing Server	Toezichtservice van Web Intelligence	Web Intelligence-services
Central Management Server	Central Management-service	Kernservices
Central Management Server	Service voor enkelvoudige aanmelding	Kernservices
Verbindingsserver	Eigen Connectivity-service	Connectivity-services
Verbindingsserver	Systeemeigen verbindingsservice (32 bits).	Connectivity-services
Verbindingsserver	Service voor eenmalige aanmelding*	Kernservices
Crystal Reports Cache Server	Crystal Reports-service voor opslaan in cache	Crystal Reports-services
Crystal Reports-verwerkingsserver	Crystal Reports 2020-verwerkingsservice	Crystal Reports-services
Crystal Reports-verwerkingsserver	Crystal Reports-verwerkingsservice	Crystal Reports-services
Crystal Reports-verwerkingsserver	Service voor eenmalige aanmelding*	Kernservices
Event Server	Gebeurtenisservice	Kernservices
Input File Repository Server	Input Filestore-service	Kernservices
Output File Repository Server	Output Filestore-service	Kernservices
Report Application Server (RAS)	Service voor weergave en wijziging van Crystal Reports 2020	Crystal Reports-services
RAS	Service voor eenmalige aanmelding*	Kernservices
Containerserver voor webtoepassingen	RESTful Web Service	Kernservices

Servertype	Service	Servicecategorie
Containerserver voor webtoepassingen	Containerservice voor webtoepassingen	Kernservices
Web Intelligence-verwerkingsserver	Service van Informatie-engine	Web Intelligence-services
Web Intelligence-verwerkingsserver	Service voor eenmalige aanmelding*	Kernservices
Web Intelligence-verwerkingsserver	Algemene service van Web Intelligence	Web Intelligence-services
Web Intelligence-verwerkingsserver	Web Intelligence-kernservice	Web Intelligence-services
Web Intelligence-verwerkingsserver	Web Intelligence-verwerkingsserver	Web Intelligence-services

Servertype	Service	Servicecategorie
Adaptive Job Server	Planningsservice voor verificatie-update	Kernservices
Adaptive Job Server	Planningsservice van Crystal Reports 2020	Crystal Reports-services
Adaptive Job Server	Planningsservice van Crystal Reports	Crystal Reports-services
Adaptive Job Server	Planningsservice voor doelbezorging	Kernservices
Adaptive Job Server	Planningsservice promotiebeheer	Services voor promotiebeheer
Adaptive Job Server	Planningsservice voor Platform zoeken	Kernservices
Adaptive Job Server	Planningsservice van test	Kernservices
Adaptive Job Server	Programmaplanningsservice	Kernservices
Adaptive Job Server	Planningsservice voor publicatie	Kernservices
Adaptive Job Server	Herhalingsservice	Kernservices
Adaptive Job Server	Planningsservice voor beveiligingsquery	Kernservices
Adaptive Job Server	Planningsservice voor Visueel verschil	Services voor promotiebeheer
Adaptive Job Server	Planningsservice voor Web Intelligence	Web Intelligence-services
Adaptive Processing Server	Adaptive Connectivity-service	Connectivity-services
Adaptive Processing Server	BEx-webtoepassingsservice	Analysis Services
Adaptive Processing Server	Proxyservice voor clientcontrole	Kernservices
Adaptive Processing Server	Service voor aangepaste gegevenstoegang	Web Intelligence-services
Adaptive Processing Server	Data Federator-service	Data Federator-services
Adaptive Processing Server	Service voor document herstellen	Web Intelligence-services
Adaptive Processing Server	DSL Bridge-service	Web Intelligence-services
Adaptive Processing Server	Service voor Excel-gegevenstoegang	Web Intelligence-services
Adaptive Processing Server	Insight to Action Service	Kernservices
Adaptive Processing Server	ClearCase-service promotiebeheer	Services voor promotiebeheer
Adaptive Processing Server	Service voor promotiebeheer	Services voor promotiebeheer

Servertype	Service	Servicecategorie
Adaptive Processing Server	Toezichtservice.	Kernservices
Adaptive Processing Server	Multi-Dimensional Analysis-service	Analysis Services
Adaptive Processing Server	Service Platform zoeken	Kernservices
Adaptive Processing Server	Publicatienaverwerkingsservice	Kernservices
Adaptive Processing Server	Publicatieservice	Kernservices
Adaptive Processing Server	Rebean-service	Web Intelligence-services
Adaptive Processing Server	Service voor beveiligingstokens	Kernservices
Adaptive Processing Server	Vertaalservice	Kernservices
Adaptive Processing Server	Service voor Visueel verschil	Services voor promotiebeheer
Adaptive Processing Server	Visualisatieservice	Web Intelligence-services
Central Management Server	Central Management-service	Kernservices
Verbindingsserver	Eigen Connectivity-service	Connectivity-services
Verbindingsserver	Systeemeigen verbindingsservice (32 bits).	Connectivity-services
Crystal Reports-cacheserver	Crystal Reports-cacheservice	Crystal Reports-services
Crystal Reports-verwerkingsserver	Crystal Reports 2020-verwerkingsservice	Crystal Reports-services
Crystal Reports-verwerkingsserver	Crystal Reports-verwerkingsservice	Crystal Reports-services
Event Server	Gebeurtenisservice	Kernservices
Input File Repository Server	Input Filestore-service	Kernservices
Output File Repository Server	Output Filestore-service	Kernservices
Report Application Server (RAS)	Service voor weergave en wijziging van Crystal Reports 2020	Crystal Reports-services
Containerserver voor webtoepassingen	RESTful-webservice	Kernservices
Web Intelligence-verwerkingsserver	Information Engine-service	Web Intelligence-services
Web Intelligence-verwerkingsserver	Algemene service van Web Intelligence	Web Intelligence-services
Web Intelligence-verwerkingsserver	Web Intelligence-kernservice	Web Intelligence-services
Web Intelligence-verwerkingsserver	Web Intelligence-verwerkingsserver	Web Intelligence-services

3.2.5 Servers

Servers zijn serviceverzamelingen die op een host worden uitgevoerd onder een SIA (Server Intelligence Agent). Het type server wordt aangeduid door de services die erop worden uitgevoerd. Servers kunnen worden gemaakt in de CMC (Central Management Console) In de volgende tabel worden de verschillende servertypen vermeld die in de CMC kunnen worden gemaakt.

Server	Beschrijving
Adaptive Job Server	Een generieke server die geplande taken verwerkt. Wanneer u een taakserver toevoegt aan het BI-platformsysteem, kunt u de taakserver configureren voor de verwerking van rapporten, documenten, programma's of publicaties, en de resultaten naar de verschillende doelen verzenden.
Adaptive Processing Server	Een algemene server die fungeert als host voor services waarmee aanvragen van diverse bronnen worden verwerkt. Het installatieprogramma installeert één APS (Adaptive Processing Server) per hostsysteem. Afhankelijk van de functies die u hebt geïnstalleerd, kan deze APS host zijn voor een groot aantal services, zoals de Toezichtservice, Service voor beheer van levenscyclus, MDAS-service (Multi-Dimensional Analysis) en Publicatieservice. Voor productie- of testsystemen kunt u het beste extra Adaptive Processing Servers maken en deze configureren om aan uw bedrijfsvereisten te voldoen. Zie Inleiding tot de wizard Systeemconfiguratie [pagina 87] en Adaptive Processing Servers configureren voor productiesystemen [pagina 450] voor meer informatie.
Central Management Server (CMS)	Hiermee wordt een database met informatie onderhouden over uw BI-platformsysteem (in de CMS-systeemdatabase) en gecontroleerde gebruikersacties (in de Controlegegevensopslag). Alle platformservices worden door de CMS beheerd. De CMS beheert ook toegang tot de systeembestanden waar documenten worden opgeslagen, en informatie over gebruikers, gebruikersgroepen, beveiligingsniveaus (inclusief verificatie en autorisatie) en inhoud.
Verbindingsserver	Biedt databasetoegang tot brongegevens. Hiermee worden relationele databases ondersteunt, evenals OLAP-indelingen en andere indelingen. De Verbindingsserver is verantwoordelijk voor de verbinding en interactie met de verschillende gegevensbronnen en voor het aanbieden van een algemene functieset aan clients.
Crystal Reports Cache Server	Onderschept rapportaanvragen die door clients naar de pagina server zijn verzonden. Als de Cache Server niet aan de aanvraag kan voldoen met een rapportpagina uit de cache, wordt de aanvraag doorgestuurd naar de Crystal Reports-verwerkingsserver; deze voert het rapport uit en retourneert het resultaat. De cacheserver plaatst de rapportpagina vervolgens in de cache voor mogelijk toekomstig gebruik.
Crystal Reports-verwerkingsserver	Beantwoordt pagina-aanvragen door rapporten te verwerken en pagina's in de EPF-indeling te genereren (Encapsulated Page Format). Het grootste voordeel van EPF is dat het ondersteuning biedt voor pagina's op aanvraag; alleen de aangevraagde pagina wordt dus geretourneerd,

Server	Beschrijving
	niet het gehele rapport. Dit komt de prestaties ten goede en vermindert onnodig netwerkverkeer voor grote rapporten.
Event Server	Controleert het systeem op gebeurtenissen die ertoe kunnen leiden dat een rapport wordt uitgevoerd. Wanneer u een gebeurtenis instelt waarmee een bepaalde actie moet worden gestart, wordt door de Event Server gecontroleerd of aan de voorwaarde is voldaan en wordt er vervolgens een bericht naar de CMS gestuurd wanneer de bestandsgebeurtenis heeft plaatsgevonden. Vervolgens worden op de CMS de taken gestart die afhankelijk zijn van deze gebeurtenis. De Event Server beheert bestandsgebeurtenissen die plaatsvinden op de opslaglaag.
File Repository Server	Maakt bestandssysteemobjecten, zoals geëxporteerde rapporten en geïmporteerde bestanden in niet-eigen indelingen. Op de Input FRS worden rapport- en programmaobjecten opgeslagen die naar het systeem zijn gepubliceerd door beheerders of eindgebruikers. Een uitvoer-FRS slaat alle rapportexemplaren op die door de Job Server worden gegenereerd.
Web Intelligence-verwerkingsserver	Verwerkt SAP BusinessObjects Web Intelligence-documenten.
Report Application Server	Hiermee worden functies geboden voor ad-hocrapporten waarmee gebruikers Crystal Reports-rapporten kunnen maken en wijzigen via de SDK (Software Development Kit) van SAP Crystal Reports Server Embedded.

3.3 Clienttoepassingen

U kunt via twee hoofdtypen clienttoepassingen met het BI-platform werken:

- Bureaubladtoepassingen
  Deze toepassingen moeten geïnstalleerd worden op een ondersteund Microsoft Windows-besturingssysteem, en kunnen lokaal gegevens verwerken en rapporten maken.

  > **Opmerking**
  >
  > Bureaubladtoepassingen worden niet langer door het installatieprogramma van het BI-platform geïnstalleerd. Als u een bureaubladtoepassing op een server wilt installeren, gebruikt u het zelfstandige installatieprogramma van de clienthulpprogramma's van SAP BusinessObjects Business Intelligence-platform.

  Via desktopclients kunt u bepaalde BI-rapportverwerking doorsturen naar andere afzonderlijke clientcomputers. De meeste bureaubladtoepassingen krijgen rechtstreeks toegang tot de gegevens in uw organisatie via stuurprogramma's op de desktopcomputer en communiceren met uw BI-platformimplementatie via CORBA of gecodeerde CORBA SSL.
  Voorbeelden van dit type toepassing zijn Crystal Reports en Live Office.

> **Opmerking**
>
> Hoewel Live Office een toepassing met rijke functionaliteit is, verloopt de communicatie met BI-platformwebservices via HTTP.

- Webtoepassingen
  Deze toepassingen worden gehost door een webtoepassingsserver en kunnen worden opgeroepen via een ondersteunde webbrowser op de besturingssystemen van Windows, Macintosh, Unix en Linux.
  Deze werkwijze biedt u de mogelijkheid om BI-toegang (business intelligence) te verschaffen aan grote groepen gebruikers zonder desktopsoftware te moeten implementeren. Communicatie verloopt via HTTP, met of zonder SSL-codering (HTTPS).
  Voorbeelden van dit type toepassing zijn het BI-startpunt, SAP BusinessObjects Web Intelligence, de CMC (Central Management Console) en rapportviewers.

3.3.1 Geïnstalleerd met Clienthulpprogramma's van SAP BusinessObjects Business Intelligence-platform

3.3.1.1 Web Intelligence Rich Client

Web Intelligence Rich Client is een hulpprogramma voor ad-hocanalyse en -rapportage, dat bedoeld is voor bedrijfsgebruikers met of zonder toegang tot het BI-platform.

Met Rich Client krijgen zakelijke gebruikers toegang tot gegevens via universes (.unv en .unx), BEx-query's of andere bronnen, met behulp van vertrouwde zakelijke termen in een sleep en neerzet-interface. Dankzij werkstromen kunnen zeer algemene of zeer specifieke vragen worden geanalyseerd en kunnen op elk punt in de analysewerkstroom verdere vragen worden gesteld.

Web Intelligence Rich Client-gebruikers kunnen ook wanneer ze geen verbinding met een CMS (Central Management Server) kunnen maken, met Web Intelligence-documentbestanden (.wid) blijven werken.

> **Opmerking**
>
> - Het installeren van Web Intelligence Rich Client op dezelfde machine als de BI-platformservers wordt niet aanbevolen. Web Intelligence Rich Client en de BI-platformservers hebben binaire bestanden met elkaar gemeen, wat problemen met uw implementatie kan veroorzaken als u een upgrade van de installatie (client of server) uitvoert. Installeer Web Intelligence Rich Client op een afzonderlijke machine.
> - Als u een upgrade uitvoert van 4.2, stop en sluit deze versie dan voordat u versie 4.3 installeert. Controleer het Windows-systeemvak. Mogelijk is de Rich Client geminimaliseerd en nog steeds actief.

3.3.1.2 Business Views-beheer

Gebruikers kunnen met Business Views-beheer objecten met semantische lagen maken die de onderliggende complexiteit van databases vereenvoudigen.

Met Business Views-beheer kunnen gegevensverbindingen, dynamische gegevensverbindingen, gegevensverzamelingen, bedrijfselementen, bedrijfsweergaven en relationele weergaven gemaakt worden. Ook kan uitgebreide beveiliging op kolom- en rijniveau ingesteld worden voor de objecten in een rapport.

Ontwerpers kunnen verbindingen naar meerdere gegevensbronnen instellen, tabellen samenvoegen, aliassen toewijzen aan veldnamen, berekende velden maken en deze vereenvoudigde structuur vervolgens als een Business Views-weergave gebruiken. Ontwerpers en gebruikers van rapporten kunnen de bedrijfsweergave vervolgens als basis voor hun rapporten gebruiken, in plaats van hun eigen query's aan de hand van de gegevens te moeten samenstellen.

3.3.1.3 Hulpprogramma Rapportconversie

Het hulpprogramma Rapportconversie is uit gebruik genomen in de BI 4.3-release. Zie 2801797 voor meer informatie.

3.3.1.4 Hulpprogramma voor universe-ontwerp

In het hulpprogramma voor universe-ontwerp (voorheen Universe Designer) kunnen gegevensontwerpers gegevens van meerdere bronnen in een semantische laag combineren, waardoor de complexiteit van databases verborgen blijft voor eindgebruikers. De complexiteit van gegevens wordt vereenvoudigd door zakelijke taal in plaats van technische taal te gebruiken voor de toegang, bewerking en indeling van gegevens.

Het hulpprogramma voor universe-ontwerp biedt een grafische interface waarmee u tabellen in een database kunt selecteren en bekijken. De databasetabellen worden in de vorm van tabelsymbolen in een schemadiagram weergegeven. Ontwerpers kunnen via deze interface tabellen bewerken, joins tussen tabellen maken, aliastabellen maken, contexten maken en lussen in een schema verhelpen.

U kunt ook universes maken op basis van metagegevensbronnen. Het hulpprogramma voor universe-ontwerp wordt gebruikt om universes te genereren aan het eind van het ontwerpproces.

3.3.1.5 Hulpprogramma voor informatieontwerp

Het hulpprogramma voor informatieontwerp (voorheen Information Designer) is een ontwerpomgeving voor metagegevens waarmee ontwerpers metagegevens uit relationele en OLAP-bronnen kunnen ophalen, definiëren en manipuleren om SAP BusinessObjects-universes te maken en implementeren.

3.3.1.6 Hulpprogramma voor vertaalbeheer

Het BI-platform biedt ondersteuning voor meertalige documenten en universes. Een meertalig document bevat gelokaliseerde versies van universe-metagegevens en documentaanwijzingen. Een gebruiker kan bijvoorbeeld rapporten in bepaalde gekozen talen maken op basis van dezelfde universe.

Het Hulpprogramma voor vertaalbeheer (voorheen Translation Manager) definieert de meertalige universes en beheert de vertaling van universes en andere analytische en rapportbronnen in de CMS-gegevensopslagruimte.

Hulpprogramma voor vertaalbeheer:

- Vertaalt een universe of documenten voor een meertalig publiek.
- Definieert de taalonderdelen van de metagegevens van het document en de juiste vertaling. Genereert een externe XLIFF-indeling en importeert XLIFF-bestanden om vertaalde informatie te verkrijgen.
- Geeft de structuur weer van de universe of het document die/dat moet worden vertaald.
- Kunt u de metagegevens vertalen via de gebruikersinterface of via een extern vertaalhulpprogramma door XLIFF-bestanden te importeren en exporteren.
- Worden documenten in meerdere talen gemaakt.

3.3.1.7 Data Federator-beheerprogramma

Het Data Federator-beheerprogramma (voorheen Data Federator) is een Rich Client-toepassing met gebruiksvriendelijke functies voor het beheer van uw Data Federator-service.

De Data Federator-service is nauw geïntegreerd in het BI-platform en maakt universes met meerdere bronnen mogelijk door query's te verdelen over ongelijkwaardige gegevensbronnen, en u kunt gegevens verbinden via één gegevensverzameling.

Met het Data Federator-beheerprogramma kunt u Data Federator-query's optimaliseren en de Data Federator-queryengine afstemmen voor optimale prestaties.

U gebruikt het Data Federator-beheerprogramma voor het volgende:

- SQL-query's testen.
- Optimalisatieplannen visualiseren die in detail beschrijven hoe verbonden query's naar alle bronnen worden verspreid.
- Statistieken berekenen en systeemparameters instellen om de Data Federator-services af te stemmen en prestaties te optimaliseren.
- Eigenschappen beheren om te bepalen hoe query's op connectorniveau worden uitgevoerd in elke gegevensbron.
- Actieve SQL-query's controleren.
- Bladeren door de geschiedenis van uitgevoerde query's.

3.3.2 Geïnstalleerd met SAP BusinessObjects Business Intelligence-platform

3.3.2.1 Central Configuration Manager (CCM)

De CCM (Central Configuration Manager) is een serverprogramma voor probleemoplossing en knooppuntbeheer dat beschikbaar is in twee vormen. In een Microsoft Windows-omgeving kunt u met de CCM lokale en externe servers beheren. U gebruikt daartoe de grafische gebruikersinterface (GUI) van het

programma of een opdrachtregel. In een Unix-omgeving kunt u servers met behulp van het CCM-shellscript (`ccm.sh`) via de opdrachtregel beheren.

U gebruikt de CCM voor het maken en configureren van knooppunten of het starten en stoppen van de webtoepassingsserver, als dit de standaard gebundelde Tomcat-webtoepassingsserver is. In Windows kunt u de CCM ook gebruiken om netwerkparameters te configureren, bijvoorbeeld SSL-codering (Secure Sockets Layer). Deze parameters zijn van toepassing op alle servers binnen een knooppunt.

> **Opmerking**
>
> De meeste serverbeheertaken worden nu via de CMC verwerkt, niet via de CCM. De CCM wordt nu voor probleemoplossing en knooppuntconfiguratie gebruikt.

3.3.2.2 Hulpprogramma voor upgradebeheer

Het hulpprogramma UMT is uit gebruik genomen in de BI 4.3-release. Zie 2801797 voor meer informatie.

3.3.2.3 Diagnostisch hulpprogramma voor gegevensopslagruimten

Met het diagnostische hulpprogramma voor gegevensopslagruimten kunt u inconsistenties die zich voordoen tussen de CMS-systeemdatabase (Central Management Server) en de FRS's (File Repository Servers), scannen, diagnosticeren en herstellen.

Bovendien kunnen de reparatiestatus en voltooide acties worden gerapporteerd. Om de synchronisatie tussen het bestandssysteem en de database te bepalen, moet de RDT worden gebruikt nadat de gebruiker een hot back-up heeft voltooid. U kunt het hulpprogramma ook gebruiken na een herstelactie en voordat u BI-platformservices start. De gebruiker kan een limiet instellen voor het aantal fouten dat het RDT per sessie kan detecteren en herstellen.

3.3.3 Apart verkrijgbaar

3.3.3.1 SAP BusinessObjects Analysis, editie voor Microsoft Office

SAP BusinessObjects Analysis, editie voor Microsoft Office is een eersteklas alternatief voor BEx (Business Explorer) en biedt bedrijfsanalisten de mogelijkheid multidimensionale OLAP-gegevens (Online Analytical Processing) te verkennen.

Analisten kunnen bedrijfsvragen snel beantwoorden en hun analyse en werkruimte als *analyses* met anderen delen.

SAP BusinessObjects Analysis, editie voor Microsoft Office, stelt analisten in staat om het volgende te doen:

- Trends, afwijkende waarden, en details in financiële systemen ontdekken zonder tussenkomst van een databasebeheerder
- Antwoorden op bedrijfsvragen vinden terwijl grote of kleine sets met multidimensionale gegevens grondig kunnen worden bestudeerd.
- De volledige reeks OLAP-gegevensbronnen oproepen die binnen de organisatie beschikbaar is, en resultaten delen via een eenvoudige, intuïtieve interface.
- Verschillende OLAP-bronnen in dezelfde analyses oproepen voor een uitgebreid overzicht van het bedrijf en de impact die trens op elkaar kunnen hebben.
- Zakelijke factoren onderzoeken, analyseren, vergelijken en voorspellen.
- Een uitgebreide reeks bedrijfs- en tijdberekeningen gebruiken.

3.3.3.2 SAP Crystal Reports

Met SAP Crystal Reports-software kunnen gebruikers interactieve rapporten met behulp van een gegevensbron ontwerpen.

3.3.3.3 SAP Lumira

Met de toepassing SAP Lumira kunt u gegevens visualiseren en artikelen over gegevens creëren. Met SAP Lumira kunt u uw gegevens manipuleren, bewerken, opmaken, verfijnen, visualisaties om de gegevens grafisch te vertegenwoordigen en uw visualisaties via artikelen delen.

SAP Lumira wordt nu als toepassing in CMC vermeld. Hiermee kunt u rechten beheren die gerelateerd zijn aan de functionaliteit voor gegevens verzamelen en content delen van SAP Lumira voor elke gebruiker of gebruikersgroep.

> ⓘ Opmerking
>
> Alle aan de toepassing SAP Lumira gerelateerde gebeurtenissen worden zonder client-ID in de controledatabase geregistreerd.

3.3.4 Webtoepassingsclients

Webtoepassingsclients bevinden zich op een webtoepassingsserver en worden geopend in een webbrowser op een clientcomputer. Webtoepassingen worden automatisch geïmplementeerd wanneer u het BI-platform installeert.

Gebruikers kunnen webtoepassingen gemakkelijk vanuit een webbrowser openen en de gegevensuitwisseling kan worden beveiligd via SSL-codering als u van plan bent om externe gebruikers toegang tot uw bedrijfsnetwerk te verlenen.

Java-webtoepassingen kunnen ook opnieuw worden geconfigureerd of geïmplementeerd na de eerste installatie door het meegeleverde WDeploy-opdrachtregelprogramma te gebruiken. Hiermee kunt u webtoepassingen op twee manieren op een webtoepassingsserver implementeren:

1. Zelfstandige modus
   Alle webtoepassingsbronnen worden op een webtoepassingsserver geïmplementeerd die zowel dynamische als statische inhoud biedt. Deze opstelling is geschikt voor kleine installaties.
2. Modus Splitsen
   De statische inhoud van de webtoepassing (HTML, afbeeldingen, CSS) wordt geïmplementeerd op een specifieke webserver, terwijl dynamische inhoud (JSP's) wordt geïmplementeerd op een webtoepassingsserver. Deze opstelling is geschikt voor grotere installaties die er baat bij hebben als de webtoepassingsserver geen statische webinhoud hoeft te verstrekken.

Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over WDeploy.

3.3.4.1 Central Management Console (CMC)

De Central Management Console (CMC) is een webtoepassing waarmee u beheertaken kunt uitvoeren (bijvoorbeeld gebruikers-, inhoud- en serverbeheer) en beveiligingsopties kunt instellen. Omdat de CMC een webtoepassing is, kunt u de gewenste beheertaken uitvoeren in een webbrowser op elke computer met een verbinding met de webtoepassingsserver.

Alleen leden van de groep Administrators kunnen beheerinstellingen wijzigen, tenzij aan andere gebruikers expliciet de rechten hiertoe zijn verleend. In CMC kunnen aan gebruikers rollen worden toegekend waarmee zij beperkte beheertaken kunnen uitvoeren, zoals het beheren van gebruikers in uw groep en het beheren van rapporten in teammappen.

3.3.4.2 Fiorified BI-startpunt

Fiorified BI-startpunt (voorheen InfoView) is een webinterface die eindgebruikers openen om gepubliceerde BI-rapporten (business intelligence) weer te geven, te plannen en bij te houden. Fiorified BI-startpunt biedt toegang, interactie en exportbewerkingen voor alle typen bedrijfsgegevens, zoals rapporten, analyses en dashboards.

Met Fiorified BI-startpunt kunnen gebruikers het volgende beheren:

- Bladeren en zoeken in BI-inhoud
- BI-inhoud maken, bewerken en weergeven
- BI-inhoud plannen en publiceren

3.3.4.3 BI-werkruimten

Met BI-werkruimten kunt u uw bedrijfsactiviteiten en -prestaties volgen aan de hand van modules (sjablonen voor gegevens) en BI-werkruimten (gegevens weergeven in één of meer modules). Modules en BI-werkruimten bieden informatie die nodig is om bedrijfsregels aan gewijzigde omstandigheden aan te passen. Hiermee kunt u belangrijke bedrijfsgegevens volgen en analyseren via BI-werkruimten en modules voor beheer. Hiermee

wordt ook de besluitvorming en analyse in groepen ondersteund via de geïntegreerde samenwerkings- en werkstroommogelijkheden. BI-werkruimten bieden de volgende functies:

- Tabsgewijs bladeren
- Pagina maken: BI-werkruimten en modules beheren
- Een gemakkelijke opbouwfunctie voor toepassingen
- Koppelen van inhoud tussen modules voor grondige gegevensanalyse

> ⓘ Opmerking
>
> Inhoudskoppeling wordt niet ondersteund voor Design Studio-documenten.

3.3.4.4 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Business Web Intelligence is een webhulpprogramma dat query-, rapportage- en analysefunctionaliteit voor relationele gegevensbronnen biedt in één webproduct.

Gebruikers kunnen rapporten maken, ad-hocquery's uitvoeren, gegevens analyseren en rapporten opmaken via een interface met sleep-en-neerzetfunctionaliteit. Web Intelligence verbergt de complexiteit van onderliggende gegevensbronnen.

Rapporten kunnen worden gepubliceerd naar een ondersteunde webportal of naar Microsoft Office-toepassingen via SAP BusinessObjects Live Office.

3.3.4.5 SAP BusinessObjects Analysis, editie voor OLAP

SAP BusinessObjects Analysis, editie voor OLAP (voorheen Voyager) is een OLAP-hulpprogramma (Online Analytical Processing) in de portal van het BI-startpunt en wordt gebruikt om met multidimensionale gegevens te werken. Voyager kan ook informatie van verschillende OLAP-gegevensbronnen in één werkruimte combineren. SAP BW en Microsoft Analysis Services zijn twee voorbeelden van ondersteunde OLAP-providers.

De Analysis OLAP-functieset combineert elementen van SAP Crystal Reports (directe gegevenstoegang tot OLAP-kubussen voor productierapportage) en SAP BusinessObjects Web Intelligence-oplossingen (ad-hocanalyserapportage met universes uit OLAP-gegevensbronnen). Voyager biedt een uitgebreide reeks bedrijfs- en tijdberekeningen, en functies zoals tijdschuifregelaars, om de analyse van OLAP-gegevens zoveel mogelijk te vereenvoudigen.

> ⓘ Opmerking
>
> De webtoepassing Analysis, editie voor OLAP is alleen beschikbaar als Java-webtoepassing. Er is geen gelijkwaardige toepassing voor .NET.

3.3.4.6 SAP BusinessObjects Mobile

Dankzij SAP BusinessObjects Mobile kunnen uw gebruikers de BI-rapporten, gegevens en realtime-informatie die op desktopclients beschikbaar zijn, ook via een draadloos apparaat oproepen. De inhoud wordt

geoptimaliseerd voor mobiele apparaten, zodat uw gebruikers zonder extra training gemakkelijk vertrouwde rapporten kunnen openen, doornemen en analyseren.

Met SAP BusinessObjects Mobile kunnen kenniswerker up-to-date blijven en beslissingen nemen op basis van de recentste informatie. Verkoopmedewerkers en personeel in de buitendienst hebben toegang tot de juiste klant-, product- en werkordergegevens, waar en wanneer die nodig zijn.

SAP BusinessObjects Mobile ondersteunt een breed scala aan mobiele apparaten, zoals Blackberry, Windows Mobile en Symbian.

Raadpleeg de handleiding *SAP BusinessObjects Mobile installeren en implementeren* voor meer informatie over mobiele installatie, configuratie en implementatie. Zie voor meer informatie over SAP BusinessObjects Mobile de handleiding *SAP BusinessObjects Mobile gebruiken*.

3.4 Proceswerkstromen

Wanneer taken zoals aanmelding, rapportplanning of rapportweergave worden uitgevoerd, komt een gegevensstroom op gang in het systeem en communiceren de servers met elkaar. In de volgende sectie wordt een aantal van de processtromen beschreven zoals deze zich voordoen in het BI-platform.

Als u aanvullende proceswerkstromen visueel wilt weergeven, raadpleegt u de officiële studielessen voor SAP BusinessObjects Business Intelligence-platform 4.x op: http://scn.sap.com/docs/DOC-8292

3.4.1 Opstarten en verificatie

3.4.1.1 Aanmelden bij het BI-platform

Deze werkstroom beschrijft een gebruiker die zich aanmeldt bij een webtoepassing van het BI-platform vanuit een webbrowser. Deze werkstroom geldt voor webtoepassingen zoals het BI-startpunt en de CMC (Central Management Console).

1. Het aameldingsverzoek wordt door de browser (de webclient) via de webserver verzonden naar de webtoepassingsserver waarop de webtoepassing wordt uitgevoerd.
2. De webtoepassingsserver stelt vast dat het om een aanmeldingsaanvraag gaat. De webtoepassingsserver verzendt de gebruikersnaam, het wachtwoord en het verificatietype naar de CMS voor verificatie.
3. De CMS vergelijkt de gebruikersnaam en het wachtwoord met de gegevens in de juiste database (in dit geval wordt Enterprise-verificatie gebruikt en worden de gebruikersreferenties geverifieerd op basis van de CMS-systeemdatabase).
4. Na de verificatie wordt door de CMS een sessie voor de gebruiker gemaakt in het geheugen.
5. De CMS stuurt een bericht naar de webtoepassingsserver om te laten weten dat de verificatie is gelukt.
6. De webtoepassingsserver genereert in het geheugen een aanmeldingstoken voor de gebruikerssessie. Voor de overige duur van de sessie gebruikt de webtoepassingsserver deze aanmeldingstoken om de gegevens van de gebruiker te vergelijken met de gegevens in de CMS. De webtoepassingsserver genereert de volgende webpagina die aan de webclient moet worden verzonden.

7. De webtoepassingsserver verzendt deze pagina naar de webserver.
8. De webserver verzendt webpagina naar de webclient, waar deze wordt weergegeven in de browser van de gebruiker.

3.4.1.2 SIA starten

Een SIA (Server Intelligence Agent) kan worden geconfigureerd om automatisch met het hostbesturingssysteem te starten, of deze kan handmatig worden gestart met de CCM (Central Configuration Manager).

Een SIA haalt gegevens op over de servers die deze beheert, uit een CMS (Central Management Server). Indien de SIA gebruikmaakt van een lokale CMS, en die CMS is niet actief, dan start de SIA de CMS. Indien een SIA gebruikmaakt van een externe CMS, probeert deze verbinding te maken met de CMS.

Zodra een SIA gestart is, wordt de volgende reeks gebeurtenissen uitgevoerd.

1. De SIA zoekt in de cache naar een CMS.
   a. Als de SIA geconfigureerd is om een lokale CMS te starten en de CMS niet actief is, wordt de CMS door de SIA gestart en de verbinding tot stand gebracht.
   b. Als de SIA geconfigureerd is om een actieve CMS (lokaal of extern) te gebruiken, wordt geprobeerd om verbinding te maken met de eerste CMS in de cache. Als de CMS momenteel niet beschikbaar is, probeert de SIA verbinding te maken met de volgende CMS in de cache. Als geen van de CMS'en in de cache beschikbaar is, wacht de SIA tot er één beschikbaar komt.
2. De CMS controleert de identiteit van de SIA op geldigheid.
3. Wanneer de SIA een verbinding met een CMS tot stand heeft gebracht, wordt een lijst aangevraagd met servers die moeten worden beheerd.

   > **Opmerking**
   >
   > Een SIA bewaart geen informatie over de servers die worden beheerd. De configuratiegegevens die bepalen welke server door een SIA wordt beheerd, worden bewaard in de CMS-systeemdatabase en bij het opstarten door de SIA uit de CMS opgehaald.

4. De CMS vraagt de CMS-systeemdatabase om een lijst met servers die door de SIA worden beheerd. Daarnaast wordt de configuratie voor elke server opgehaald.
5. De CMS retourneert de lijst met servers en hun configuratie naar de SIA.
6. De SIA start elke server die geconfigureerd is om automatisch te starten, met de juiste configuratie en controleert de status ervan. Elke server die door de SIA wordt gestart, wordt geconfigureerd voor gebruik van dezelfde CMS als die van de SIA.

   Alle servers die niet geconfigureerd zijn om automatisch te starten met de SIA, worden niet gestart.

3.4.1.3 SIA sluiten

De SIA (Server Intelligence Agent) stopt automatisch wanneer u het besturingssysteem van de host afsluit. U kunt de SIA ook handmatig stoppen via de CCM (Central Configuration Manager).

Wanneer de SIA wordt gesloten, worden de volgende stappen uitgevoerd.

De SIA geeft aan de CMS door dat deze bezig is met sluiten.

a. Als de SIA stopt omdat het hostbesturingssysteem wordt afgesloten, verzoekt de SIA om de servers te laten stoppen. Bij servers die niet binnen 25 seconden stoppen, wordt beëindiging afgedwongen.
b. Als de SIA handmatig wordt gestopt, wacht deze tot de beheerde server klaar is met het verwerken van bestaande taken. Beheerde servers accepteren dan geen nieuwe taken meer. Zodra alle taken voltooid zijn, worden de servers stopgezet. Zijn alle servers eenmaal gestopt, dan stopt de SIA ook.

Bij een geforceerde beëindiging geeft de SIA alle beheerde servers de opdracht om onmiddellijk te stoppen.

3.4.2 Programmaobjecten

3.4.2.1 Een planning voor een programmaobject instellen

In deze werkstroom wordt het proces beschreven waarbij een gebruiker een programmaobject plant om in de toekomst vanuit een webtoepassing te worden uitgevoerd, zoals de CMC (Central Management Console) of BI-startpunt.

1. De gebruiker verzendt de planningsaanvraag vanuit de webclient via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag en stelt vast of het een planningsaanvraag betreft. De webtoepassingsserver verzendt het geplande tijdstip, de aanmeldingswaarden voor de database, de parameterwaarden, het doel en de indeling naar de opgegeven CMS (Central Management Server).
3. De CMS controleert of de gebruiker de vereiste rechten heeft om het object te plannen. Als de gebruiker voldoende rechten heeft, voegt de CMS een nieuwe record toe aan de CMS-systeemdatabase en wordt het exemplaar toegevoegd aan de lijst met wachtende planningen.
4. De CMS stuurt een respons aan de webtoepassingsserver dat de planningsbewerking is uitgevoerd.
5. De webtoepassingsserver genereert de volgende HTML-pagina en verzendt deze via de webserver naar de webclient.

3.4.2.2 Een gepland programmaobject wordt uitgevoerd

In deze werkstroom wordt het proces beschreven van een gepland programmaobject dat op een geplande tijd wordt uitgevoerd. De Adaptive Job Server en Input File Repository Server moeten ook actief zijn.

> **Opmerking**
>
> Voor deze werkstroom moeten de CMS, Adaptive Job Server en Input File Repository Server ook actief zijn.

1. De CMS (Central Management Server) controleert in de CMS-systeemdatabase of er een gepland SAP Crystal Reports-rapport is dat op dat tijdstip uitgevoerd moet worden.
2. Op de geplande tijd zoekt de CMS een beschikbare programmaplanningsservice op een Adaptive Job Server. De CMS verzendt de taakgegevens naar de programmaplanningsservice.
3. De programmaplanningsservice communiceert met de Input File Repository Server (FRS) zodat het programmaobject kan worden opgehaald.

> **Opmerking**
>
> In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

4. De programmaplanningsservice start het programma.
5. De programmaplanningsservice werkt de taakstatus periodiek bij op de CMS. De huidige status is Bezig met verwerken.
6. De programmaplanningsservice verzendt een logbestand naar de Output FRS. De Output File Repository Server meldt via een objectlogbestand aan de programmaplanningsservice dat de planning van het object is gelukt.

> **Opmerking**
>
> In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

7. De programmaplanningsservice werkt de taakstatus periodiek bij op de CMS. De huidige status is Geslaagd.
8. De CMS werkt de taakstatus bij in het geheugen en schrijft de exemplaargegevens vervolgens naar de CMS-systeemdatabase.

3.4.3 Crystal Reports

3.4.3.1 Een SAP Crystal Reports-rapportpagina in de cache weergeven

In deze werkstroom wordt het proces omschreven waarbij een gebruiker een pagina uit een SAP Crystal Reports-rapport (bijvoorbeeld uit de rapportviewer in het BI-startpunt) opvraagt terwijl de rapportpagina al bestaat in een cacheserver. Deze werkstroom geldt voor zowel SAP Crystal Reports 2020 als SAP Crystal Reports voor Enterprise.

> **Opmerking**
>
> Voor deze werkstroom moeten de CMS en de Crystal Reports-cacheserver actief zijn.

1. De webclient verzendt een aanvraag voor weergave in de vorm van een URL via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag en stelt vast dat het een aanvraag betreft om een geselecteerde rapportpagina weer te geven. De webtoepassingsserver verzendt een aanvraag naar de CMS (Central Management Server) om te controleren of de gebruiker beschikt over de vereiste rechten om het rapport weer te geven.
3. De CMS controleert in de CMS-systeemdatabase of de gebruiker over de vereiste rechten beschikt om het rapport weer te geven.
4. De CMS verzendt een reactie naar de webtoepassingsserver om te bevestigen dat de gebruiker de vereiste rechten heeft om het rapport weer te geven.

5. De webtoepassingsserver vraagt bij de Crystal Reports Cache Server de desbetreffende pagina van het rapport aan (EPF-bestand).
6. De Crystal Reports Cache Server controleert of het aangevraagde EPF-bestand voorkomt in de cachemap. In dit voorbeeld wordt het EPF-bestand gevonden.
7. De Crystal Reports Cache Server verzendt de aangevraagde pagina naar de webtoepassingsserver.
8. De webtoepassingsserver verzendt de pagina via de webserver naar de webclient, waar de pagina wordt weergegeven.

3.4.3.2 Een SAP Crystal Reports 2020-rapportpagina weergeven die niet in de cache aanwezig is

In deze werkstroom wordt het proces beschreven waarbij een gebruiker een pagina uit een SAP Crystal Reports 2020-rapport opvraagt (bijvoorbeeld uit de rapportviewer in BI-startpunt), maar de rapportpagina niet bestaat in een cacheserver.

> **Opmerking**
>
> Hiervoor moeten de CMS, Crystal Reports Cache Server, Crystal Reports 2020-verwerkingsserver en Output File Repository Server actief zijn.

1. De gebruiker verzendt de weergaveaanvraag via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag, bepaalt dat het een aanvraag is om een geselecteerde rapportpagina weer te geven en stuurt een aanvraag naar de CMS (Central Management Server) om te controleren of de gebruiker voldoende rechten heeft om het rapport weer te geven.
3. De CMS controleert in de CMS-systeemdatabase of de gebruiker over de vereiste rechten beschikt om het rapport weer te geven.
4. De CMS verzendt een reactie naar de webtoepassingsserver om te bevestigen dat de gebruiker de vereiste rechten heeft om het rapport weer te geven.
5. De webtoepassingsserver vraagt bij de Crystal Reports Cache Server de desbetreffende pagina van het rapport aan (EPF-bestand).
6. De Crystal Reports Cache Server controleert of het aangevraagde bestand voorkomt in de cachemap. In dit voorbeeld wordt het aangevraagde EPF-bestand niet in de cachemap gevonden.
7. De Crystal Reports Cache Server verzendt de aanvraag naar de Crystal Reports 2020-verwerkingsserver.
8. De Crystal Reports 2020-verwerkingsserver voert een query uit op de FRS (Output File Repository Server) naar het opgevraagde rapportexemplaar, en de Output FRS stuurt het opgevraagde rapportexemplaar naar de Crystal Reports 2020-verwerkingsserver.

   > **Opmerking**
   >
   > In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

9. De Crystal Reports 2020-verwerkingsserver opent het rapportexemplaar en controleert of het rapport gegevens bevat.

   De Crystal Reports 2020-verwerkingsserver controleert of het rapport gegevens bevat en maakt het EPF-bestand voor de aangevraagde rapportpagina zonder dat verbinding met de productiedatabase nodig is.

10. De Crystal Reports 2020-verwerkingsserver verzendt het EPF-bestand naar de Crystal Reports Cache Server.
11. De Crystal Reports Cache Server schrijft het EPF-bestand naar de cachemap.
12. De Crystal Reports Cache Server verzendt de aangevraagde pagina naar de webtoepassingsserver.
13. De webtoepassingsserver verzendt de pagina via de webserver naar de webclient, waar de pagina wordt weergegeven.

3.4.3.3 Een SAP Crystal Reports 2020-rapport weergeven op aanvraag

In deze werkstroom wordt het proces beschreven waarbij een gebruiker een SAP Crystal Reports 2020-rapportpagina opvraagt om de nieuwste gegevens weer te geven, bijvoorbeeld uit de rapportviewer in BI-startpunt.

> **Opmerking**
>
> Voor deze werkstroom moeten de CMS, Crystal Reports-cacheserver, Crystal Reports 2020-verwerkingsserver en Input File Repository Server actief zijn.

1. De gebruiker verzendt de weergaveaanvraag via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag en stelt vast dat het een aanvraag betreft om een geselecteerde rapportpagina weer te geven. De webtoepassingsserver verzendt een aanvraag naar de CMS (Central Management Server) om te controleren of de gebruiker beschikt over de vereiste rechten om het rapport weer te geven.
3. De CMS controleert in de CMS-systeemdatabase of de gebruiker over de vereiste rechten beschikt om het rapport weer te geven.
4. De CMS verzendt een reactie naar de webtoepassingsserver om te bevestigen dat de gebruiker de vereiste rechten heeft om het rapport weer te geven.
5. De webtoepassingsserver vraagt bij de Crystal Reports Cache Server de desbetreffende pagina van het rapport aan (EPF-bestand).
6. De Crystal Reports Cache Server controleert of de pagina al bestaat. Als het rapport voldoet aan de vereisten voor het delen van rapporten op aanvraag (binnen de tijd die is ingesteld voor een ander verzoek op aanvraag, databaseaanmelding, parameters), wordt door de Crystal Reports Cache Server een verzoek naar de Crystal Reports 2020-verwerkingsserver verzonden om de pagina te genereren.
7. De Crystal Reports 2020-verwerkingsserver vraagt het rapportobject aan bij de Input FRS (File Repository Server). De Input FRS stuurt een kopie van het object door naar de Crystal Reports 2020-verwerkingsserver.

   > **Opmerking**
   >
   > In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

8. De Crystal Reports 2020-verwerkingsserver opent het rapport in het eigen geheugen en controleert of het gegevens bevat. In dit voorbeeld bevat het rapportobject geen gegevens. De Crystal Reports 2020-verwerkingsserver maakt verbinding met de gegevensbron om de gegevens op te halen en het rapport te genereren.

9. De Crystal Reports 2020-verwerkingsserver verzendt de pagina (EPF-bestand) naar de Crystal Reports Cache Server. Vooruitlopend op nieuwe weergaveaanvragen wordt in de cachemap van de Crystal Reports Cache Server een kopie van het EPF-bestand opgeslagen.
10. De Crystal Reports Cache Server verzendt de pagina naar de webtoepassingsserver.
11. De webtoepassingsserver verzendt de pagina via de webserver naar de webclient, waar de pagina wordt weergegeven.

3.4.3.4 Een planning instellen voor een Crystal Reports-rapport

In deze werkstroom wordt het proces omschreven waarbij een gebruiker een SAP Crystal Reports-rapport in de toekomst plant vanuit een webtoepassing zoals de CMC (Central Management Console) of het BI-startpunt. Deze werkstroom geldt voor zowel SAP Crystal Reports 2020 als SAP Crystal Reports voor Enterprise.

1. De webclient verzendt een planningsaanvraag in de vorm van een URL via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag in de URL en stelt vast of het een planningsaanvraag betreft. De webtoepassingsserver verzendt het geplande tijdstip, de aanmeldingswaarden voor de database, de parameterwaarden, het doel en de indeling naar de opgegeven CMS (Central Management Server).
3. De CMS controleert of de gebruiker de vereiste rechten heeft om het object te plannen. Als de gebruiker over de vereiste rechten beschikt, voegt de CMS een nieuwe record toe aan de CMS-systeemdatabase. Bovendien wordt het exemplaar door de CMS toegevoegd aan de lijst met uitstaande planningen.
4. De CMS stuurt een bericht naar de webtoepassingsserver om te laten weten dat de planning is gelukt.
5. De webtoepassingsserver genereert de volgende HTML-pagina en verzendt deze via de webserver naar de webclient.

3.4.3.5 Een gepland SAP Crystal Reports 2020-rapport wordt uitgevoerd

In deze werkstroom wordt het proces beschreven waarbij een SAP Crystal Reports 2020-rapport op een gepland tijdstip wordt uitgevoerd.

1. De CMS (Central Management Server) controleert in de CMS-systeemdatabase of er een gepland SAP Crystal Reports-rapport is dat op dat tijdstip uitgevoerd moet worden.
2. Op het geplande tijdstip wordt door de CMS een beschikbare planningsservice van Crystal Reports 2020 gezocht die wordt uitgevoerd op een Adaptive Job Server (op basis van de waarde voor *Maximumaantal toegestane taken* die op elke Adaptive Job Server is ingesteld). De CMS verzendt de taakgegevens (rapport-ID, indeling, doel, aanmeldingsgegevens, parameters en selectieformules) naar de planningsservice van Crystal Reports 2020.
3. De planningsservice van Crystal Reports 2020 communiceert met de FRS (Input File Repository Server) om een rapportsjabloon te verkrijgen voor de aangevraagde rapport-ID.

> **Opmerking**
>
> In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

4. De planningsservice van Crystal Reports 2020 start het JobChildserver-proces.
5. Het onderliggende proces (JobChildserver) start `ProcReport.dll` zodra het de sjabloon van de Input File Repository Server ontvangt. `ProcReport.dll` bevat alle parameters die van de CMS naar de planningsservice van Crystal Reports 2020 zijn verzonden.
6. `ProcReport.dll` start `crpe32.dll`, waarmee het rapport wordt verwerkt aan de hand van de doorgegeven parameters.
7. Terwijl het rapport door `crpe32.dll` wordt verwerkt, worden de voor het rapport vereiste records opgehaald uit de gegevensbron.
8. De planningsservice van Crystal Reports 2020 werkt de taakstatus periodiek bij op de CMS. De huidige status is Bezig met verwerken.
9. Wanneer het rapport is samengesteld in het geheugen van de planningsservice van Crystal Reports 2020, kan het naar een andere indeling worden geëxporteerd, bijvoorbeeld PDF (Portable Document Format). Voor het exporteren naar PDF wordt `crxfpdf.dll` gebruikt.
10. Het rapport met de opgeslagen gegevens wordt ingediend bij de geplande locatie (bijvoorbeeld e-mail) en wordt vervolgens verzonden naar de Output FRS.

> **Opmerking**
>
> In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

11. De planningsservice van Crystal Reports 2020 werkt de taakstatus bij op de CMS. De huidige status is Geslaagd.
12. De CMS werkt de taakstatus bij in het geheugen en schrijft de exemplaargegevens vervolgens naar de CMS-systeemdatabase.

3.4.4 Web Intelligence

3.4.4.1 Een SAP BusinessObjects Web Intelligence-document weergeven op aanvraag

Bij deze werkstroom wordt het proces beschreven waarbij een gebruiker een SAP Business Objects Web Intelligence-document opvraagt om de nieuwste gegevens weer te geven, bijvoorbeeld uit de Web Intelligence-viewer in BI-startpunt.

1. Een webbrowser verzendt de weergaveaanvraag via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag en stelt vast dat het een aanvraag betreft om een Web Intelligence-document weer te geven. De webtoepassingsserver verzendt een aanvraag naar de CMS (Central Management Server) om te controleren of de gebruiker beschikt over de vereiste rechten om het document weer te geven.
3. De CMS controleert in de CMS-systeemdatabase of de gebruiker over de vereiste rechten beschikt om het document weer te geven.

4. De CMS verzendt een reactie naar de webtoepassingsserver om te bevestigen dat de gebruiker de vereiste rechten heeft om het document weer te geven.
5. De webtoepassingsserver vraagt het document aan bij de Web Intelligence-verwerkingsserver.
6. De Web Intelligence-verwerkingsserver vraagt het document en het universebestand waarop het document is gebaseerd, aan bij de Input File Repository Server. Het universebestand bevat metalaaggegevens, waaronder beveiliging op rij- en kolomniveau.
7. De Input File Repository Server stuurt een kopie van het document plus het universebestand waarop het aangevraagde document is gebaseerd, naar de Web Intelligence-verwerkingsserver.

   > **Opmerking**
   >
   > In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

8. De Web Intelligence Report-engine (op de Web Intelligence-verwerkingsserver) opent het document in het eigen geheugen en start het bestand `QT.dll` en een verbindingsserver.
9. Het bestand `QT.dll` genereert de SQL, valideert deze en genereert deze opnieuw en voert de query uit in de desbetreffende database. De verbindingsserver gebruikt de SQL om de gegevens over te brengen van de database naar de rapportengine, waar het document wordt verwerkt.
10. De Web Intelligence-verwerkingsserver verzendt de aangevraagde documentpagina die kan worden weergegeven naar de webtoepassingsserver.
11. De webtoepassingsserver verzendt de documentpagina via de webserver naar de webclient, waar de pagina wordt weergegeven.

3.4.4.2 Een planning instellen voor een SAP BusinessObjects Web Intelligence-document

In deze werkstroom wordt het proces omschreven waarbij een gebruiker een SAP BusinessObjects Web Intelligence-document in de toekomst plant vanuit een webtoepassing zoals de CMC (Central Management Console) of het BI-startpunt.

1. De webclient verzendt een planningsaanvraag in de vorm van een URL via de webserver naar de webtoepassingsserver.
2. De webtoepassingsserver interpreteert de aanvraag in de URL en stelt vast of het een planningsaanvraag betreft. De webtoepassingsserver verzendt het geplande tijdstip, de aanmeldingswaarden voor de database, de parameterwaarden, het doel en de indeling naar de opgegeven CMS (Central Management Server).
3. De CMS controleert of de gebruiker de vereiste rechten heeft om het object te plannen. Als de gebruiker over de vereiste rechten beschikt, voegt de CMS een nieuwe record toe aan de CMS-systeemdatabase. Bovendien wordt het exemplaar door de CMS toegevoegd aan de lijst met uitstaande planningen.
4. De CMS stuurt een bericht naar de webtoepassingsserver om te laten weten dat de planning is gelukt.
5. De webtoepassingsserver genereert de volgende HTML-pagina en verzendt deze via de webserver naar de webclient.

3.4.4.3 Een gepland document van SAP BusinessObjects Web Intelligence wordt uitgevoerd

In deze werkstroom wordt het proces omschreven waarbij een gepland SAP BusinessObjects Web Intelligence-document dat wordt uitgevoerd op een gepland tijdstip.

1. De CMS (Central Management Server) controleert in de CMS-systeemdatabase of een Web Intelligence-document is gepland om te worden uitgevoerd.
2. Op de geplande tijd zoekt de CMS een beschikbare planningsservice voor Web Intelligence op een Adaptive Job Server. De CMS verzendt de planningsaanvraag en alle aanvraaggegevens naar de planningsservice voor Web Intelligence.
3. De planningsservice voor Web Intelligence zoekt een beschikbare Web Intelligence-verwerkingsserver op basis van de waarde voor *Maximumaantal verbindingen* die op elke Web Intelligence-verwerkingsserver is ingesteld.
4. De Web Intelligence-verwerkingsserver stelt de locatie vast van de Input FRS (File Repository Server) waarop het document en het metalaagbestand van de universe waarop het document is gebaseerd zich bevinden. Vervolgens vraagt de Web Intelligence-verwerkingsserver het document op bij de Input FRS. De Input FRS zoekt het Web Intelligence-document en het universebestand waarop het document is gebaseerd op en stuurt deze door naar de Web Intelligence-verwerkingsserver.

   > **Opmerking**
   >
   > In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

5. Het Web Intelligence-document wordt in een tijdelijke map op de Web Intelligence-verwerkingsserver geplaatst. De Web Intelligence-verwerkingsserver opent het document in het geheugen, en `QT.dll` genereert de SQL van de universe waarop het document is gebaseerd. De verbindingsserverbibliotheken die zijn opgenomen in de Web Intelligence-verwerkingsserver maken verbinding met de gegevensbron. The querygegevens worden via `QT.dll` doorgegeven aan de Report-engine in de Web Intelligence-verwerkingsserver, waar het document wordt verwerkt. Er is een nieuw exemplaar gemaakt.
6. Het documentexemplaar wordt door de Web Intelligence-verwerkingsserver naar de Output FRS geüpload.

   > **Opmerking**
   >
   > In deze stap moet ook worden gecommuniceerd met de CMS om de desbetreffende server en objecten te lokaliseren.

7. De Web Intelligence-verwerkingsserver geeft aan de planningsservice voor Web Intelligence (op de Adaptive Job Server) door dat het document is gemaakt. Als het document is gepland om naar een doel te worden verzonden (bestandssysteem, FTP, SFTP, SMTP of Postvak IN), wordt het verwerkte document door de Adaptive Job Server bij de Output FRS opgehaald en bij de opgegeven doelen bezorgd. In dit voorbeeld veronderstellen we dat dit niet het geval is.
8. De planningsservice voor Web Intelligence werkt de taakstatus bij op de CMS.
9. De CMS werkt de taakstatus bij in het geheugen en schrijft de exemplaargegevens vervolgens naar de CMS-systeemdatabase.

3.4.5 Analyse

3.4.5.1 Een werkruimte van SAP BusinessObjects Analysis, editie voor OLAP weergeven

In deze werkstroom wordt het proces omschreven waarbij een gebruiker een werkruimte voor SAP Analysis, editie voor OLAP, wilt weergeven vanuit BI-startpunt.

> ⓘ Opmerking
>
> Voor deze werkstroom moeten de CMS, de Adaptive Processing Server (met de MDAS (Multi-Dimensional Analysis Service)) en Input File Repository Server actief zijn.

1. De webclient verzendt een aanvraag om een nieuwe werkruimte weer te geven via de webserver naar de webtoepassingsserver. De webclient communiceert met de webtoepassingsserver via DHTML AJAX-technologie (Asynchrone JavaScript en XML). De AJAX-technologie maakt het mogelijk om pagina's gedeeltelijk bij te werken, waardoor er niet bij elke nieuwe aanvraag een nieuwe pagina hoeft te worden opgebouwd.
2. De webtoepassingsserver converteert de aanvraag en verzendt deze naar de CMS (Central Management Server), waar wordt gecontroleerd of de gebruiker over de vereiste rechten beschikt om een nieuwe werkruimte weer te geven of te maken.
3. De CMS haalt de referenties van de gebruiker op bij de CMS-systeemdatabase.
4. Als de gebruiker de vereiste rechten heeft om een werkruimte weer te geven of te maken, ontvangt de webtoepassingsserver groen licht van de CMS. Tegelijkertijd wordt er een lijst met een of meer beschikbare exemplaren van de MDAS (Multi-Dimensional Analysis Services) verstuurd.
5. De webtoepassingsserver kiest een MDAS uit deze lijst en verzendt een CORBA-aanvraag naar de service om de juiste OLAP-server(s) te vinden voor het maken van een nieuwe werkruimte of het vernieuwen van een bestaande werkruimte.
6. De MDAS moet verbinding maken met de Input FRS (File Repository Server) om het juiste werkruimtedocument op te halen dat informatie bevat over de onderliggende OLAP-database en waarbij een eerste OLAP-query is opgeslagen. De Input FRS haalt de relevante Analysis-werkruimte op uit de onderliggende map en stuurt deze werkruimte door naar de MDAS.
7. De MDAS opent de werkruimte, stelt een query op en verzendt deze naar de OLAP-databaseserver. Voor de MDAS moet er een OLAP-databaseclient geconfigureerd zijn voor de OLAP-gegevensbron. De query van de webclient moet naar de juiste OLAP-query worden geconverteerd. De OLAP-databaseserver retourneert het queryresultaat naar de MDAS.
8. Op basis van de aanvraag voor maken, weergeven, afdrukken of exporteren wordt het resultaat door de MDAS voorbewerkt, zodat de Java WAS het opbouwen sneller kan voltooien. De MDAS retourneert XML-pakketten met het eindresultaat naar de webtoepassingsserver.
9. De webtoepassingsserver bouwt de werkruimte op en verzendt de opgemaakte pagina of een deel van de pagina via de webserver naar de webclient. De bijgewerkte of nieuwe pagina wordt op de webclient weergegeven. Dit is een Zero-Clientoplossing waarvoor geen Java- of ActiveX-onderdelen hoeven te worden gedownload.

3.5 Integratie met launchpad voor SAP Fiori op SAP Enterprise Portal

Overzicht

Door de integratie van SAP BusinessObjects BI met launchpad voor SAP Fiori-platforms kunnen eindgebruikers van SAP Enterprise Portal de BI-rapporten in SAP BusinessObjects CMS weergeven. Op het tabblad hebben eindgebruikers toegang tot BI-rapporten waarvan de maphiërarchie overeenkomt met die in SAP BusinessObjects CMS.

Vereisten

- Business Intelligence 4.2 SP4
- Web Dispatcher 7.49 voor de connectiviteit
- NetWeaver 7.5 SP7
- Verificatie Active Directory en SSO-configuratie op basis van Kerberos zoals beschreven in SAP Note 1631734

Procedure

De inhoudbeheerder van het SAP Fiori-startpunt en de Enterprise Portal-beheerder kunnen SAP BusinessObjects Enterprise integreren met het Fiori-startpunt.

Zie Integratie van SAP BusinessObjects Enterprise in SAP NetWeaver 7.5 Portal-documentatie voor volledige configuratie informatie.

> **Opmerking**
>
> - BI-platform biedt nu ondersteuning voor OData-services voor de integratie tussen het launchpad voor SAP Fiori en SAP Enterprise Portal.
> - BI-platform biedt ondersteuning voor OData-services op SAP NetWeaver Application Server.
> - U hebt na de integratie toegang tot de Openbare mappen, Persoonlijke mappen en het Postvak IN voor BI vanuit SAP Enterprise Portal.

4 Wizard Systeemconfiguratie

4.1 Inleiding tot de wizard Systeemconfiguratie

Nadat u SAP BusinessObjects Business Intelligence-platform hebt geïnstalleerd, wilt u waarschijnlijk essentiële configuratietaken uitvoeren, zoals een implementatiesjabloon kiezen en de SAP BusinessObjects-producten kiezen die uw organisatie gaat gebruiken. Om deze configuratie uit te voeren en zo snel mogelijk aan de slag te gaan met het BI-platform, voert u de *wizard Systeemconfiguratie* uit.

Belangrijke voordelen van de wizard

- De wizard geeft extra uitleg en begeleidt u bij de configuratiestappen die u moet uitvoeren.
- U verkleint de kans op een onjuiste systeemconfiguratie door de wizard te gebruiken.
- De wizard configureert instellingen voor u, waardoor de systeemconfiguratie sneller verloopt.

De wizard is standaard ingesteld om automatisch te worden uitgevoerd wanneer u zich aanmeldt bij de CMC (Central Management Console), maar u kunt de wizard ook starten via het gebied *Beheren* in de CMC. U kunt de wizard op elk moment opnieuw uitvoeren om uw configuratie aan te passen, en u kunt via de beheerpagina *Servers* in de CMC altijd instellingen beter afstemmen, waaronder de instellingen die u via de wizard hebt geconfigureerd.

> ⓘ Opmerking
>
> Voor verbeterde beveiliging hebben alleen leden van de groep Beheerders toegang tot de wizard.

> ⓘ Opmerking
>
> Om te voorkomen dat de wizard automatisch wordt uitgevoerd, kan de “beheerder”gebruiker het selectievakje *Deze wizard niet weergeven wanneer de CMC wordt gestart* op de eerste pagina van de wizard inschakelen.

> ⓘ Opmerking
>
> Als u van plan bent invoegtoepassingen te installeren of knooppunten aan uw BI-platformimplementatie toe te voegen, is het raadzaam deze stappen uit te voeren voordat u de wizard Systeemconfiguratie uitvoert.

4.2 De producten opgeven die u gebruikt

U kunt de configuratie van BI-platformservers vereenvoudigen door de producten op te geven die uw organisatie gebruikt, en u kunt brontoewijzing optimaliseren door de servers te stoppen voor producten die uw organisatie niet gebruikt. Hiervoor selecteert u producten op de pagina *Producten*. Wanneer u producten opgeeft die uw organisatie gebruikt, start de wizard alle servers en afhankelijkheden die vereist zijn om deze

producten te gebruiken, en worden deze servers en afhankelijkheden geconfigureerd om automatisch te worden gestart wanneer het BI-platform start. Bovendien kunt u door de selectie van niet-gebruikte producten op te heffen, de opstarttijd en het bronverbruik van het BI-platform verbeteren.

Als u bijvoorbeeld het product Crystal Reports selecteert, start het BI-platform automatisch alle Crystal Reports-servers en toepasselijke afhankelijkheden.

Voor een lijst met servers die automatisch voor een product worden gestart, klikt u op het pictogram *?* naast de naam van een product.

De wizard configureert productservers als volgt:

- Wanneer u een product selecteert, worden alle servers voor dat product gestart, evenals andere servers die vereist zijn om dat product te gebruiken (afhankelijkheden), wanneer de wizard wordt voltooid. Wanneer u een product selecteert, wordt ook ingesteld dat de servers van dat product automatisch met het BI-platform worden gestart. Als een server services van meerdere producten host, wordt de server gestart wanneer een van deze producten wordt geselecteerd. Sommige services van producten die niet zijn geselecteerd, zijn mogelijk actief als ze worden gehost door een server die ook services host van producten die zijn geselecteerd.
- Wanneer u selectie van een product opheft, worden de servers voor dit product gestopt, mits deze servers niet ook services hosten van een product dat nog geselecteerd is, of sercies die tot de categorie Kernservices behoren. De gestopte productservers worden ingesteld om niet automatisch te starten met het BI-platform. Als een server services host van geselecteerde en niet-geselecteerde producten, blijft de server actief.
- Als u selectie van een product opheft, kan het voorkomen dat servers worden gestopt die niet tot dit product behoren, als er afhankelijke services zijn die alleen door dit product worden gebruikt. Hiermee worden bronnen vrijgemaakt, omdat deze afhankelijke servers niet langer nodig zijn.
- Wanneer u een product selecteert of selectie ervan opheft, worden alle servers die services hosten van de categorie Kernservice in het BI-platform (met uitzondering van services die door WACS worden gehost), automatisch gestart. De WACS behoudt de huidige status.
- Wanneer u selectie van een product opheft, worden bestanden voor dit product niet verwijderd.

Wanneer u de pagina *Producten* opent, representeren de productstatussen op de pagina de huidige status van het systeem.

Als alle servers voor een product actief zijn, is het selectievakje voor dat product ingeschakeld. Als alle servers voor een product gestopt zijn, is het selectievakje voor dat product uitgeschakeld. Als slechts enkele servers voor een product actief zijn terwijl andere servers een andere status hebben, bijvoorbeeld gestopt, wordt op de pagina *Producten* het selectievakje *Bestaande configuratie behouden* weergegeven om aan te geven dat het systeem buiten de wizard om is geconfigureerd. U kunt het selectievakje uitschakelen als u de wizard wilt gebruiken om uw configuratie te wijzigen.

> **Opmerking**
>
> Op de pagina *Producten* worden alle producten weergegeven die in het cluster zijn geïnstalleerd. Als op computer A bijvoorbeeld producten P1 en P2 zijn geïnstalleerd en op computer B producten P2 en P3, ziet u producten P1, P2 en P3 op de pagina *Producten*. Niet-geïnstalleerde producten worden niet op de pagina *Producten* weergegeven.

> **Opmerking**
>
> Ter vereenvoudiging van de implementatie hoeft de configuratie op deze pagina niet voor elk knooppunt worden herhaald maar wordt de configuratie op het gehele cluster toegepast.

> **Opmerking**
>
> Als instellingen reeds in de CMC zijn gewijzigd, geeft de wizard een bericht weer om te melden dat de instellingen buiten de wizard om zijn gewijzigd. U kunt de bestaande configuratie behouden of de huidige instellingen overschrijven.

> **Opmerking**
>
> Wijzigingen die u in de wizard maakt, worden toegepast wanneer u op *Toepassen* op de pagina *Controleren* klikt.

Wanneer u uw wijzigingen hebt gemaakt, klikt u op *Volgende* om naar de volgende pagina van de wizard te gaan. U kunt ook via het navigatievenster aan de linkerkant rechtstreeks naar een eerder bezochte pagina gaan.

4.3 Een implementatiesjabloon kiezen

Bij de standaardinstallatie van het BI-platform wordt een kleine implementatie geconfigureerd die geschikt is voor een demo-omgeving op beperkte systeemhardware. Kies een van de vooraf gedefinieerde implementatiesjablonen op de pagina *Capaciteit* om de implementatie beter af te stemmen op uw hardware en beoogde gebruik (bijvoorbeeld een test- of productiesysteem voorbereiden). Deze sjablonen zijn bedoeld om u snel aan de slag te laten gaan met uw BI-platformsysteem en de tijd die benodigd is voor de eerste implementatie, te verkorten.

Hoewel het kiezen van een toepasselijk implementatiesjabloon helpt bij de eerste configuratie en een goed beginpunt biedt, vormt het geen vervanging van het aanpassen en afstellen van uw systeem, dat ook moet worden uitgevoerd. Voor optimale prestaties past u uw systeem aan met behulp van toepasselijke richtlijnen: http://www.sap.com/bisizing

Er zijn verschillende redenen waarom het belangrijk is om een geschikte implementatiesjabloon te kiezen:

- De capaciteit van uw systeem voor de verwerking van verzoeken wordt beïnvloed door de implementatiesjabloon die u kiest. Een grotere implementatie biedt meer capaciteit voor de verwerking van grotere aantallen of complexere verzoeken. Een grotere implementatie vereist echter meer systeembronnen.
- Een grotere implementatie betekent niet persé betere prestaties, met name wanneer u niet over voldoende beschikbare hardwarebronnen beschikt.
- De implementatiesjabloon die u kiest, moet afgestemd zijn op uw bedrijfsvereisten en uw beschikbare hardwarebronnen. Het systeem heeft mogelijk verminderde capaciteit en vertraagde prestaties als u een sjabloon kiest die te klein is voor uw bedrijfsbehoeften of te groot voor de beschikbare hardwarebronnen.
- Grotere implementatiesjablonen bieden betere verdeling: er is minder kans dat fouten in een bepaald product invloed hebben op andere producten. Kies een sjabloon met een goed evenwicht tussen bronverbruik (RAM) en prestaties. Als er bijvoorbeeld een grote hoeveelheid RAM beschikbaar is, kunt u de grootste implementatiesjabloon kiezen die uw RAM toestaat zodat u profiteert van betere systeemverdeling.

U kunt met de schuifregelaar een implementatiesjabloon kiezen, of u kunt een RAM-hoeveelheid in de vervolgkeuzelijst kiezen. Wanneer u de instelling wijzigt, kunt u zien dat de indicator van *Aantal Adaptive Processing Servers* ook verandert om aan te geven hoe uw systeem wordt geconfigureerd als u die instelling kiest.

ⓘ Opmerking

De gekozen implementatiesjabloon heeft alleen betrekking op de APS (Adaptive Processing Servers), en niet op andere servers, zoals de CMS of Adaptive Job Servers.

ⓘ Opmerking

Hoeveelheid vereiste RAM is de minimumhoeveelheid RAM die is vereist voor BI-platformservers. Op een computer met 16 GB RAM waarbij het besturingssysteem 1 GB RAM gebruikt, de databaseserver ook 1 GB gebruikt en de servers van het BI-platform 10 GB gebruiken, is de vereiste RAM gelijk aan 10 GB, niet 12 of 16 GB. Het cijfer voor vereiste RAM is slechts een representatie van een standaardwaarde; bij een zware belasting kan uw systeem meer RAM nodig hebben. Voor optimale systeemprestaties moet u het systeem altijd aanpassen.

ⓘ Opmerking

Wanneer u de pagina *Capaciteit* opent, is de implementatiesjabloon op de pagina een representatie van de huidige systeemstatus, als deze overeenkomt met een van de vooraf gedefinieerde implementatiesjablonen. Als u bijvoorbeeld handmatig een extra Adaptive Processing Server hebt gemaakt met de CMC, komt de huidige status van uw systeem niet overeen met de implementatiesjablonen. Op de pagina *Capaciteit* wordt dus het selectievakje *Bestaande configuratie behouden* weergegeven om aan te geven dat het systeem buiten de wizard om is geconfigureerd. In een implementatie met meerdere knooppunten wordt het selectievakje *Huidige configuratie behouden* ook weergegeven als een knooppunt een aantal APS's heeft die niet overeenkomen met een implementatiesjabloon, of als het aantal APS's op verschillende knooppunten niet overeenkomt. U kunt het selectievakje uitschakelen als u de wizard wilt gebruiken om uw configuratie te wijzigen.

ⓘ Opmerking

Ter vereenvoudiging van de implementatie wordt de geselecteerde APS-configuratie op elk knooppunt toegepast (mits een APS op deze knooppunten is geïnstalleerd). Hoe meer knooppunten u dus heeft, des te meer capaciteit uw cluster zal hebben.

ⓘ Opmerking

Invoegtoepassingen (bijvoorbeeld Data Services of AADS (Analysis Application Design Service)) worden niet beheerd door de wizard. Services die door de invoegtoepassingen worden gemaakt, worden door de wizard niet naar andere Adaptive Processing Servers verplaatst.

Voorbeelden:

- Als AADS wordt gehost door een APS die andere services van de hoofdinstallatie van BI-platform host, en u voert de wizard uit en wijzigt de grootte van de implementatiesjabloon van XS naar M, maakt de wizard zeven nieuwe Adaptive Processing Servers en worden alle services naar de zeven servers verplaatst, met uitzondering van de AADS-service die op de oorspronkelijke APS blijft staan.
- De invoegtoepassing Data Services maakt een specifieke APS. De wizard wijzigt deze specifieke APS niet en telt deze APS niet wanneer het aantal Adaptive Processing Servers in het systeem wordt gerapporteerd.

Het bestand DeploymentTemplates.pdf

Voor een uitgebreide beschrijving van de instellingen die de wizard configureert voor elke beschikbare implementatiesjabloon, klikt u op de koppeling voor de *implementatiesjabloon* op de pagina *Capaciteit* om het bestand `DeploymentTemplates.pdf` te openen.

In het bestand `DeploymentTemplates.pdf` worden de implementatiesjablonen uitvoerig besproken. In de sjablonen wordt niet opgegeven hoeveel gebruikers kunnen worden ondersteund, omdat dit aantal afhankelijk is van de belasting. U moet het systeem aanpassen om te bepalen hoeveel gebruikers u moet ondersteunen, en dus de hoeveelheid vereiste RAM, de CPU-vereisten enzovoort.

4.4 Locaties voor gegevensmappen opgeven

Op de pagina *Mappen* kunt u opgeven waar het BI-platform de gegevens- en logboekbestanden moet opslaan. U kunt maplocaties opgeven of de huidige locaties accepteren.

Als uw BI-platformimplementatie meerdere knooppunten heeft, hebt u twee opties om de maplocaties te definiëren:

- Als u dezelfde maplocaties voor alle knooppunten wilt configureren, selecteert u de optie *Alle knooppunten hebben dezelfde maplocaties*.
- Als de servers in uw cluster niet identiek zijn ingesteld, kunnen de installatiepaden of de bestandsmapstructuren verschillen. U kunt de optie *Knooppunten hebben verschillende maplocaties* kiezen om specifieke maplocaties voor elk knooppunt te configureren.

Wanneer de wizard wordt geopend op de pagina *Mappen*, worden de mapnamen als volgt weergegeven:

- Als alle knooppunten mappen hebben met precies dezelfde waarden (dat wil zeggen, alle logboekmappen op alle servers in het cluster zijn identiek, en alle gegevensmappen op alle servers in het cluster zijn identiek, enzovoort), is de optie *Alle knooppunten hebben dezelfde maplocaties* geselecteerd en worden de huidige mapnamen weergegeven.
- Als alle mappen van een bepaald type (Logboek, Gegevens, Controle, Opslag van invoerbestand, Opslag van uitvoerbestand) identiek zijn binnen elk knooppunt maar anders zijn tussen de knooppunten, is de optie *Knooppunten hebben verschillende maplocaties* geselecteerd en worden de huidige mapnamen weergegeven.
- Als alle mapnamen van een bepaald type niet identiek zijn binnen elk knooppunt en verschillend zijn tussen de knooppunten, is de optie *Knooppunten hebben verschillende maplocaties* geselecteerd maar zijn de mapnamen leeg.

Als u de locaties van de mappen wijzigt, configureert de wizard het systeem om de nieuwe mappen te gebruiken. Met uitzondering van de controlegegevensmap kopieert of verplaatst de wizard de inhoud van de oorspronkelijke mappen niet naar de nieuwe mappen. Als de nieuwe mappen niet reeds de juiste inhoud bevatten, of als u gegevens in de oorspronkelijke mappen hebt die u wilt migreren, wilt u die gegevens wellicht naar de nieuwe mappen verplaatsen of kopiëren.

Als de nieuwe maplocatie voor de mappen Opslag van invoerbestand, Opslag van uitvoerbestand en Gegevens leeg is, moet u de bestanden handmatig uit de oude maplocatie kopiëren of de bestanden uit een back-up herstellen. Voor de logboekmap kopieert u bestanden alleen uit de oude map als u wilt dat de nieuwe map de logboekbestanden bevat die op de oude maplocatie staan.

→ Tip

Als u van plan bent bestanden naar de nieuwe mappen te kopiëren of herstellen, moet u dit doen voordat u de knooppunten opnieuw start.

Voorbeeldscenario's:

- Als u een maplocatie wijzigt en de oorspronkelijke map bevat rapporten, zijn deze rapporten niet beschikbaar in het BI-platform tot u ze naar de nieuwe map kopieert en de knooppunten opnieuw opstart.
- Als uw oorspronkelijke map beschadigde of gewijzigde rapporten bevat en u wilt terugkeren naar een back-up waarvan u weet dat deze in orde is, haalt u de rapporten op uit de back-up en zet u ze in de nieuwe map, in plaats van de inhoud in de oorspronkelijke map te kopiëren.
- Als uw gegevensbestanden oorspronkelijk op een schijf met stationsletter X stonden en u wijzigt de stationsletter naar Y in het besturingssysteem, hoeft u de gegevensbestanden niet te kopiëren of verplaatsen, maar wijzigt u alleen de maplocatie in het BI-platform.

Als u bepaalde maplocaties handmatig hebt gewijzigd zodat sommige servers op een knooppunt één set mappen gebruiken terwijl andere servers op hetzelfde knooppunt andere mappen gebruiken, wordt op de pagina *Mappen* het selectievakje *Bestaande configuratie behouden* weergegeven om aan te geven dat het systeem buiten de wizard om is geconfigureerd. U hebt bijvoorbeeld twee File Repository Servers op hetzelfde knooppunt geconfigureerd om verschillende paden voor logboekmappen te gebruiken. U kunt het selectievakje uitschakelen als u de wizard wilt gebruiken om de huidige configuratie te wijzigen.

Voor meer informatie over de typen bestanden die in elke map zijn opgeslagen, klikt u op de *?*-pictogrammen.

ⓘ Opmerking

Als u de volgende maplocaties wijzigt, moet u nadat de wizard is voltooid, alle knooppunten handmatig opnieuw starten om de wijzigingen te implementeren:

- Opslag invoerbestand
- Opslag uitvoerbestand
- Logboekmap
- Gegevensmap

4.5 Uw wijzigingen controleren

Wanneer u uw configuratie-instellingen hebt gekozen, worden ze op de pagina *Controleren* weergegeven zodat u ze kunt bekijken voordat de wijzigingen op uw BI-platformsysteem worden toegepast. Voor elke categorie met instellingen kunt u op *Details* klikken voor een uitgebreide beschrijving of weergave van de instellingen en de wijzigingen die worden toegepast.

Als u instellingen wilt wijzigen, kunt u rechtstreeks via het navigatiemenu aan de linkerkant van de wizard naar de afzonderlijke pagina's gaan.

Uw selecties worden opgeslagen naar een logboekbestand, dat u kunt downloaden vanaf de pagina Voltooid.

Er wordt ook een antwoordbestand gegenereerd en opgeslagen. Het antwoordbestand helpt u om configuratie van uw systeem te automatiseren. U kunt op de knop *Downloaden* klikken om het antwoordbestand weer te geven of naar een lokale schijf te downloaden.

Wanneer u op *Toepassen* klikt, worden uw configuratie-instellingen toegepast op uw BI-platformimplementatie. Wanneer de wizard is voltooid, wordt de pagina *Voltooid* weergegeven met de volgende stappen die u handmatig moet uitvoeren.

Verwante informatie

Logboekbestanden en antwoordbestanden [pagina 93]

4.6 Logboekbestanden en antwoordbestanden

Op de pagina *Voltooid* ziet u de status van uw wijzigingen en kunt u de logboek- en antwoordbestanden voor uw sessie downloaden en weergeven.

De logboek- en antwoordbestanden worden automatisch opgeslagen naar de map Wizard Systeemconfiguratie, die u kunt oproepen vanuit de CMC. De bestandsnamen hebben een tijdstempel met de notatie `jaar_maand_dag_uur_minuut_seconde`. Logboekbestanden hebben de extensie `.log`, antwoordbestanden de extensie `.ini`.

U kunt ook op de *download*knoppen klikken om de logboek- en antwoordbestanden weer te geven of naar een lokale schijf te downloaden.

Het logboekbestand heeft de volgende inhoud:

- Een record van alle wijzigingen die u in deze configuratiesessie hebt aangebracht.
- De locatie van het antwoordbestand.
- Een lijst met de volgende stappen die u moet uitvoeren.

Verwante informatie

Een antwoordbestand gebruiken [pagina 93]

4.6.1 Een antwoordbestand gebruiken

Elke keer wanneer de wizard wordt voltooid, wordt een antwoordbestand opgeslagen met uw selecties of antwoorden op de vragen van de wizard. U kunt het antwoordbestand gebruiken om andere clusters in uw BI-platformimplementatie te configureren zonder hiervoor de wizard te gebruiken. U kunt het antwoordbestand ook later gebruiken als u dezelfde configuratie voor het systeem wilt gebruiken. Met een antwoordbestand kunt u uw implementatie automatiseren en operatorfouten vermijden.

Als u een antwoordbestand wilt gebruiken, voert u een script uit dat het antwoordbestand als parameter gebruikt. Ga om te beginnen naar het antwoordbestand dat u wilt gebruiken en sla het op naar een

schijf. Antwoordbestanden worden automatisch opgeslagen naar de map Wizard Systeemconfiguratie, die beheerders kunnen oproepen vanuit de CMC. De bestandsnamen hebben een tijdstempel met de notatie `jaar_maand_dag_uur_minuut_seconde` en hebben een `INI`-extensie. Via de CMC kunt u het antwoordbestand weergeven en naar schijf opslaan, of de menuopdrachten *Ordenen* > *Verzenden* > *Bestandslocatie* gebruiken.

U kunt het antwoordbestand voor uw huidige wizardsessie ook downloaden via de pagina *Controle* of *Voltooid* en naar schijf opslaan.

Als u de instellingen in het antwoordbestand wilt wijzigen voordat u het bestand gebruikt, kunt u het bestand in een teksteditor bewerken. In het onderstaande voorbeeld van een antwoordbestand vindt u meer details.

Het script uitvoeren

Wanneer u het juiste antwoordbestand hebt, gebruikt u het bestand als opdrachtregelparameter voor de scripts die de wizard uitvoeren:

- Voer in Windows het bestand `SWC.bat` uit.
- Voer in Unix het bestand `scw.sh` uit.

De batch- en scriptbestanden staan in dezelfde map waar andere scripts voor serverbeheer zijn opgeslagen:

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

De batch- en scriptbestanden gebruiken de volgende opdrachtregelparameters:

- `-help`: geef de Help van de opdrachtregel weer.
- `-r`: geef het pad en de naam van het antwoordbestand op.
- `-cms`: geef de CMS (Central Management Server) op waarbij u zich wilt aanmelden. Als deze parameter wordt weggelaten, gaat de CMS standaard naar de lokale computer en de standaardpoort (6400). Voorbeeld: `computer_naam:6500`
- `-username`: geef een account op die beheerdersrechten aan het BI-platform verleent. Als deze parameter wordt weggelaten, wordt de standaardbeheerdersaccount gebruikt.
- `-password`: geef het wachtwoord voor de account op. Als u niets opgeeft, wordt een leeg wachtwoord gebruikt. Als u de parameter `-password` wilt gebruiken, moet u ook de parameter `-username` gebruiken.

Voorbeelden

In Windows: `SCW.bat –r c:\folder\filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

In Unix: `./scw.sh –r /home/folder/filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

Voorbeeldantwoordbestand

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

Alle instellingen in het antwoordbestand moeten worden opgegeven, en instellingen mogen niet leeg zijn, met de volgende uitzonderingen:

- Als u een implementatie met meerdere knooppunten hebt, kunt u ervoor kiezen om de mapinstellingen voor een of meer knooppunten weg te laten. De mappen op deze knooppunten blijven dan ongewijzigd. Voor de knooppunten die u in het antwoordbestand opgeeft, moeten echter alle maplocaties worden opgegeven.
- Als de parameter `KeepExistingConfiguration` is ingesteld op `true`, kunt u de overige instellingen voor die pagina weglaten. Voorbeeld: als `Products.KeepExistingConfiguration = true`, kunt u de overige instellingen voor *Producten* weglaten uit het antwoordbestand.

In sommige gevallen bevat het antwoordbestand andere producten dan de producten die in uw doelcluster zijn geïnstalleerd. In deze gevallen is de volgende werking van toepassing:

- Als het antwoordbestand geen definities voor producten bevat die in het doelcluster zijn geïnstalleerd, mislukt de bewerking.
- Als het antwoordbestand definities bevat voor producten die niet voorkomen in het doelcluster, wordt een waarschuwing toegevoegd aan het logboekbestand en worden de overige producten goed geconfigureerd.

> **ⓘ Opmerking**
>
> Nadat u een antwoordbestand hebt gebruikt om een cluster te configureren, moet u handmatig de extra stappen uitvoeren die in de sectie “Volgende stappen” van het logboekbestand zijn beschreven.

> **ⓘ Opmerking**
>
> Voor extra beveiliging is alleen ondersteuning voor Enterprise-verificatie vereist (niet Windows AD, LDAP of SAP).

> **ⓘ Opmerking**
>
> Als u het opnieuw opstarten van knooppunten liever uitstelt tot de volgende geplande datum voor opnieuw opstarten, voert u het script vlak voor een geplande downtime van het systeem uit.

5 Licenties beheren

5.1 Licentiesleutels beheren

In deze sectie wordt beschreven hoe u licentiesleutels kunt beheren voor uw BI-platformimplementatie.

Verwante informatie

Licentiegegevens weergeven [pagina 97]
Een licentiesleutel toevoegen [pagina 97]
De huidige accountactiviteit weergeven [pagina 98]

5.1.1 Licentiegegevens weergeven

In het beheergebied *Licentiesleutels* van de CMC staat het aantal gelijktijdige licenties, licenties op naam en processorlicenties dat aan een sleutel is gekoppeld.

1. Ga naar het beheergebied *Licentiesleutels* van de CMC.
2. Selecteer een licentiesleutel.

   De gegevens die bij de sleutel horen, worden in het gebied *Licentiesleutelinformatie* weergegeven. Als u extra licentiesleutels wilt aanschaffen, neemt u contact op met de SAP-verkoopvertegenwoordiger.

Verwante informatie

Een licentiesleutel toevoegen [pagina 97]
De huidige accountactiviteit weergeven [pagina 98]

5.1.2 Een licentiesleutel toevoegen

Als u een upgrade uitvoert vanuit een testversie van het product, moet u de evaluatiesleutel verwijderen voordat u nieuwe licentiesleutels of productactiveringscodes toevoegt. Nadat u de nieuwe licentiesleutels hebt toegevoegd, moet u alle servers opnieuw activeren.

> **Opmerking**
>
> Als u nieuwe licentiesleutels hebt ontvangen omdat de implementatiemethode van BI-platformlicenties binnen uw organisatie is gewijzigd, moet u alle oude licentiesleutels van het systeem verwijderen om compatibiliteit te kunnen garanderen.

> **Opmerking**
>
> Als u vanaf eerdere versies een update uitvoert naar SAP BusinessObjects Business Intelligence-platform 4.2 Support Package 2 of een latere versie, zullen de bestaande licenties zich als verlopen licenties gedragen. U moet een nieuwe licentiesleutel voor SAP BusinessObjects Business Intelligence-platform 4.2 genereren en gebruiken.

1. Ga naar het beheergebied *Licentiesleutels* van de CMC.
2. Typ de sleutel in het vak *Sleutel toevoegen*.
3. Klik op *Toevoegen*.

De sleutel wordt aan de lijst toegevoegd.

Verwante informatie

Licentiegegevens weergeven [pagina 97]
De huidige accountactiviteit weergeven [pagina 98]

5.1.3 De huidige accountactiviteit weergeven

1. Ga naar het beheergebied *Instellingen* van de CMC.
2. Klik op *Globale systeemgegevens weergeven*.

   Hier worden het huidige licentiegebruik en aanvullende informatie over de taken weergegeven.

Verwante informatie

Een licentiesleutel toevoegen [pagina 97]
Licentiegegevens weergeven [pagina 97]

6 Gebruikers en groepen beheren

6.1 Overzicht van accountbeheer

Accountbeheer omvat alle taken die betrekking hebben op het maken, toewijzen, wijzigen en organiseren van gebruikers- en groepsgegevens. U kunt deze taken uitvoeren in het beheergebied *Gebruikers en groepen* van de CMC (Central Management Console).

Wanneer de gebruikersaccounts en groepen zijn gemaakt, kunt u objecten toevoegen en de rechten voor deze objecten opgeven. Wanneer de gebruikers zich aanmelden, kunnen ze de objecten bekijken in BI-startpunt of in hun eigen webtoepassing.

6.1.1 Gebruikersbeheer

In het beheergebied *Gebruikers en groepen* kunt u alle instellingen opgeven die vereist zijn om een gebruiker toegang te verlenen tot het BI-platform. U kunt ook de twee standaardgebruikersaccounts weergeven die zijn vermeld in de tabel "Standaardgebruikersaccounts".

Standaardgebruikersaccounts

Accountnaam	Beschrijving
Beheerder	Deze gebruiker is lid van de groepen *Administrators* en *Iedereen*. Een beheerder kan alle taken uitvoeren in alle BI-platformtoepassingen (bijvoorbeeld de CMC, CCM, Wizard Publiceren en BI-startpunt).
Guest	Deze gebruiker is lid van de groep *Iedereen*. Deze account is standaard ingeschakeld en krijgt niet automatisch een wachtwoord toegewezen door het systeem. Als u aan deze account een wachtwoord toewijst, werkt de eenmalige aanmelding van BI-startpunt niet meer.
SMAdmin	Dit is een alleen-lezen account die door SAP Solution Manager wordt gebruikt om onderdelen van BI-platform op te roepen.

> **Opmerking**
>
> Objectmigraties kunnen het beste worden uitgevoerd door leden van de Beheerdersgroep, met name de gebruikersaccount Beheerder. Als u een object wilt migreren, moeten veel verwante objecten misschien ook worden gemigreerd. Het is misschien niet mogelijk om de vereiste beveiligingsrechten voor alle objecten te verkrijgen voor een gedelegeerde beheerdersaccount.

6.1.2 Groepsbeheer

Groepen zijn verzamelingen gebruikers die dezelfde accountrechten hebben. U kunt bijvoorbeeld groepen maken waarvan de gebruikers werken op dezelfde afdeling, dezelfde functie hebben of op dezelfde locatie werken. Met groepen kunt u de rechten voor gebruikers op één plaats (een groep) wijzigen, zodat u niet voor elke gebruikersaccount afzonderlijk rechten hoeft te wijzigen. Bovendien kunt u objectrechten aan een groep toewijzen.

In het gebied *Gebruikers en groepen* maakt u groepen die een aantal mensen toegang geven tot een rapport of map. Als u groepen definieert, kunt u wijzigingen op één plaats aanbrengen (voor de groep) en hoeft u niet elke gebruikersaccount afzonderlijk te wijzigen. U kunt ook de diverse standaardgroepsaccounts weergeven die zijn vermeld in de tabel "Standaardgroepsaccounts".

Als u beschikbare groepen in de CMC wilt weergeven, klikt u in de *structuurweergave* op *Groepenlijst*. U kunt ook op *Groepshiërarchie* klikken om een hiërarchisch overzicht van alle beschikbare groepen weer te geven.

Standaardgroepsaccounts

Accountnaam	Beschrijving
Administrators	Leden van deze groep kunnen alle taken uitvoeren in alle BI-platformtoepassingen (CMC, CCM, Wizard Publiceren en BI-startpunt). De groep *Administrators* bevat standaard alleen de beheerders.
Iedereen	Iedere gebruiker is lid van de groep *Iedereen*.
QaaWS-groep ontwerpen	Leden van deze groep hebben toegang tot Query als een webservice.
Gebruikers van het hulpprogramma voor rapportconversie	Leden van deze groep hebben toegang tot het hulpprogramma voor rapportconversie.
Vertaalprogramma's	Leden van deze groep hebben toegang tot de toepassing Translation Manager.
Gebruikers van Universe Designer	Gebruikers die tot deze groep behoren, hebben toegang tot de mappen *Universe Designer* en *Connections*. Deze gebruikers kunnen bepalen wie toegangsrechten heeft tot de toepassing Designer. U voegt gebruikers aan deze groep toe wanneer dit nodig is. Standaard behoort geen enkele gebruiker tot deze groep.

Verwante informatie

Werking van rechten in BI-platform [pagina 123]
Toegang verlenen aan gebruikers en groepen [pagina 112]

6.1.3 Beschikbare verificatietypen

Voordat u gebruikersaccounts en groepen in het BI-platform instelt, bepaalt u welk verificatietype u wilt gebruiken: De tabel "Verificatietypen" bevat een overzicht van de beschikbare verificatietypen voor elk beveiligingsprogramma dat in uw bedrijf wordt gebruikt.

Verificatietypen

Verificatietype	Beschrijving
Enterprise	Gebruik de systeemstandaard voor Enterprise-verificatie als u afzonderlijke accounts en groepen voor BI-platform wilt maken of als u al een hiërarchie van gebruikers en groepen hebt gemaakt op een LDAP-directoryserver of een Windows Active Directory-server.
LDAP	Als u een LDAP-directoryserver installeert, kunt u in het BI-platform bestaande LDAP-gebruikersaccounts en groepen gebruiken. Als u LDAP-accounts toewijst aan het BI-platform, kunnen gebruikers zich met hun LDAP-gebruikersnaam en -wachtwoord aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.
Windows AD	U kunt bestaande Windows AD-gebruikersaccounts en -groepen gebruiken in het BI-platform. Als u Active Directory-accounts toewijst aan het BI-platform, kunnen gebruikers zich met hun Active Directory-gebruikersnaam en -wachtwoord aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.
SAP	U kunt bestaande SAP-functies in BI-platformaccounts importeren. Nadat u SAP-functies hebt toegewezen, kunnen gebruikers zich met hun SAP-referentiegegevens aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.
Oracle EBS	U kunt bestaande Oracle EBS-functies in BI-platformaccounts toewijzen. Nadat u Oracle EBS-functies hebt toegewezen, kunnen gebruikers zich met hun Oracle EBS-referentiegegevens aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.
Siebel	U kunt bestaande Siebel-functies in BI-platformaccounts toewijzen Nadat u Siebel-functies hebt toegewezen, kunnen gebruikers zich met hun Siebel-referentiegegevens aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.
PeopleSoft Enterprise	U kunt bestaande PeopleSoft-functies in BI-platformaccounts toewijzen Nadat u PeopleSoft-functies hebt toegewezen, kunnen gebruikers zich met hun PeopleSoft-referentiegegevens aanmelden bij BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.

Verificatietype	Beschrijving
JD Edwards EnterpriseOne	U kunt bestaande JD Edwards-functies in BI-platformaccounts toewijzen Nadat u JD Edwards-functies hebt toegewezen, kunnen gebruikers zich met hun JD Edwards-referentiegegevens aanmelden bij SAP BI-platformtoepassingen. U hoeft dan geen afzonderlijke gebruikers- en groepsaccounts in het BI-platform te maken.

6.2 Enterprise-accounts en algemene accounts beheren

Omdat Enterprise-verificatie de standaardverificatiemethode is voor het BI-platform, is deze methode standaard ingeschakeld wanneer u het systeem installeert. Wanneer u gebruikers en groepen toevoegt en beheert, slaat het platform de gebruikers- en groepsgegevens op in een database.

> ⓘ Opmerking
>
> Wanneer een gebruiker tijdens een websessie op het BI-platform naar een pagina buiten het platform gaat of de webbrowser sluit, wordt de Enterprise-sessie niet afgemeld en blijft de licentie behouden. De Enterprise-sessie verloopt na ongeveer 24 uur. Als de gebruiker zich bij het platform afmeldt, wordt de Enterprise-sessie beëindigd en is de licentie beschikbaar voor andere gebruikers.

6.2.1 Een gebruikersaccount maken

Wanneer u een nieuwe gebruiker maakt, geeft u de eigenschappen van de gebruiker op en selecteert u de groep of groepen voor de gebruiker.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Klik op *Beheren* > *Nieuw* > *Nieuwe gebruiker*.
   Het dialoogvenster *Nieuwe gebruiker* wordt weergegeven.
3. Een Enterprise-gebruiker maken:
   a. Selecteer in de lijst *Verificatietype* de optie *Enterprise*.
   b. Typ de accountnaam, de volledige naam, het e-mailadres en een beschrijving.

      > → Tip
      >
      > Gebruik het vak Beschrijving als u extra informatie over de gebruiker of account wilt opnemen.

   c. Geef de wachtwoordgegevens en -instellingen op in overeenstemming met de wachtwoordcriteria die zijn gedefinieerd voor Enterprise-verificatie.
4. Selecteer de toepasselijke optie in de lijst *Verificatietype* en typ de accountnaam om een gebruiker te maken die zich aanmeldt met een ander verificatietype.
5. Voer een van de volgende acties uit om de gebruikersaccount aan te wijzen (op basis van uw licentieovereenkomst voor het BI-platform):

- Selecteer *Gelijktijdige gebruiker* als deze gebruiker valt onder een licentieovereenkomst waarin wordt gestipuleerd hoeveel gebruikers gelijktijdig verbonden mogen zijn.
- Selecteer *Op naam* als deze gebruiker valt onder een licentieovereenkomst waarin licenties worden verstrekt aan specifieke gebruikers. Licenties op naam zijn handig voor mensen die altijd toegang tot het BI-platform moeten hebben, ongeacht hoeveel gebruikers verbonden zijn.

> **Opmerking**
>
> Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

6. Klik op *Maken en sluiten*.

   De gebruiker wordt toegevoegd aan het systeem en wordt automatisch toegevoegd aan de groep Iedereen. Er wordt automatisch een Postvak IN voor de gebruiker gemaakt, evenals een Enterprise-alias.

U kunt de gebruiker nu aan een groep toevoegen of rechten opgeven voor de gebruiker.

6.2.2 Een gebruikersaccount wijzigen

Gebruik deze procedure als u de eigenschappen of het groepslidmaatschap van een gebruiker wilt wijzigen.

> **Opmerking**
>
> De wijzigingen worden meteen doorgevoerd als de gebruiker is aangemeld.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker van wie u de eigenschappen wilt wijzigen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven voor de gebruiker.
4. Wijzig de eigenschappen van de gebruiker.

   Naast de opties waarover u kon beschikken toen u de account maakte, kunt u de account nu ook uitschakelen door het selectievakje *Account is uitgeschakeld* in te schakelen.

   > **Opmerking**
   >
   > Wijzigingen die u in de gebruikersaccount aanbrengt, worden pas geactiveerd wanneer de gebruiker zich weer aanmeldt.

5. Klik op *Opslaan en sluiten*.

Verwante informatie

Een nieuwe alias maken voor een bestaande gebruiker [pagina 120]

6.2.3 Een gebruikersaccount verwijderen

Gebruik deze procedure als u een gebruikersaccount wilt verwijderen. Het is mogelijk dat de gebruiker een foutmelding ontvangt wanneer hij of zij is aangemeld op het moment dat de account wordt verwijderd. Wanneer u een gebruikersaccount verwijdert, worden ook de map Favorieten, de persoonlijke categorieën en het Postvak IN voor die gebruiker verwijderd.

Als u denkt dat de gebruiker in de toekomst weer toegang tot de account nodig zal hebben, verwijdert u de account niet, maar schakelt u het selectievakje *Account is uitgeschakeld* in het dialoogvenster *Eigenschappen* van de geselecteerde gebruiker in.

> **Opmerking**
>
> Wanneer u een gebruikersaccount verwijdert, betekent dat niet automatisch dat de gebruiker zich niet meer kan aanmelden bij het BI-platform. Als de gebruikersaccount ook aanwezig is in een extern systeem en als de account behoort tot een externe groep die is toegewezen aan het BI-platform, kan de gebruiker zich mogelijk toch nog aanmelden.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker die u wilt verwijderen.
3. Klik op *Beheren* > *Verwijderen*.

   Het dialoogvenster Verwijderingsbevestiging wordt weergegeven; hierin wordt aangegeven of de geselecteerde gebruiker eigenaar is van een of meer objecten.
4. Klik op *OK*.
   De gebruikersaccount is verwijderd.

Verwante informatie

Een gebruikersaccount wijzigen [pagina 103]
Een alias uitschakelen [pagina 122]

6.2.4 Een nieuwe groep maken

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Klik op *Beheren* > *Nieuw* > *Nieuwe groep*.
   Het dialoogvenster *Nieuwe gebruikersgroep maken* wordt weergegeven.

3. Geef een naam en beschrijving op voor de groep.
4. Klik op *OK*.

Wanneer u een nieuwe groep hebt gemaakt, kunt u gebruikers en subgroepen toevoegen, of een groepslidmaatschap opgeven waardoor de nieuwe groep een subgroep wordt. Omdat u via subgroepen extra niveaus hebt voor het indelen van gebruikers, zijn ze handig voor het instellen van objectrechten waarmee u de toegang van gebruikers tot uw BI-platforminhoud kunt regelen.

6.2.5 De eigenschappen van een groep wijzigen

U kunt de eigenschappen van een groep wijzigen door de bijbehorende instellingen te wijzigen.

> **Opmerking**
>
> De gebruikers die tot de groep behoren, krijgen met de wijziging te maken wanneer ze zich weer aanmelden.

1. Selecteer de groep in het beheergebied *Gebruikers en groepen* van de CMC.
2. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
3. Wijzig de eigenschappen van de groep.

   Klik op de koppelingen in de navigatielijst om naar de divere dialoogvensters te gaan en de gewenste eigenschappen te wijzigen.

   - Als u de naam of de beschrijving van de groep wilt wijzigen, klikt u op *Eigenschappen*.
   - Als u de rechten wilt wijzigen die principals voor de groep hebben, klikt u op *Gebruikersbeveiliging*.
   - Als u profielwaarden van groepsleden wilt wijzigen, klikt u op *Profielwaarden*.
   - Als u de groep als subgroep wilt toevoegen aan een andere groep, klikt u op *Lid van*.
4. Klik op *Opslaan*.

6.2.6 De leden van een groep weergeven

Met deze procedure kunt u gebruikers weergeven die tot een specifieke groep behoren.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Vouw *Groepshiërarchie* uit in de *boomstructuur*.
3. Selecteer de groep in de *boomstructuur*.

   > **Opmerking**
   >
   > Als een groep veel gebruikers bevat of als de groep is gekoppeld aan een externe map, kan het enkele minuten duren voordat de lijst wordt weergegeven.

   De lijst met gebruikers die deel uitmaken van de groep wordt weergegeven.

6.2.7 Subgroepen toevoegen

U kunt een groep toevoegen naar een andere groep. Hierbij wordt de toegevoegde groep een subgroep.

> **Opmerking**
>
> Het toevoegen van een subgroep is vergelijkbaar met het opgeven van een groepslidmaatschap.

1. Selecteer in het beheergebied *Gebruikers en groepen* van de CMC de groep die u als subgroep wilt toevoegen aan een andere groep.
2. Klik op *Acties* > *Toevoegen aan groep*.
   Het dialoogvenster *Join-groep* wordt weergegeven.
3. Verplaats de groep waaraan u de eerste groep wilt toevoegen van de lijst *Beschikbare groepen* naar de lijst *Doelgroep(en)*.
4. Klik op *OK*.

Verwante informatie

Groepslidmaatschap opgeven [pagina 106]

6.2.8 Groepslidmaatschap opgeven

U kunt een groep lid maken van een andere groep. De groep die lid wordt, wordt een subgroep genoemd. De groep waaraan u de subgroep toevoegt, is de bovenliggende groep. Een subgroep neemt de rechten van de bovenliggende groep over.

1. Klik in het beheergebied *Gebruikers en groepen* van de CMC op de groep die u wilt toevoegen aan een andere groep.
2. Klik op *Acties* > *Lid van*.
   Het dialoogvenster *Lid van* wordt weergegeven.
3. Klik op *Join-groep*.
   Het dialoogvenster *Join-groep* wordt weergegeven.
4. Verplaats de groep waaraan u de eerste groep wilt toevoegen van de lijst *Beschikbare groepen* naar de lijst *Doelgroep(en)*.

   De subgroep die u hebt gemaakt, neemt alle rechten van de bovenliggende groep over.
5. Klik op *OK*.
   U gaat terug naar het dialoogvenster *Lid van* en de bovenliggende groep wordt weergegeven in de lijst met bovenliggende groepen.

6.2.9 Een groep verwijderen

Een groep die u niet meer nodig hebt, kunt u verwijderen. De standaardgroepen Administrator en Iedereen kunt u niet verwijderen.

> **Opmerking**
>
> De gebruikers die tot de verwijderde groep behoren, krijgen met de wijziging te maken wanneer ze zich weer aanmelden.

> **Opmerking**
>
> De gebruikers die deel uitmaken van de verwijderde groep, verliezen de rechten die ze eventueel van de groep hebben overgenomen.

Gebruik het beheergebied *Verificatie* in de CMC om externe verificatiegroepen te verwijderen, zoals de groep Windows AD-gebruikers.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de groep die u wilt verwijderen.
3. Klik op *Beheren* > *Verwijderen*.
   In een volgend dialoogvenster moet u de verwijdering bevestigen.
4. Klik op *OK*.
   De groep wordt verwijderd.

6.2.10 Gebruikers of gebruikersgroepen bulksgewijs toevoegen

U kunt een CSV-bestand (Comma-Separated Values) gebruiken om gebruikers of gebruikersgroepen tegelijk aan de CMC toe te voegen. In een goed opgemaakt CSV-bestand worden gegevens door komma's op een regel gescheiden, zoals u kunt zien in het volgende voorbeeld:

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

De volgende voorwaarden zijn van toepassing op bulksgewijs toevoegen:

- Regels in het CSV-bestand met een fout worden weggelaten uit het importproces.
- Na de import zijn gebruikersaccounts in eerste instantie uitgeschakeld.
- U kunt een leeg wachtwoord gebruiken wanneer u een nieuwe gebruiker maakt. U moet echter een geldig wachtwoord voor Enterprise-verificatie gebruiken wanneer u bestaande gebruikers vervolgens bijwerkt.
- Wanneer een databasereferentie aan een account wordt toegevoegd, wordt de referentie in het gebruikersprofiel ingeschakeld.

> **Opmerking**
>
> Alleen gebruikers die lid zijn van de standaardgroep Administrators kunnen gebruikers tegelijk toevoegen. Deze functie wordt niet ondersteund voor gedelegeerde beheerders.

1. Selecteer in het beheergebied *Gebruikers en groepen* van de CMC ▶ *Beheren* ▶ *Importeren* ▶ *Gebruiker/groep/databasereferentie* ▶.

   Nu wordt het dialoogvenster *Gebruiker/groep/databasereferentie voor import* weergegeven.
2. Klik op *Bladeren*, selecteer een CSV-bestand en klik op *Verifiëren*.

   Het bestand wordt verwerkt. Als gegevens goed zijn opgemaakt in het bestand, wordt de knop *Importeren* geactiveerd. Als gegevens niet goed zijn opgemaakt, wordt informatie over de fout weergegeven en moet u het probleem oplossen voordat de CMC het bestand kan verifiëren voor import.
3. Klik op *Importeren*.

De gebruikers of gebruikersgroepen worden in de CMC geïmporteerd.

Als u de gebruikers of gebruikersgroepen wilt bekijken die u hebt toegevoegd, selecteert u ▶ *Beheren* ▶ *Importeren* ▶ *Geschiedenis* ▶ in het beheergebied *Gebruikers en groepen*.

6.2.11 De Guest-account inschakelen

De Guest-account wordt standaard uitgeschakeld, zodat u er zeker van kunt zijn dat niemand zich met deze account bij het BI-platform kan aanmelden. Met deze standaardinstelling schakelt u ook de functie voor eenmalige anonieme aanmelding van het BI-platform uit. Gebruikers hebben dan geen toegang meer tot BI-startpunt zonder een geldige gebruikersnaam en geldig wachtwoord op te geven.

Voer deze taak uit als u de Guest-account wilt inschakelen, zodat gebruikers niet hun eigen accounts hoeven te gebruiken voor toegang tot BI-startpunt.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Klik op *Gebruikerslijst* in het navigatievenster.
3. Selecteer *Gast*.
4. Klik op ▶ *Beheren* ▶ *Eigenschappen* ▶.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
5. Schakel het selectievakje *Account is uitgeschakeld* uit.
6. Klik op *Opslaan en sluiten*.

6.2.12 Gebruikers toevoegen aan groepen

Met gebruikersgroepen kunnen beheerders BI-startpunttaken uitvoeren voor batches met gebruikers (u kunt bijvoorbeeld voorkeuren aanpassen of publicaties voor bepaalde gebruikersgroepen plannen).

U kunt op de volgende manieren gebruikers toevoegen aan groepen:

- Selecteer de groep en klik op ▶ *Acties* ▶ *Leden toevoegen aan groep* ▶.
- Selecteer de gebruiker en klik op ▶ *Acties* ▶ *Lid van* ▶.
- Selecteer de gebruiker en klik op ▶ *Acties* ▶ *Toevoegen aan groep* ▶.

U kunt een gebruiker toevoegen aan meer dan één gebruikersgroep. Als een gebruiker bij twee of meer gebruikersgroepen hoort, geeft het BI-startpunt slechts de voorkeuren weer voor één groep.

Verwante informatie

Groepslidmaatschap opgeven [pagina 106]

6.2.12.1 Een gebruiker toevoegen aan een of meer gebruikersgroepen

U kunt een gebruiker toevoegen aan meer dan één gebruikersgroep. Met BI-startpunt worden echter voor slechts een van de gebruikersgroepen voorkeuren weergegeven.

1. Selecteer de gebruiker om aan een groep toe te voegen in het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer *Acties* > *Join-groep*.

   > **Opmerking**
   >
   > Alle BI-platformgebruikers van het systeem behoren tot de groep Iedereen.

3. Verplaats de groep in het dialoogvenster *Join-groep* om de gebruiker van de lijst *Beschikbare groepen* toe te voegen aan de lijst *Doelgroep(en)*.

   > **Tip**
   >
   > Gebruik `SHIFT`+`muisklik` of `CTRL`+`muisklik` als u meerdere groepen wilt selecteren.

4. Klik op *OK*.

6.2.12.2 Een of meer gebruikers toevoegen aan een gebruikersgroep

U kunt meerdere gebruikers toevoegen aan een gebruikersgroep.

Voorkeuren die zijn ingesteld voor een gebruikersgroep, zijn van toepassing op alle gebruikers in de groep. In BI-startpunt worden voorkeuren voor één gebruikersgroep tegelijkertijd weergegeven.

1. Selecteer de gebruikersgroep in het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer *Acties* > *Leden toevoegen aan groep*.
3. Klik in het dialoogvenster *Toevoegen* op *Gebruikerslijst*.
   De lijst *Beschikbare gebruikers/groepen* wordt vernieuwd, waarna alle gebruikersaccounts in het systeem worden weergegeven.
4. Verplaats een of meer gebruikers naar de groep vanuit de lijst *Beschikbare gebruikers/groepen* naar de lijst *Geselecteerde gebruikers/groepen*.

> → Tip
>
> Gebruik `SHIFT`+`muisklik` of `CTRL`+`muisklik` als u meerdere gebruikers wilt selecteren. Om een bepaalde gebruiker te zoeken, voert u de gebruikersnaam in in het vak *Zoeken*.

> → Tip
>
> Als uw systeem veel gebruikers heeft, klikt u op de knoppen *Vorige* en *Volgende* om in de lijst met gebruikers te navigeren.

5. Klik op *OK*.

6.2.13 Wachtwoordinstellingen wijzigen

In de CMC (Central Management Console) kunt u de wachtwoordinstellingen voor een specifieke gebruiker of voor alle gebruikers in het systeem wijzigen. De beperkingen die hierna worden besproken, zijn alleen van toepassing op Enterprise-accounts. Deze beperkingen zijn dus niet van toepassing op accounts die zijn toegewezen aan een externe gebruikersdatabase (LDAP of Windows Active Directory). U kunt echter meestal wel met het externe systeem zelf soortgelijke beperkingen op de externe accounts toepassen.

6.2.13.1 De wachtwoordinstellingen van gebruikers wijzigen

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker van wie u de wachtwoordinstellingen wilt wijzigen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Schakel de selectievakjes van de wachtwoordinstellingen die u wilt wijzigen, in of uit.

   De beschikbare opties zijn:

   - *Wachtwoord verloopt nooit*
   - *Gebruiker moet wachtwoord bij volgende aanmelding wijzigen*
   - *Gebruiker kan wachtwoord niet wijzigen*
5. Klik op *Opslaan en sluiten*.

> ⓘ Opmerking
>
> Wanneer u het wachtwoord van een gebruiker wijzigt, wordt gebruiker afgemeld van alle bestaande sessies en naar de startpagina geleid om zich opnieuw aan te melden.

6.2.13.2 Algemene wachtwoordinstellingen wijzigen

> **Opmerking**
>
> Inactieve gebruikersaccounts worden niet automatisch gedeactiveerd.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Enterprise*.
   Het dialoogvenster *Enterprise* wordt weergegeven.
3. Schakel het selectievakje in voor elke wachtwoordinstelling die u wilt gebruiken en geef indien nodig een waarde op.

   In de volgende tabel vindt u de minimum- en maximumwaarden voor de instellingen die u kunt configureren:

   Wachtwoordinstellingen

Wachtwoordinstelling	Standaard	Minimum	Aanbevolen maximum
Moet ten minste N tekens bevatten	8 tekens	6 tekens	255 tekens
Mag niet langer zijn dan N tekens, waarbij N is:	255 tekens	13 tekens	255 tekens
Moet wachtwoord elke N dag(en) wijzigen	30 dagen	2 dagen	100 dagen
Mag de laatste N wachtwoorden niet opnieuw gebruiken	3 wachtwoorden	1 wachtwoord	100 wachtwoorden
Moet N minuten wachten voor wachtwoord kan worden gewijzigd	0 minuten	0 minuten	100 minuten
Account uitschakelen na N mislukte aanmeldingspogingen	10 mislukte poging	1 mislukte poging	100 mislukte pogingen
Aantal mislukte aanmeldingspogingen na N minuten op nul stellen	5 minuten	1 minuut	100 minuten
Account na N minuten opnieuw inschakelen	5 minuten	0 minuten	100 minuten

> **Opmerking**
>
> Als u vanaf een eerdere versie van SAP BusinessObjects Business Intelligence-platform een upgrade uitvoert naar een latere versie of tracht een willekeurig type uitbreidingsinstallatie uit te voeren, moet u *Account uitschakelen na N mislukte aanmeldingspogingen* op de standaardwaarde instellen.

> **Opmerking**
>
> De hierboven vermelde regels zijn alleen van toepassing op Enterprise-gebruikers en niet op andere verificatietypen van derden.

4. Klik op *Bijwerken*.

6.2.14 Toegang verlenen aan gebruikers en groepen

U kunt aan gebruikers en groepen beheerderstoegang verlenen tot andere gebruikers en groepen. Beheerdersrechten zijn er onder andere voor: objecten weergeven, bewerken en verwijderen, en objectexemplaren weergeven, verwijderen en onderbreken. U kunt bijvoorbeeld aan de IT-afdeling de toegangsrechten Bewerken en Verwijderen toekennen die nodig zijn om probleemoplossing en systeemonderhoud goed te kunnen uitvoeren.

Verwante informatie

Principals toewijzen aan de ACL van een object [pagina 133]

6.2.15 Toegang verlenen tot het Postvak IN van gebruikers

Wanneer u een gebruiker toevoegt, wordt automatisch een Postvak IN voor die gebruiker gemaakt. Het Postvak IN krijgt dezelfde naam als de gebruiker. Standaard hebben alleen de gebruiker zelf en de beheerder toegangsrechten voor het Postvak IN van een gebruiker.

Verwante informatie

Beveiligingsinstellingen voor objecten beheren in de CMC [pagina 132]

6.2.16 Fiorified-BI-startpuntopties configureren

In de CMC kunnen beheerders Fiorified-BI-startpuntvoorkeuren voor gebruikersgroepen configureren.

> **Opmerking**
>
> Als een gebruiker bij twee of meer gebruikersgroepen hoort, geeft het Fiorified BI-startpunt alleen de voorkeuren weer die voor één groep zijn geconfigureerd.

6.2.16.1 Het aanmeldingsvenster van Fiorified BI-startpunt configureren

In het aanmeldingsvenster van Fiorified BI-startpunt wordt standaard om de gebruikersnaam en het wachtwoord van gebruikers gevraagd. U kunt de gebruikers echter ook vragen naar de CMS-naam en het verificatietype. Als u deze instelling wilt wijzigen, moet u de eigenschappen van het Fiorified BI-startpunt bewerken voor het BOE.war-bestand.

6.2.16.1.1 Het aanmeldingsvenster van Fiorified BI-startpunt configureren

Als u de standaardinstellingen van het Fiorified BI-startpunt wilt wijzigen, moet u aangepaste eigenschappen instellen voor het BOE.war-bestand. Dit bestand wordt geïmplementeerd op de computer die uw webtoepassingsserver host.

1. Ga naar de volgende map in uw installatie van BI-platform:

   `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Maak een nieuw bestand in een teksteditor.
3. Sla het bestand op onder de volgende naam:

   `FioriBI.properties`
4. Als u de verificatieopties wilt opnemen in het aanmeldingsvenster van Fiorified BI-startpunt, voegt u de volgende regel toe:

   ```
   authentication.visible=true
   ```
5. Als u de standaardverificatie wilt wijzigen, voegt u de volgende regel toe:

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

   Vervang `<verificatie>` door een van de volgende opties

Verificatietype	<verificatie> waarde
Enterprise	`secEnterprise`
LDAP	`secLDAP`
Windows AD	`secWinAD`
SAP	`secSAPR3`

6. Als u gebruikers wilt vragen om de CMS-naam in het aanmeldingsvenster van Fiorified BI-startpunt, voegt u de volgende regel toe:

```
cms.visible=true
```

7. Sla het bestand op en sluit het.
8. Start de webtoepassingsserver opnieuw op.

Gebruik WDeploy om het `BOE.war`-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u meer informatie wilt over het gebruik van WDeploy.

6.2.16.2 Fiorified BI-startpuntvoorkeuren voor gebruikersgroepen in de CMC instellen

Beheerders configureren de standaard SAP Fiori-BI-startpuntvoorkeuren voor gebruikersgroepen in de CMC.

Door de beheerder geconfigureerde voorkeuren voor een gebruikersgroep zijn van toepassing op alle gebruikers in de groep. Als een gebruiker bij twee of meer gebruikersgroepen hoort, geeft het Fiorified BI-startpunt alleen de voorkeuren weer die voor één groep zijn geconfigureerd.

Gebruikers kunnen hun eigen voorkeuren configureren in het Fiorified BI-startpunt; de voorkeuren hebben voorrang boven de standaardwaarden. Gebruikers kunnen op elk gewenst moment terugschakelen naar de standaardvoorkeuren. Raadpleeg de sectie *Paginavoorkeuren instellen* in de *Gebruikershandleiding voor Fiorified Business Intelligence-startpunt*.

Als de beheerder echter de standaard-Fiorified-BI-startpuntvoorkeuren in de CMC wijzigt, hebben de standaardwaarden voorrang boven de door de gebruiker gedefinieerde waarden.

6.2.16.2.1 Fiorified BI-startpuntvoorkeuren voor een gebruikersgroep instellen

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer onder *Groepenlijst* de gebruikersgroep waarvoor u de Fiorified BI-startpuntvoorkeuren wilt instellen.
3. Klik met de rechtermuisknop en selecteer *Voorkeuren van BI-startpunt van Fiori*.
4. Schakel het selectievakje *Geen voorkeuren gedefinieerd* uit.
5. U kunt het tabblad *Start* aanpassen via een van de volgende acties om de gewenste startpagina op het tabblad te kiezen:

Optie voor tabblad Start	Actie
Het standaardtabblad Start BI-startpunt van Fiori weergeven	Selecteer *Standaardtabblad Start*

Optie voor tabblad Start	Actie
Een specifiek starttabblad weergeven	Kies *Tabblad Start selecteren* en doe het volgende: 1. Selecteer een landingpage in het veld *Landingpage*. • *Mijn startpagina* • *Planning* • *Postvak IN* • *Mappen* • *Prullenbak* 2. Selecteer in het veld *Documenten weergeven als Tegelweergave (standaard)* of *Lijstweergave*. 3. Selecteer een landingfilter in het veld *Landingfilter*: • *Alles weergeven* • *Mijn documenten* • *Alle categorieën* • *Mijn favorieten* • *Mijn recent bekeken* • *Mijn recent uitgevoerde* U kunt een object kiezen uit *Mijn mappen*, *Openbare mappen*, *Persoonlijke categorieën* en *Bedrijfscategorieën* en dit vervolgens weergeven als standaardlandingpage.
Een specifiek rapport als startpagina weergeven	Selecteer *Rapport selecteren* en klik vervolgens op *Door documenten bladeren* om een document te selecteren uit *Mijn mappen* of *Openbare mappen*.
Een categorie als startpagina weergeven	Kies *Categorie selecteren* en klik vervolgens op *Categorieën doorbladeren* om een categorie te selecteren uit *Persoonlijke categorieën* of *Bedrijfscategorieën*.

6. Selecteer in het veld *Kolommen kiezen om weer te geven op tabblad Documenten* de kolomvoorkeuren:
   - *Type*
   - *Laatst uitgevoerd op*
   - *Exemplaren*
   - *Beschrijving*
   - *Gemaakt door*
   - *Laatste keer bijgewerkt*
   - *Gemaakt op*
   - *Locatie (categorieën)*
   - *Mijn favorieten (startpagina)*
   - *Status (planning)*
   - *Exemplaartijd (planning)*
   - *Pad van map*

> **Opmerking**
>
> De kolommen *Type*, *Beschrijving*, *Laatste keer bijgewerkt*, *Mijn favorieten (startpagina)*, *Status (planning)* en *Exemplaartijd (planning)* zijn standaard geselecteerd. U kunt wijzigen welke kolommen u wilt weergeven.

7. Selecteer *Opslaan en sluiten*.

Om de voorkeuren die door een beheerder zijn gedefinieerd in de interface te kunnen zien, moeten gebruikers zich aanmelden bij het Fiorified BI-startpunt, *Instellingen* > *Accountvoorkeuren* > *Paginavoorkeuren* >, selecteren en *Beheerdersinstellingen gebruiken* inschakelen.

6.2.17 Attributen voor systeemgebruikers beheren

Beheerders van het BI-platform beheren attributen voor systeemgebruikers via het gebied *Beheer van gebruikersattributen* in de CMC (Central Management Console). U kunt attributen beheren en uitbreiden voor de volgende gebruikersdirectory's:

- Enterprise
- SAP
- LDAP
- Windows Active Directory

Wanneer gebruikers uit externe directory's zoals SAP, LDAP en Windows AD worden geïmporteerd, zijn de volgende attributen meestal beschikbaar voor de geïmporteerde gebruikersaccounts:

- Volledige naam
- E-mailadres

Attribuutnamen

Alle gebruikersattributen die aan het systeem worden toegevoegd, moeten de volgende eigenschappen hebben:

- *Naam*
- *Interne naam*

De eigenschap “Naam” is de beschrijvende aanduiding van het attribuut. Deze wordt gebruikt voor queryfilters bij het gebruik van de semantische Universe-laag. Zie voor meer informatie de documentatie bij het Hulpprogramma voor universe-ontwerp. De “Interne naam” wordt gebruikt door ontwikkelaars die met de SDK van het BI-platform werken. Deze eigenschap is een naam die automatisch wordt gegenereerd.

Attribuutnamen mogen niet langer zijn dan 256 tekens en mogen alleen alfanumerieke tekens en onderstrepingstekens bevatten.

> **→ Tip**
>
> Als u ongeldige tekens opgeeft voor het attribuut Naam, genereert het BI-platform geen interne naam. Interne namen die eenmaal aan het systeem zijn toegevoegd, kunnen niet worden gewijzigd.

> Het is daarom raadzaam nauwkeurig geschikte attribuutnamen te kiezen die alfanumerieke tekens en onderstrepingstekens bevatten.

Vereisten voor het uitvouwen van toegewezen gebruikersattributen

Voordat u gebruikersattributen aan het systeem toevoegt, moet u alle relevante verificatie-invoegtoepassingen voor de externe gebruikersdirectory's configureren voor toewijzing en import van gebruikers. Daarnaast moet u bekend zijn met het schema van de externe directory's, in het bijzonder met de namen die voor de doelattributen worden gebruikt.

> ⓘ Opmerking
>
> Voor de verificatie-invoegtoepassing van SAP kunnen alleen attributen uit de BAPIADDR3-structuur worden opgegeven.

Nadat het BI-platform is geconfigureerd voor de toewijzing van de nieuwe gebruikersattributen, worden waarden ingevuld na de volgende geplande vernieuwing. In het beheergebied *Gebruikers en groepen* van de CMC worden alle gebruikersattributen weergegeven.

6.2.18 Prioriteit toekennen aan gebruikersattributen tussen meerdere verificatie-opties

Wanneer u de verificatie-invoegtoepassingen instelt voor SAP, LDAP en AD kunt u voor elke invoegtoepassing de prioriteitsniveaus opgeven in verhouding tot de andere twee. In het LDAP-verificatiegebied kunt u bijvoorbeeld de optie *Prioriteit van AD-attribuutbinding instellen in verhouding tot andere attribuutbindingen* gebruiken om de LDAP-prioriteit in verhouding tot SAP en AD op te geven. De Enterprise-attribuutwaarde heeft standaard prioriteit over alle waarden uit een externe directory. Prioriteiten voor attribuutbinding worden niet voor een specifiek attribuut ingesteld maar op het niveau van de verificatie-invoegtoepassing.

Verwante informatie

De LDAP-host configureren [pagina 270]
SAP-rollen importeren [pagina 340]

6.2.19 Een nieuw gebruikersattribuut toevoegen

Voordat u nieuwe gebruikersattributen aan het BI-platform toevoegt, moet u de verificatie-invoegtoepassing configureren voor de externe directory vanwaaruit u gebruikersaccounts toewijst. Dit is van toepassing op SAP, LDAP en Windows AD. Controleer de optie *Volledige naam, e-mailadres en andere attributen importeren* voor alle vereiste invoegtoepassingen.

> **Opmerking**
>
> U hoeft geen voorlopige taken uit te voeren voordat u attributen voor Enterprise-gebruikersaccounts uitbreidt.

> **Tip**
>
> Als u dezelfde attributen over meerdere invoegtoepassingen wilt uitbreiden, is het raadzaam het toepasselijke prioriteitsniveau voor attribuutbinding in te stellen op basis van de vereisten van uw organisatie.

1. Ga naar het beheergebied *Beheer van gebruikersattributen* van de CMC.
2. Klik op het pictogram *Een nieuw aangepast toegewezen attribuut toevoegen*.
   Het dialoogvenster *Attribuut toevoegen* verschijnt.
3. Geef een naam op voor het nieuwe attribuut in het veld *Naam*.

   Het BI-platform gebruikt nu de opgegeven naam als een beschrijvende naam voor het nieuwe attribuut.

   Wanneer u de beschrijvende naam invoert, wordt het veld *Interne naam* automatisch ingevuld volgens deze indeling: `SI_[Friendlyname]` Terwijl de systeembeheerder een 'beschrijvende attribuutnaam' invoert, genereert het BI-platform automatisch de 'interne' naam.
4. Wijzig indien nodig het veld *Interne naam* met letters, cijfers of onderstrepingstekens.

   > **Tip**
   >
   > Het veld *Interne naam* kan alleen tijdens dit stadium gewijzigd worden. Nadat u het nieuwe attribuut hebt opgeslagen, kunt u deze waarde niet meer wijzigen.

   Is het nieuwe attribuut voor Enterprise-accounts, dan kunt u verdergaan naar stap 8.
5. Geef de toepasselijke optie op voor *Een nieuwe bron toevoegen voor* in de lijst en klik op het pictogram *Toevoegen*. De volgende opties zijn beschikbaar:

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

   Er wordt een tabelrij gemaakt voor de attributen die in attribuutbron zijn opgegeven.
6. Geef in de kolom *Naam van attribuutbron* de naam van het attribuut in de brondirectory op.

   Het BI-platform biedt geen mechanisme waarmee automatisch gecontroleerd kan worden of de opgegeven attribuutnaam bestaat in de externe directory. Zorg ervoor dat de opgegeven naam juist en geldig is.
7. Herhaal stap 5 en 6 als er aanvullende bronnen vereist zijn voor het nieuwe attribuut.
8. Klik op *OK* om het nieuwe attribuut naar het BI-platform op te slaan.
   Naam, Interne naam, Bron en Naam van attribuutbron van het nieuwe attribuut worden in een tabel in het beheergebied *Beheer van gebruikersattributen* van de CMC weergegeven.

Het nieuwe attribuut en de bijbehorende waarde voor elke betrokken gebruikersaccount worden in het beheergebied *Gebruikers en groepen* weergegeven wanneer na de volgende geplande vernieuwing.

Als u meerdere bronnen voor het nieuwe attribuut gebruikt, moet u ervoor zorgen dat voor elke verificatie-invoegtoepassing de juiste prioriteiten voor attribuutbinding zijn opgegeven.

6.2.20 Aangepaste gebruikersattributen bewerken

Gebruik de volgende procedure om gebruikersattributen te bewerken die in het BI-platform zijn gemaakt. U kunt het volgende wijzigen:

- De naam van het attribuut in het BI-platform.

  > ⓘ Opmerking
  >
  > Dit is niet de Interne naam die voor het attribuut wordt gebruikt. Is een attribuut eenmaal gemaakt en aan het BI-platform toegevoegd, dan kan de interne naam niet meer gewijzigd worden. Beheerders die een interne naam willen verwijderen, moeten het bijbehorende attribuut verwijderen.

- De naam van de attribuutbron
- Aanvullende bronnen voor het attribuut

1. Ga naar het beheergebied *Beheer van gebruikersattributen* van de CMC.
2. Selecteer het attribuut dat u wilt bewerken.
3. Klik op het pictogram *Geselecteerd attribuut bewerken*.
   Het dialoogvenster *Bewerken* verschijnt.
4. Wijzig de naam of brongegevens van het attribuut.
5. Klik op *OK* om de wijzigingen op te slaan en naar het BI-platform te verzenden.
   De gewijzigde waarden verschijnen in het beheergebied *Beheer van gebruikersattributen* van de CMC.

De gewijzigde attribuutnaam en waarden worden in het beheergebied *Gebruikers en groepen* weergegeven na de volgende geplande vernieuwing.

6.3 Aliassen beheren

Als een gebruiker meerdere accounts in het BI-platform heeft, kunt u de accounts onderling koppelen met de functie Alias toewijzen. Dit is nuttig wanneer een gebruiker een externe account heeft die is toegewezen aan Enterprise en een Enterprise-account.

Door een alias toe te wijzen aan de gebruiker kan de gebruiker zich aanmelden met een externe gebruikersnaam en een extern wachtwoord of met een Enterprise-gebruikersnaam en -wachtwoord. Met een alias kan een gebruiker zich dus met meer verificatietypen aanmelden.

In de CMC worden de aliasgegevens voor een gebruiker onder in het dialoogvenster *Eigenschappen* weergegeven. Een gebruiker kan een willekeurige combinatie van Enterprise-, LDAP- of Windows AD-aliassen hebben.

6.3.1 Een gebruiker maken en een externe alias toevoegen

Wanneer u een gebruiker maakt en daarbij een ander verificatietype kiest dan Enterprise, wordt de nieuwe gebruiker in het BI-platform gemaakt en wordt automatisch een externe alias voor de gebruiker gemaakt.

> **Opmerking**
>
> Om de externe alias automatisch te kunnen maken moet aan de volgende criteria worden voldaan:
>
> - Het verificatiehulpprogramma moet zijn ingeschakeld in de CMC.
> - De notatie van de accountnaam moet overeenkomen met de vereiste notatie voor het type verificatie.
> - De gebruikersaccount moet bestaan in het externe verificatiehulpprogramma en moet behoren tot een groep die al is toegewezen aan het BI-platform.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Klik op *Beheren* > *Nieuw* > *Nieuwe gebruiker*.
   Het dialoogvenster *Nieuwe gebruiker* wordt weergegeven.
3. Selecteer het verificatietype voor de gebruiker, bijvoorbeeld Windows AD.
4. Typ de externe accountnaam voor de gebruiker, bijvoorbeeld `bsmeets`.
5. Selecteer het type verbinding voor de gebruiker.
6. Klik op *Maken en sluiten*.

   De gebruiker wordt aan het BI-platform toegevoegd en aan de gebruiker wordt een alias toegewezen voor het verificatietype dat u hebt geselecteerd, bijvoorbeeld secWindowsAD:ENTERPRISE:bsmeets. Indien nodig kunt u aliassen toevoegen, toewijzen en opnieuw toewijzen aan gebruikers.

6.3.2 Een nieuwe alias maken voor een bestaande gebruiker

U kunt aliassen maken voor bestaande BI-platformgebruikers. De alias kan een Enterprise-alias zijn of een alias voor een extern verificatiehulpprogramma.

> **Opmerking**
>
> Om de externe alias automatisch te kunnen maken moet aan de volgende criteria worden voldaan:
>
> - Het verificatiehulpprogramma moet zijn ingeschakeld in de CMC.
> - De notatie van de accountnaam moet overeenkomen met de vereiste notatie voor het type verificatie.
> - De gebruikersaccount moet aanwezig zijn in het externe verificatiehulpprogramma en moet behoren tot een groep die is toegewezen aan het platform.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker aan wie u een alias wilt toevoegen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt geopend.
4. Klik op *Nieuwe alias*.
5. Selecteer het gewenste verificatietype.
6. Typ de accountnaam voor de gebruiker.
7. Klik op *Bijwerken*.

   Er wordt een alias gemaakt voor de gebruiker. Wanneer u de gebruiker in de CMC bekijkt, worden ten minste twee aliassen weergegeven: de alias die al aan de gebruiker was toegewezen en de alias die u net hebt gemaakt.

8. Klik op *Opslaan en sluiten* om het dialoogvenster *Eigenschappen* af te sluiten.

6.3.3 Een alias van een andere gebruiker toewijzen

Wanneer u een alias toewijst aan een gebruiker, verplaatst u de externe alias van een andere gebruiker naar de gebruiker die u momenteel weergeeft. Enterprise-aliassen kunt u niet (opnieuw) toewijzen.

> ⓘ Opmerking
>
> Als een gebruiker slechts één alias heeft en u die alias toewijst aan een andere gebruiker, worden de gebruikersaccount en de map Favorieten, de persoonlijke categorieën en het Postvak IN voor die account automatisch verwijderd.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker aan wie u een alias wilt toekennen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Klik op *Alias toewijzen*.
5. Geef de gebruikersaccount op waartoe de alias behoort die u wilt toewijzen en klik op *Nu zoeken*.
6. Verplaats de gewenste alias van de lijst *Beschikbare aliassen* naar de lijst *Aliassen die moeten worden toegevoegd aan* `<gebruikersnaam>`.

   Waarbij `<gebruikersnaam>` de naam is van de gebruiker aan wie u de alias wilt toewijzen.

   > → Tip
   >
   > Als u meerdere aliassen tegelijkertijd wilt selecteren, houdt u de toets `SHIFT` + ⇧ of de toets `CTRL` + ⇧ ingedrukt terwijl u op de gewenste aliassen klikt.

7. Klik op *OK*.

6.3.4 Een alias verwijderen

Wanneer u een alias verwijdert, wordt de alias uit het systeem verwijderd. Als een gebruiker slechts één alias heeft en u die alias verwijdert, worden de gebruikersaccount en de map Favorieten, de persoonlijke categorieën en het Postvak IN voor die account automatisch verwijderd.

> ⓘ Opmerking
>
> Wanneer u de alias van een gebruiker verwijdert, betekent dat niet automatisch dat de gebruiker zich niet meer kan aanmelden bij het BI-platform. Als de gebruikersaccount nog steeds voorkomt in het externe systeem en als de account behoort tot een groep die is toegewezen aan het BI-platform, kan de gebruiker zich toch nog aanmelden bij het BI-platform. Of door het systeem een nieuwe gebruiker wordt gemaakt of de alias aan een bestaande gebruiker wordt toegewezen, hangt af van de bijwerkopties die u voor het verificatiehulpprogramma hebt geselecteerd in het beheergebied *Verificatie* van de CMC.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker van wie u de alias wilt verwijderen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Klik op de knop *Alias verwijderen* naast de alias die u wilt verwijderen.
5. Als u wordt gevraagd om de opdracht te bevestigen, klikt u op *OK*.
   De alias wordt verwijderd.
6. Klik op *Opslaan en sluiten* om het dialoogvenster *Eigenschappen* af te sluiten.

6.3.5 Een alias uitschakelen

U kunt voorkomen dat een gebruiker zich met een bepaalde verificatiemethode bij het BI-platform aanmeldt door de alias van de gebruiker die aan die methode is gekoppeld, uit te schakelen. Als u wilt dat een gebruiker helemaal geen toegang heeft tot het platform, schakelt u alle aliassen voor die gebruiker uit.

> **Opmerking**
>
> Wanneer u een gebruiker uit het systeem verwijdert, betekent dit niet automatisch dat de gebruiker zich niet meer kan aanmelden bij het BI-platform. Als de gebruikersaccount nog steeds voorkomt in het externe systeem en als de account behoort tot een groep die is toegewezen aan het platform, kan de gebruiker zich toch nog aanmelden bij het systeem. Als u er zeker van wilt zijn dat een gebruiker zich niet meer bij het platform kan aanmelden met een bepaalde alias, kunt u de alias het beste uitschakelen.

1. Ga naar het beheergebied *Gebruikers en groepen* van de CMC.
2. Selecteer de gebruiker van wie u de alias wilt uitschakelen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Schakel het selectievakje *Ingeschakeld* uit voor de alias die u wilt uitschakelen.

   Herhaal deze stap voor elke alias die u wilt uitschakelen.
5. Klik op *Opslaan en sluiten*.
   De gebruiker kan zich nu niet meer aanmelden met het verificatietype dat u net hebt uitgeschakeld.

Verwante informatie

Een alias verwijderen [pagina 121]

7 Rechten instellen

7.1 Werking van rechten in BI-platform

Rechten zijn de basiseenheden voor het beheren van gebruikerstoegang tot objecten, gebruikers, toepassingen, servers en andere functies in het BI-platform. Ze spelen een belangrijke rol in de beveiliging van het systeem omdat ze aangeven welke acties gebruikers mogen uitvoeren met objecten. U kunt met rechten niet alleen de toegang tot uw BI-platforminhoud regelen, maar ook gebruikers- en groepsbeheer aan verschillende afdelingen delegeren en uw IT-medewerkers beheerderstoegang geven tot servers en servergroepen.

Een belangrijk punt is dat de rechten worden ingesteld voor objecten, zoals rapporten en mappen, en niet voor de principals (gebruikers en groepen) die toegang hebben tot deze objecten en mappen. Als u bijvoorbeeld een manager toegang wilt geven tot een bepaalde map, voegt u de manager in het gebied *Mappen* toe aan de toegangscontrolelijst (ACL, de lijst van principals die toegang hebben tot een object) voor die map. U kunt de manager geen toegang geven door de rechteninstellingen te definiëren in het gebied *Gebruikers en groepen*. De rechteninstellingen voor de manager in het gebied *Gebruikers en groepen* worden gebruikt om andere principals (zoals gedelegeerde beheerders) toegang te verlenen tot de manager als systeemobject. Op deze manier kunnen principals met hogere beheerrechten andere principals als objecten beheren.

Elk recht voor een object kan toegekend, geweigerd of niet opgegeven zijn. Het beveiligingsmodel van BI-platform is zo ontworpen dat rechten worden geweigerd als ze niet expliciet zijn toegewezen. Bovendien worden rechten ook geweigerd als er tegenstrijdige instellingen zijn (zowel toegewezen als geweigerd) voor een gebruiker of groep. Dankzij dit beveiligingsmodel "op basis van weigeringen" kunnen gebruikers en groepen alleen rechten verkrijgen als deze expliciet worden toegewezen.

Er is een belangrijke uitzondering op deze regel. Als een recht dat expliciet is ingesteld voor een onderliggend object in strijd is met de rechten die van het bovenliggende object zijn overgenomen, worden de overgenomen rechten overschreven door het recht dat voor het onderliggende object is ingesteld. Deze uitzondering is van toepassing op gebruikers die ook lid van groepen zijn. Als een gebruiker beschikt over een expliciet recht dat de groep waartoe de gebruiker behoort is geweigerd, worden de overgenomen rechten overschreven door het expliciete recht van de gebruiker.

Verwante informatie

Rechten-overrides [pagina 127]

7.1.1 Toegangsniveaus

Toegangsniveaus zijn groepen rechten die gebruikers vaak nodig hebben. Met toegangsniveaus kunnen beheerders snel en consistent algemene beveiligingsniveaus instellen in plaats van alle rechten afzonderlijk.

Het BI-platform wordt geleverd met een aantal vooraf gedefinieerde toegangsniveaus. Deze vooraf gedefinieerde toegangsniveaus zijn gebaseerd op een model van toenemende rechten, beginnend bij *Weergeven* en eindigend bij *Volledig beheer*. Elk toegangsniveau bouwt voort op de rechten van het voorgaande niveau.

U kunt toegangsniveaus echter ook aanpassen of zelf definiëren, en zo het beheer en onderhoud van de beveiliging aanzienlijk vergemakkelijken. Stel u een situatie voor waarbij een beheerder twee groepen beheert: salesmanagers en salesmedewerkers. Beide groepen hebben toegang nodig tot vijf rapporten in BI-platformsysteem, maar de salesmanagers moeten meer rechten krijgen dan de salesmedewerkers. De vooraf gedefinieerde toegangsniveaus zijn voor geen van beide groepen geschikt. In plaats van groepen aan elk rapport toe te voegen in de vorm van principals en de rechten op vijf verschillende locaties aan te passen, kan de beheerder twee nieuwe toegangsniveaus maken: Salesmanagers en Salesmedewerkers. De beheerder voegt beide groepen vervolgens aan de rapporten toe als principals en wijst het gewenste toegangsniveau toe aan elke groep. Als de rechten moeten worden gewijzigd, kan de beheerder de toegangsniveaus aanpassen. Aangezien de toegangsniveaus van toepassing zijn op beide groepen en voor alle vijf rapporten, kunnen de rechten die de groepen voor de rapporten hebben snel worden bijgewerkt.

Verwante informatie

Werken met toegangsniveaus [pagina 137]

7.1.2 Geavanceerde instellingen voor rechten

U kunt in de CMC geavanceerde rechten instellen, zodat u de beveiliging van objecten volledig naar wens kunt beheren. Deze geavanceerde rechten bieden u meer flexibiliteit bij het definiëren van objectbeveiliging op granulair niveau.

Gebruik bijvoorbeeld geavanceerde instellingen voor rechten als u de rechten van een principal voor een bepaald object of een groep objecten wilt aanpassen. Met geavanceerde rechten kunt u een gebruiker of groep expliciet rechten weigeren. Deze rechten kunnen dan later niet automatisch worden toegewezen als gevolg van wijzigingen in groepslidmaatschappen of mapbeveiligingsniveaus.

In de volgende tabel ziet u een overzicht van de opties die u kunt kiezen wanneer u geavanceerde rechten instelt.

Opties voor rechten

Pictogram	Opties voor rechten	Beschrijving
	Toegekend	Het recht wordt toegekend aan een principal.
	Geweigerd	Het recht wordt een principal geweigerd.
	Niet opgegeven	Het recht wordt niet opgegeven voor een principal. Rechten die zijn ingesteld op *Niet opgegeven*, worden standaard geweigerd.

Pictogram	Opties voor rechten	Beschrijving
	Toepassen op object	Het recht wordt op het object toegepast. Deze optie komt beschikbaar wanneer u op *Toegekend* of *Geweigerd* klikt.
	Toepassen op subobject	Het recht wordt op subobjecten toegepast. Deze optie komt beschikbaar wanneer u op *Toegekend* of *Geweigerd* klikt.

Verwante informatie

Typespecifieke rechten [pagina 130]

7.1.3 Overname

Als u de toegang tot een object wilt beheren, stelt u rechten van principals voor dat object in. Het is echter ondoenlijk om de expliciete waarde van elk mogelijk recht van elke principal voor elk object in te stellen. Neem bijvoorbeeld een systeem met 100 rechten, 1000 gebruikers en 10.000 objecten; als u voor elk object expliciet rechten zou instellen, zouden in de CMS miljarden rechten moeten worden opgeslagen die bovendien allemaal handmatig zouden moeten worden ingesteld door de beheerder.

Dit probleem wordt opgelost met overnamepatronen. Bij overname van rechten zijn de rechten van gebruikers voor objecten in het systeem afkomstig uit een combinatie van hun lidmaatschap in verschillende groepen en subgroepen, en van objecten die rechten overnemen van bovenliggende mappen en submappen. Deze gebruikers kunnen rechten overnemen op grond van hun groepslidmaatschap, subgroepen kunnen rechten overnemen van bovenliggende groepen, en zowel gebruikers als groepen kunnen rechten overnemen van bovenliggende mappen.

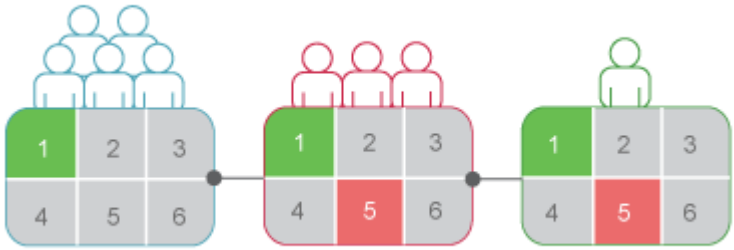
Gebruikers of groepen die rechten voor een map hebben, krijgen standaard dezelfde rechten voor de objecten die vervolgens naar die map worden gepubliceerd. U doet er daarom goed aan eerst op mapniveau de gewenste rechten aan gebruikers en groepen te verlenen en daarna pas objecten naar die map te publiceren.

Het BI-platform ondersteunt twee overnametypen: groepsovername en mapovername.

7.1.3.1 Groepsovername

Bij groepsovername nemen principals de rechten over van de groep waarvan ze lid zijn. Groepsovername is vooral heel handig als u alle gebruikers onderverdeelt in groepen waarin de huidige beveiligingsregels van uw bedrijf worden weerspiegeld.

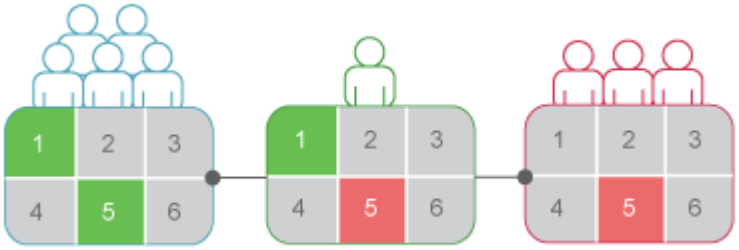
In “Groepsovername, voorbeeld 1” kunt u zien hoe groepsovername werkt. De rode groep is een subgroep van de blauwe groep en neemt dus de rechten van de blauwe groep over. In dit geval wordt recht 1 overgenomen als 'toegekend' en de overige rechten als 'niet opgegeven'. Elk lid van de rode groep neemt deze rechten over. Alle andere rechten die voor de subgroep zijn ingesteld, worden overgenomen door de leden van de subgroep. In dit voorbeeld is de groene gebruiker lid van de rode groep en wordt recht 1 overgenomen als 'toegekend', de rechten 2, 3, 4 en 6 als 'niet opgegeven' en recht 5 als 'geweigerd'.



Groepsovername, voorbeeld 1

Als groepsovername is ingeschakeld voor een gebruiker die lid is van meer dan één groep, worden de rechten van alle bovenliggende groepen betrokken bij de controle van de referenties. De rechten die in een van de bovenliggende groepen zijn geweigerd of niet zijn opgegeven, worden ook geweigerd voor de gebruiker. De gebruiker krijgt dus alleen rechten die in een of meer groepen zijn toegekend (expliciet of via toegangsniveaus) en die nergens expliciet zijn geweigerd.

In “Groepsovername, voorbeeld 2” is de groene gebruiker lid van twee niet-verwante groepen. Deze gebruiker neemt van de blauwe groep de rechten 1 en 5 over als 'toegekend' en de overige rechten als 'niet opgegeven'. Omdat de groene gebruiker echter ook lid is van de rode groep en recht 5 voor de rode groep expliciet is geweigerd, wordt de overname van recht 5 door de groene gebruiker overschreven.



Groepsovername, voorbeeld 2

Verwante informatie

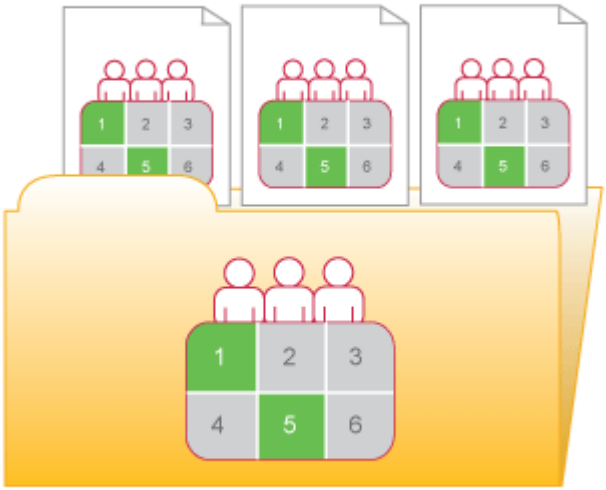
Rechten-overrides [pagina 127]

7.1.3.2 Mapovername

Bij mapovername nemen principals alle rechten over die zijn toegekend aan de bovenliggende map van een object. Mapovername is vooral handig als u BI-platforminhoud structureert in een mappenhiërarchie waarin de huidige beveiligingsregels van uw bedrijf worden weerspiegeld. Stel dat u een map maakt met de naam Verkooprapporten en dat u de groep Verkoop het recht *Weergeven op aanvraag* verleent voor deze map. Elke gebruiker die rechten voor de map Verkooprapporten heeft, krijgt dan standaard dezelfde rechten voor alle

rapporten die u daarna naar deze map publiceert. Hierdoor heeft de groep Verkoop het recht *Weergeven op aanvraag* voor alle rapporten en hoeft u de objectrechten slechts eenmaal in te stellen: op mapniveau.

In "Voorbeeld van mapovername" zijn de rechten van de rode groep ingesteld voor een map. De rechten 1 en 5 zijn toegekend, de overige rechten zijn niet opgegeven. Als mapovername is ingeschakeld, hebben leden van de rode groep dezelfde rechten op objectniveau als de groep op mapniveau. De rechten 1 en 5 zijn toegekend, de overige rechten zijn niet opgegeven.



Voorbeeld van mapovername

Verwante informatie

Rechten-overrides [pagina 127]

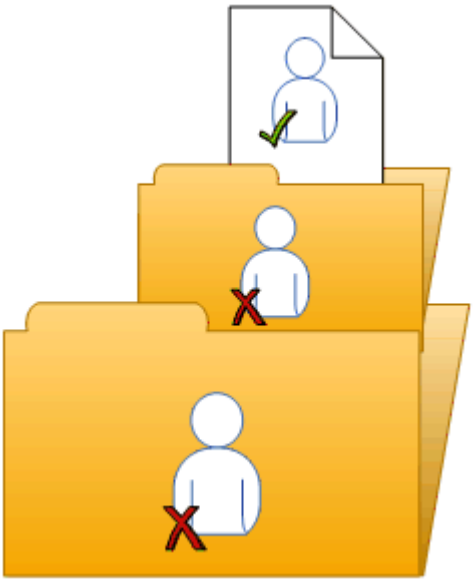
7.1.3.3 Rechten-overrides

Bij rechten-overrides hebben de rechten die zijn ingesteld voor onderliggende objecten prioriteit boven de rechten die zijn ingesteld voor bovenliggende objecten. Rechten-overrides worden in de volgende situaties toegepast:

- In het algemeen prevaleren de rechten die zijn ingesteld voor onderliggende objecten boven de overeenkomende rechten die zijn ingesteld voor bovenliggende objecten.
- In het algemeen prevaleren de rechten die zijn ingesteld voor subgroepen of leden van groepen boven de overeenkomende rechten die zijn ingesteld voor groepen.

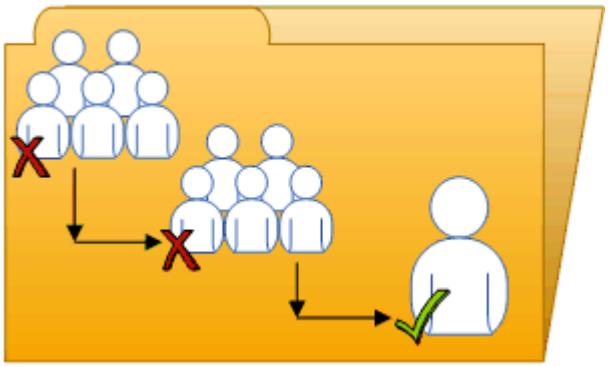
U hoeft overname hoeft niet uit te schakelen bij het instellen van aangepaste rechten voor een object. Onderliggende objecten nemen de rechteninstellingen van bovenliggende objecten over; dit geldt echter niet voor rechten die expliciet voor een onderliggend object zijn ingesteld. Wijzigingen in de rechteninstellingen van een bovenliggend object zijn ook van toepassing op onderliggende objecten.

In “Rechten-overrides, voorbeeld 1” kunt u zien hoe rechten-overrides werken voor bovenliggende en onderliggende objecten. Het recht om de inhoud van een map te bewerken, is de blauwe gebruiker geweigerd; deze rechteninstelling is overgenomen door de submap. Een beheerder heeft de blauwe gebruiker echter het recht *Bewerken*toegekend voor een document in de submap. Het recht *Bewerken* voor het document dat de blauwe gebruiker is toegekend, heeft prioriteit boven de overgenomen rechten die afkomstig zijn van de map en submap.



Rechten-overrides, voorbeeld 1

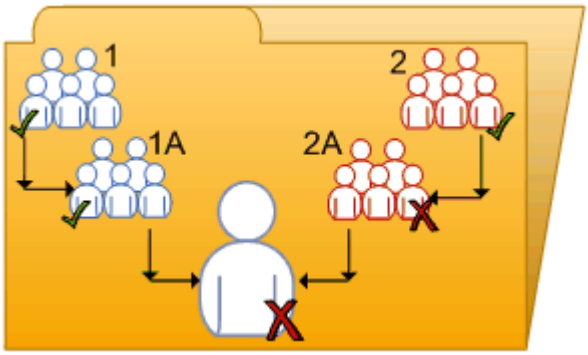
In “Rechten-overrides, voorbeeld 2” kunt u zien hoe rechten-overrides werken voor leden en groepen. Het recht om een map te bewerken, is de blauwe groep geweigerd; deze rechteninstelling is overgenomen door de blauwe subgroep. Een beheerder heeft de blauwe gebruiker, die lid is van de blauwe groep en de blauwe subgroep, echter het recht *Bewerken* toegekend voor de map. Het recht *Bewerken* voor de map dat de blauwe gebruiker is toegekend, prevaleert boven de overgenomen rechten die afkomstig zijn van de blauwe groep en de blauwe subgroep.



Rechten-overrides, voorbeeld 2

In “Complexe rechten-overrides” ziet u een situatie waarin het effect van rechten-override minder duidelijk is. De paarse gebruiker is lid van de subgroepen 1A en 2A, die deel uitmaken van respectievelijk groep 1 en groep 2. Groep 1 en groep 2 beschikken beide over het recht *Bewerken* voor de map. Subgroep 1A neemt het recht *Bewerken* van groep 1 over; het recht *Bewerken* voor subgroep 2A is echter door een beheerder

geweigerd. Vanwege rechten-override hebben de rechteninstellingen voor subgroep 2A prioriteit boven de rechteninstellingen voor groep 2. De paarse gebruiker neemt zodoende tegenstrijdige rechteninstellingen over van subgroep 1A en subgroep 2A. Subgroep 1A en subgroep 2A zijn geen bovenliggende en onderliggende elementen van elkaar, waardoor rechten-override niet van toepassing is. Dit betekent dat de subgroepen dezelfde status hebben en rechten van de ene subgroep geen prioriteit hebben boven die van de andere subgroep. Uiteindelijk krijgt de paarse gebruiker geen *bewerkingsrechten*, omdat het rechtenmodel van het " BI-platform" is gebaseerd op weigeringen.



Complexe rechten-override

Met rechten-override kunt u kleine aanpassingen in de rechteninstellingen van een onderliggend object aanbrengen zonder dat daarbij alle overgenomen rechten worden verwijderd. Stel dat een verkoopmanager vertrouwelijke rapporten in de map Vertrouwelijk wil bekijken. De verkoopmanager maakt deel uit van de groep Verkoop, die geen toegang heeft tot de map en de inhoud hiervan. De beheerder kent aan de manager het recht *Weergeven* toe voor de map Vertrouwelijk en weigert toegang aan de groep Verkoop. In dit geval heeft het recht *Weergeven* dat aan de verkoopmanager is toegekend prioriteit boven de geweigerde toegang die de manager overneemt door het lidmaatschap van de groep Verkoop.

7.1.3.4 Bereik van rechten

Bereik van rechten heeft betrekking op de mogelijkheid om het overnemen van rechten te beheren. Het bereik van een recht definieert u door aan te geven of het recht van toepassing is op het object, de subobjecten of beide. Standaard zijn in een recht de objecten en de subobjecten opgenomen.

Met het bereik van rechten kunt u persoonlijke inhoud in gedeelde locaties veiligstellen. Stel u de situatie voor waarbij een financiële afdeling de gedeelde map Onkostendeclaratie heeft, met daarin submappen voor de individuele onkostendeclaratie van iedere medewerker. De medewerkers moeten toegang krijgen tot de map Onkostendeclaratie en objecten eraan kunnen toevoegen, maar de inhoud van de hun eigen submap moet worden beveiligd. De beheerder geeft alle medewerkers de rechten *Weergeven* en *Toevoegen* voor de map Onkostendeclaratie en beperkt het bereik van deze rechten tot deze map. Dit betekent dat de rechten *Weergeven* en *Toevoegen* niet van toepassing zijn op subobjecten in de map Onkostendeclaratie. De beheerder geeft de medewerkers vervolgens de rechten *Weergeven* en *Toevoegen* voor hun eigen submap.

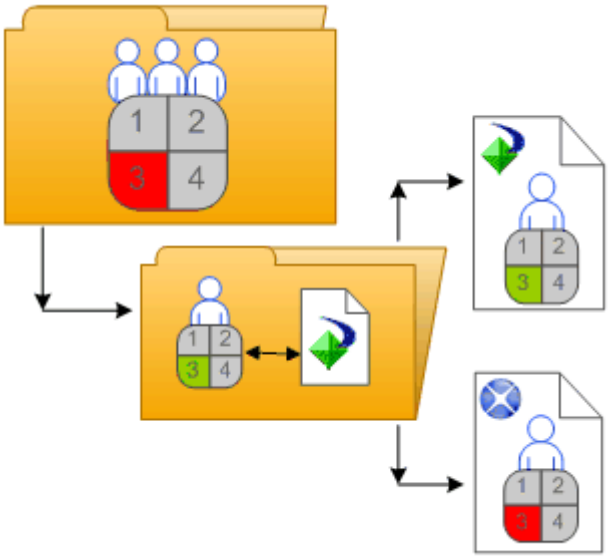
Een rechtenbereik kan ook de effectieve rechten van een gedelegdeerde beheerder beperken. Zo kan een gedelegeerde beheerder bijvoorbeeld de rechten *Rechten veilig wijzigen* en *Bewerken* hebben voor een map, maar is het bereik van deze rechten beperkt tot de map en gelden ze niet voor de subobjecten van de map. Het gevolg is dat de gedelegeerde beheerder deze rechten niet aan een andere gebruiker kan verlenen voor de subobjecten van de map.

7.1.4 Typespecifieke rechten

Typespecifieke rechten hebben uitsluitend betrekking op specifieke objecttypen, zoals Crystal Reports-rapporten, mappen of toegangsniveaus. De volgende rechten zijn typespecifiek:

- Algemene rechten voor het objecttype
  Deze rechten zijn identiek aan algemene globale rechten (bijvoorbeeld het recht om een object toe te voegen, te verwijderen of te bewerken), met het verschil dat u ze instelt op specifieke objecttypen zodat ze de algemene globale rechteninstellingen overschrijven.
- Specifieke rechten voor het objecttype
  Deze rechten zijn uitsluitend beschikbaar voor specifieke objecttypen. Het recht om rapportgegevens te exporteren is bijvoorbeeld beschikbaar voor Crystal Reports-rapporten, maar niet voor Word-documenten.

Het diagram "Voorbeeld van typespecifieke rechten" illustreert de werking van typespecifieke rechten. Recht 3 is hier het recht om een object te bewerken. Aan de blauwe groep is het recht *Bewerken* voor de bovenste map geweigerd en is het recht *Bewerken* toegekend voor Crystal Reports-rapporten in de map en de submap. Dit recht *Bewerken* is specifiek voor Crystal Reports-rapporten en overschrijft de rechteninstellingen op een algemeen globaal niveau. Het resultaat is dat leden van de blauwe groep het recht *Bewerken* hebben voor Crystal Reports-rapporten, maar niet voor het XLF-bestand in de submap.



Voorbeeld van typespecifieke rechten

Met typespecifieke rechten kunt u de rechten van principals beperken op basis van objecttype. Stel dat een beheerder wil instellen dat werknemers objecten aan een map kunnen toevoegen, maar geen submappen kunnen maken. De beheerder kent het recht *Toevoegen* toe op het algemene globale niveau voor de map en weigert vervolgens het recht *Toevoegen* voor het objecttype van de map.

Rechten worden onderscheiden in de volgende verzamelingen, op basis van de objecttypen waarop ze van toepassing zijn:

- *Algemeen*
  Deze rechten zijn van toepassing op alle objecten.
- *Inhoud*

Deze rechten worden onderscheiden aan de hand van bepaalde objecttypen met inhoud. Objecttypen met inhoud zijn bijvoorbeeld Crystal Reports-rapporten en Adobe Acrobat PDF-bestanden.

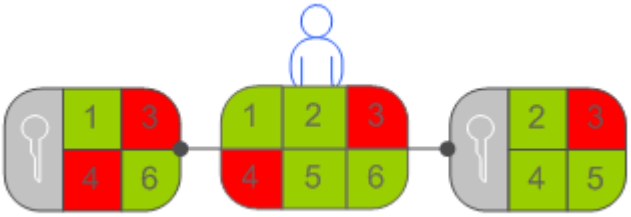
- *Toepassing*
  Deze rechten worden onderscheiden aan de hand van de BI-platformtoepassing waarvoor ze gelden. Toepassingen zijn bijvoorbeeld de CMC en het BI-startpunt.
- *Systeem*
  Deze rechten worden onderscheiden aan de hand van het kernsysteem waarop ze van toepassing zijn. Onderdelen van het kernsysteem zijn bijvoorbeeld agenda's, gebeurtenissen, gebruikers en groepen.

Typespecifieke rechten bevinden zich in de verzameling *Inhoud*, *Toepassing* en *Systeem*. In elke verzameling zijn de typespecifieke rechten op basis van objecttype onderverdeeld in categorieën.

7.1.5 Effectieve rechten bepalen

Houd bij het instellen van rechten voor een object rekening met de volgende zaken:

- Bij elk toegangsniveau worden bepaalde rechten toegekend, bepaalde rechten geweigerd en de overige rechten niet opgegeven. Als bepaalde toegangsniveaus aan een gebruiker worden toegekend, worden de effectieve rechten door het systeem samengevoegd en worden niet-opgegeven rechten standaard geweigerd.
- Als u een principal meerdere toegangsniveaus voor een object toekent, beschikt de principal over de rechten van elk toegangsniveau. Aan de gebruiker in "Meerdere toegangsniveaus" worden twee toegangsniveaus toegekend. Met het ene toegangsniveau krijgt de gebruiker de rechten 3 en 4 en met het andere toegangsniveau alleen recht 3. De effectieve rechten voor de gebruiker zijn dan 3 en 4.



Meerdere toegangsniveaus

- U kunt geavanceerde rechten en toegangsniveaus combineren om zo de rechten aan te passen die een principal voor een object heeft. Als een geavanceerd recht en een toegangsniveau bijvoorbeeld beide expliciet aan een principal worden toegewezen voor een object en het geavanceerde recht conflicteert met een recht in het toegangsniveau, wordt het recht in het toegangsniveau door het geavanceerde recht overschreven.
  Geavanceerde rechten overschrijven het recht in het bijbehorende toegangsniveau alleen als ze worden ingesteld voor hetzelfde object voor dezelfde principal. Een geavanceerd recht Toevoegen dat is ingesteld op het algemene globale niveau kan bijvoorbeeld alleen het algemene recht Toevoegen in een toegangsniveau overschrijven. Een typespecifiek recht Toevoegen in een toegangsniveau kan niet worden overschreven.
  Toegangsniveaus worden echter niet altijd door geavanceerde rechten overschreven. Stel dat een principal het recht *Bewerken* wordt geweigerd voor een bovenliggend object. Voor het onderliggende object krijgt de principal een toegangsniveau waarmee het recht *Bewerken* wel wordt verkregen. Uiteindelijk beschikt de principal over het recht *Bewerken* voor het onderliggende object, omdat de rechten voor het bovenliggende object worden overschreven door de rechten voor het onderliggende object.

- Rechten overschrijven maakt het mogelijk dat rechten die zijn overgenomen van een bovenliggend object, worden overschreven door rechten die zijn ingesteld voor een onderliggend object.

7.2 Beveiligingsinstellingen voor objecten beheren in de CMC

U kunt beveiligingsinstellingen voor de meeste objecten in de CMC beheren met de beveiligingsopties in het menu *Beheren*. Met deze opties kunt u principals toewijzen aan de ACL van een object, de rechten van een principal weergeven en de rechten wijzigen die een principal voor een object heeft.

De specifieke details van het beveiligingsbeheer variëren afhankelijk van uw beveiligingsbehoeften en het type object waarvoor u rechten instelt. In het algemeen worden de volgende taken echter grotendeels op dezelfde manier uitgevoerd:

- De rechten weergeven die een principal voor een object heeft.
- Principals toewijzen aan de ACL van een object en de rechten en toegangsniveaus van deze principals opgeven.
- Rechten voor een map op het bovenste niveau instellen in het BI-platform.

7.2.1 De rechten van een principal voor een object weergeven

In het algemeen gaat u als volgt te werk om de rechten weer te geven die een principal voor een object heeft.

1. Selecteer het object waarvan u de beveiligingsinstellingen wilt weergeven.
2. Klik op *Beheren* > *Gebruikersbeveiliging*.
   Het dialoogvenster *Gebruikersbeveiliging* wordt weergegeven, met daarin de ACL van het object.
3. Selecteer de principal in de ACL en klik op *Beveiliging weergeven*

   De *Machtigingenverkenner* wordt gestart en er wordt een overzicht weergegeven van de effectieve rechten die de principal voor het object heeft. Bovendien kunt u in de *Machtigingenverkenner* het volgende doen:

   - Bladeren naar een andere principal waarvan u de rechten wilt weergeven.
   - De rechten filteren die op basis van de volgende criteria worden weergegeven:

     Toegewezen rechten
     Verleende rechten
     Niet-toegewezen rechten
     Van toegangsniveau
     Objecttype
     De naam van het recht
   - De lijst met rechten in oplopende of aflopende volgorde sorteren op basis van de volgende criteria:

     Verzameling
     Type
     De naam van het recht

De status van het recht (verleend, geweigerd of niet opgegeven)

Daarnaast kunt u op een van de koppelingen in de kolom *Bron* klikken om de bron van de overgenomen rechten weer te geven.

7.2.2 Principals toewijzen aan de ACL van een object

In een ACL (Access Control List) staan de gebruikers aan wie rechten voor een object zijn toegekend of geweigerd. In het algemeen gaat u als volgt te werk om een principal toe te wijzen aan een ACL en de rechten op te geven die de principal voor het object heeft.

1. Selecteer het object waaraan u een principal wilt toevoegen.
2. Klik op *Beheren* > *Gebruikersbeveiliging*.
   Het dialoogvenster *Gebruikersbeveiliging* wordt weergegeven, met daarin de ACL.
3. Klik op *Principals toevoegen*.
   Het dialoogvenster *Principals toevoegen* wordt weergegeven.
4. Verplaats de gebruikers en groepen die u als principals wilt toevoegen van de lijst *Beschikbare gebruikers/groepen* naar de lijst *Geselecteerde gebruikers/groepen*.
5. Klik op *Beveiliging toevoegen en toewijzen*.
6. Selecteer de toegangsniveaus die u de principal wilt toekennen.
7. Geef aan of u map- of groepsovername wilt in- of uitschakelen.

U kunt zo nodig ook rechten wijzigen op granulair niveau om bepaalde rechten van een toegangsniveau te overschrijven.

Verwante informatie

De beveiliging van een object wijzigen voor een principal [pagina 133]

7.2.3 De beveiliging van een object wijzigen voor een principal

Over het algemeen wordt u aangeraden toegangsniveaus te gebruiken waarmee u rechten kunt toewijzen aan een principal. Mogelijk moet u echter soms bepaalde granulaire rechten voor een toegangsniveau overschrijven. Met geavanceerde rechten kunt u de rechten van een principal aanpassen, boven op de toegangsniveaus die de principal al heeft. In het algemeen gaat u als volgt te werk om geavanceerde rechten voor een object toe te kennen aan een principal.

1. Wijs de principal toe aan de ACL van het object.
2. Wanneer de principal is toegevoegd, gaat u naar *Beheren* > *Gebruikersbeveiliging* om de ACL voor het object weer te geven.
3. Selecteer de principal in de ACL en klik op *Beveiliging toewijzen*.

Het dialoogvenster *Beveiliging toewijzen* wordt weergegeven.

4. Klik op het tabblad *Geavanceerd*.
5. Klik op *Rechten toevoegen/verwijderen*.
6. Wijzig de rechten van de principal.

   Alle beschikbare rechten worden samengevat in de *Rechtenbijlage*

Verwante informatie

Principals toewijzen aan de ACL van een object [pagina 133]

7.2.4 Rechten voor een map op het bovenste niveau instellen in het BI-platform

In het algemeen gaat u als volgt te werk om rechten in te stellen voor een map op het bovenste niveau in het BI-platform.

> **Opmerking**
>
> In deze versie hebben principals het recht *Weergeven* voor een containermap nodig om in deze map te navigeren en de subobjecten weer te geven. Dit houdt in dat principals het recht *Weergeven* voor de map op het hoogste niveau nodig hebben om de objecten in mappen weer te geven. Als u het recht *Weergeven* voor een principal wilt beperken, kunt u aan een principal het recht *Weergeven* toekennen voor een bepaalde map en het rechtenbereik alleen op deze map toepassen.

1. Ga naar het gebied in de CMC waarin de map op het bovenste niveau bevindt waarvoor u rechten wilt instellen.
2. Klik op *Beheren* > *Beveiliging op hoogste niveau* > *Alle* `<objecten>`.

   Hier geeft `<objecten>` de inhoud weer van de map op het hoogste niveau. Als u wordt gevraagd om de opdracht te bevestigen, klikt u op *OK*.

   Het dialoogvenster *Gebruikersbeveiliging* wordt weergegeven, met daarin de ACL van de map op het bovenste niveau.
3. Wijs de principal toe aan de ACL van de map op het bovenste niveau.
4. Wijs zo nodig geavanceerde rechten toe aan de principal.

Verwante informatie

Principals toewijzen aan de ACL van een object [pagina 133]
De beveiliging van een object wijzigen voor een principal [pagina 133]

7.2.5 Beveiligingsinstellingen voor een principal controleren.

In bepaalde gevallen wilt u mogelijk weten voor welke objecten een principal al dan niet toegang heeft. U kunt hiervoor een beveiligingsquery uitvoeren. Met behulp van een beveiligingsquery kunt u gebruikersrechten beheren en vaststellen welke rechten een principal heeft voor welke objecten. Geef voor elke beveiligingsquery de volgende gegevens op:

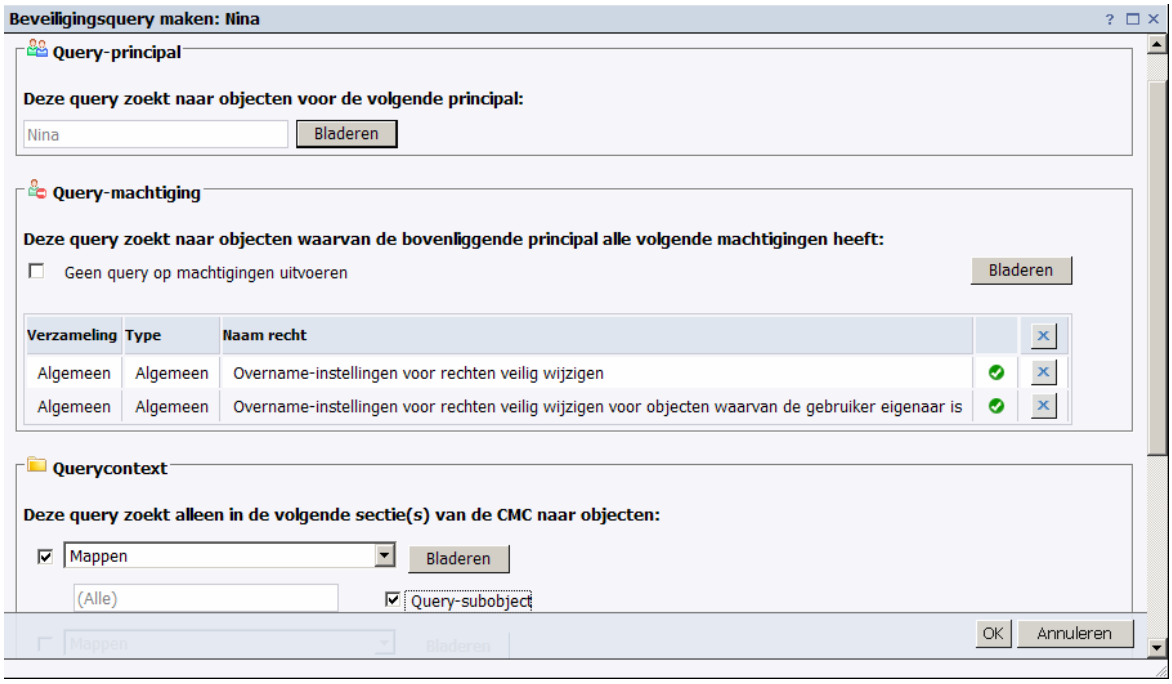
- Queryprincipal
  Geef de gebruiker of groep op waarvoor u de beveiligingsquery wilt uitvoeren. U kunt één principal per beveiligingsquery opgeven.
- Querymachtiging
  Geef de rechten op waarvoor u de beveiligingsquery wilt uitvoeren, de status van deze rechten en het objecttype waarvoor deze rechten zijn ingesteld. U kunt bijvoorbeeld een beveiligingsquery uitvoeren voor alle rapporten die door een principal kunnen worden vernieuwd of voor alle rapporten die niet door een gebruiker kunnen worden geëxporteerd.
- Querycontext
  Geef de CMC-gebieden op waarop de beveiligingsquery moet worden uitgevoerd. U kunt voor elk gebied aangeven of er subobjecten in de beveiligingsquery moeten worden opgenomen. Een beveiligingsquery kan in maximaal vier gebieden worden uitgevoerd.

Het resultaat van een beveiligingsquery wordt in de *structuurweergave* onder *Beveiligingsquery's* weergegeven in het gebied *Queryresultaten*. U kunt een beveiligingsquery verfijnen door een tweede query uit te voeren op de resultaten van de eerste query.

Beveiligingsquery's zijn handig om te achterhalen voor welke objecten een principal bepaalde rechten heeft en als u de rechten wilt aanpassen, worden bovendien de locaties van de objecten weergegeven. Neem nu een situatie waarbij een salesmedewerker wordt benoemd tot salesmanager. De salesmanager heeft *planning*srechten nodig voor Crystal Reports-rapporten waartoe hij voorheen alleen *weergave*rechten had. De rapporten bevinden zich in verschillende mappen. De beheerder voert op alle mappen een beveiligingsquery uit om te achterhalen voor welke Crystal Reports-rapporten de nieuwe salesmanager weergaverechten heeft en neemt daarbij ook subobjecten in de query op. Wanneer de beveiligingsquery is voltooid, krijgt de beheerder in het gebied *Queryresultaten* alle Crystal Reports-rapporten te zien waarvoor de salesmanager *weergave*rechten heeft. In het venster *Details* wordt de locatie van elk Crystal Reports-rapport weergegeven, waardoor de beheerder naar elk rapport kan gaan om de rechten van de salesmanager voor dat rapport te wijzigen.

7.2.5.1 Een beveiligingsquery uitvoeren

1. Selecteer de gebruiker of groep waarvoor u een beveiligingsquery wilt uitvoeren in het gebied *Gebruikers en groepen* van het venster *Details*.
2. Klik op *Beheren* > *Extra* > *Beveiligingsquery maken*.



Het dialoogvenster *Beveiligingsquery maken* wordt weergegeven.

3. Controleer of de principal in het gebied *Query-principal* correct is.

   Als u een beveiligingsquery voor een andere principal wilt uitvoeren, klikt u op *Bladeren* om een andere principal te selecteren. Vouw *Gebruikerslijst* of *Groepenlijst* in het dialoogvenster *Bladeren naar query-principal* uit om naar de principal te bladeren of geef de naam van de gewenste principal op. Als u gereed bent, klikt u op *OK* om terug te gaan naar het dialoogvenster *Beveiligingsquery maken*.

4. Geef in het gebied *Querymachtiging* de rechten op plus de status van elk recht waarvoor u de query wilt uitvoeren.

   - Als u een query wilt uitvoeren voor specifieke rechten die een principal heeft voor objecten, klikt u op *Bladeren*, stelt u de status van elk recht waarvoor u de beveiligingsquery wilt uitvoeren in en klikt u op *OK*.

     > → Tip
     >
     > U kunt specifieke rechten uit de query verwijderen door op de verwijderknop naast het recht te klikken of alle rechten uit de query verwijderen door op de verwijderknop in de koprij te klikken.

   - Als u een algemene beveiligingsquery wilt uitvoeren, schakelt u het selectievakje *Geen query op machtigingen uitvoeren* in.
     Wanneer u dit doet, voert het BI-platform een algemene beveiligingsquery uit voor alle objecten die de principal in zijn/haar toegangscontrolelijst heeft, ongeacht de machtigingen die de principal voor de objecten heeft.

5. Geef in het gebied *Querycontext* de CMC-gebieden op waarop u een query wilt uitvoeren.

   a. Schakel het selectievak naast een lijst in.

   b. Selecteer in de lijst een CMC-gebied waarop u een query wilt uitvoeren.

      Als u een query wilt uitvoeren op een specifiekere locatie binnen een gebied (bijvoorbeeld een bepaalde map in Mappen), klikt u op *Bladeren* om het dialoogvenster *Bladeren naar querycontext* te openen. Klik in het venster *Details* op de map waarop u de query wilt uitvoeren en klik op *OK*. Wanneer

u teruggaat naar het dialoogvenster *Beveiligingsquery*, wordt de map die u hebt opgegeven in het vak onder de lijst weergegeven.

c. Selecteer *Query-subobject*.

d. Herhaal de stappen hierboven voor elk CMC-gebied waarop u een query wilt uitvoeren.

> ⓘ Opmerking
>
> u kunt query's uitvoeren op maximaal vier gebieden.

6. Klik op *OK*.
   De beveiligingsquery wordt uitgevoerd en u gaat naar het gebied *Queryresultaten*.
7. Als u het queryresultaat wilt weergeven, vouwt u *Beveiligingsquery's* in de *boomstructuur* uit en klikt u op het gewenste queryresultaat.

   > → Tip
   >
   > Het queryresultaat wordt aan de hand van de principalnamen weergegeven.

   De queryresultaten worden weergegeven in het venster *Details*.

In het gebied *Queryresultaten* worden alle resultaten van de beveiligingsquery van één gebruiker bewaard totdat de gebruiker zich afmeldt. Als u de query opnieuw wilt uitvoeren met andere specificaties, klikt u op *Acties* > *Query bewerken*. U kunt ook dezelfde query opnieuw uitvoeren door de query te selecteren en te klikken op *Acties* > *Query opnieuw uitvoeren*. Wilt u de resultaten van de beveiligingsquery bewaren, dan klikt u op *Acties* > *Exporteren* om de resultaten van de beveiligingsquery te exporteren als CSV-bestand.

7.3 Werken met toegangsniveaus

U kunt toegangsniveaus voor het volgende gebruiken:

- Een bestaand toegangsniveau kopiëren, aanpassingen aanbrengen in de kopie, deze een andere naam geven en opslaan als een nieuw toegangsniveau.
- Toegangsniveaus maken, een andere naam geven en verwijderen.
- De rechten in een toegangsniveau wijzigen.
- De relatie tussen toegangsniveaus en andere objecten in het systeem traceren.
- Toegangsniveaus herhalen en beheren op meerdere sites.
- Een van de vooraf gedefinieerde toegangsniveaus in het BI-platform gebruiken om rechten snel en uniform aan vele principals toe te wijzen.

In de volgende tabel ziet u een overzicht van de rechten in elk vooraf gedefinieerd toegangsniveau.

Voorgedefinieerde toegangsniveaus

Toegangsniveau	Beschrijving	Rechten
Weergeven	Indien ingesteld op mapniveau kan een principal de map, de objecten in de map en alle exemplaren van elk object weergeven. Indien ingesteld op objectniveau kan een principal het object, de geschiedenis van het object en alle exemplaren van elk object weergeven.	• Objecten weergeven • Documentexemplaren weergeven
Planning	Een principal kan exemplaren maken door eenmaal of regelmatig de uitvoering van een object in een opgegeven gegevensbron te plannen. De principal kan de planning van eigen exemplaren weergeven, verwijderen en onderbreken. De principal kan ook exemplaren plannen voor verschillende indelingen en doelen, parameters en databaseaanmeldingsgegevens instellen, servers voor het verwerken van taken selecteren, inhoud aan de map toevoegen, en het object of de map kopiëren.	Toegangsniveau *Weergeven* plus: • Het uit te voeren document plannen • Servergroepen definiëren voor het verwerken van taken • Objecten kopiëren naar een andere map • Plannen naar doelen • De gegevens van het rapport afdrukken • De gegevens van het rapport exporteren. • Objecten bewerken die het eigendom zijn van de gebruiker • Exemplaren verwijderen die het eigendom zijn van de gebruiker • Documentexemplaren onderbreken en hervatten die het eigendom zijn van de gebruiker
Weergeven op aanvraag	Een principal kan gegevens op verzoek vernieuwen in een gegevensbron.	Toegangsniveau *Planning* plus: • De gegevens van het rapport vernieuwen.
Volledig beheer	Een principal heeft het toegangsniveau Volledig beheer voor het object.	Alle beschikbare rechten, inclusief: • Objecten toevoegen aan de map • Objecten bewerken. • De rechten wijzigen die gebruikers hebben voor objecten • Objecten verwijderen • Exemplaren verwijderen

In de volgende tabel ziet u een overzicht van de rechten die vereist zijn om bepaalde taken op toegangsniveaus te kunnen uitvoeren.

Taak in toegangsniveau	Vereiste rechten
Een toegangsniveau maken.	Het recht *Toevoegen* voor de *toegangsniveau*map op het hoogste niveau.
Granulaire rechten in een toegangsniveau weergeven.	Het recht *Weergeven* voor het toegangsniveau.

Taak in toegangsniveau	Vereiste rechten
Een toegangsniveau voor een object toewijzen aan een principal.	Het recht *Weergeven* voor het toegangsniveau. Het recht *Toegangsniveau voor beveiligingstoewijzing gebruiken* voor het toegangsniveau Het recht *Rechten wijzigen* voor het object of het recht *Rechten veilig wijzigen* voor het object en de principal **Opmerking** aan gebruikers met het recht *Rechten veilig wijzigen* die een toegangsniveau willen toewijzen aan een principal, moet hetzelfde toegangsniveau zijn toegewezen.
Een toegangsniveau wijzigen.	De rechten *Weergeven* en *Bewerken* voor het toegangsniveau.
Een toegangsniveau verwijderen.	De rechten *Weergeven* en *Verwijderen* voor het toegangsniveau.
Een toegangsniveau kopiëren.	Het recht *Weergeven* voor het toegangsniveau. Het recht *Kopiëren* voor het toegangsniveau. Het recht *Toevoegen* voor de *toegangsniveau*map op het hoogste niveau.

7.3.1 Kiezen tussen het toegangsniveau *Weergeven* en *Weergeven op aanvraag*

Als u rapportages via het web verzorgt, is de keuze tussen het gebruik van live of opgeslagen gegevens een van de belangrijkste beslissingen die u moet nemen. Ongeacht de keuze die u maakt, wordt de eerste pagina zo snel mogelijk door het BI-platform weergegeven, zodat u het rapport kunt bekijken terwijl de resterende gegevens worden verwerkt. In deze sectie wordt het verschil tussen twee vooraf gedefinieerde toegangsniveaus beschreven.

Het toegangsniveau *Weergeven op aanvraag*

Met rapporten op aanvraag hebben gebruikers real-time toegang tot actuele gegevens, rechtstreeks van de databaseserver. Met live gegevens zijn gebruikers voortdurend op de hoogte van alle gegevenswijzigingen en kunnen ze gegevens opvragen die tot op de seconde nauwkeurig zijn. Als managers van een groot distributiecentrum bijvoorbeeld voorraad moeten bijhouden die in continudiensten wordt verzonden, beschikken ze met live rapportage over alle gewenste informatie.

Voordat u echter actuele gegevens voor al uw rapporten gaat verzorgen, moet u bedenken of u alle gebruikers continu toegang tot de database wilt geven. Als gegevens niet snel of voortdurend worden gewijzigd, leiden de talloze aanvragen aan de database alleen maar tot toegenomen netwerkverkeer en overmatig gebruik van serverbronnen. U kunt de rapporten dan beter op terugkerende basis plannen, zodat gebruikers altijd recente gegevens kunnen bekijken (rapportexemplaren) zonder de databaseserver te belasten.

Gebruikers hebben het toegangsniveau *Weergeven op aanvraag* nodig voor het vernieuwen van rapporten in de database.

Het toegangsniveau *Weergeven*

Om het netwerkverkeer en het aantal toegangspogingen voor de databaseservers te beperken kunt u rapporten plannen, zodat deze op bepaalde tijdstippen worden uitgevoerd. Wanneer het rapport is uitgevoerd, kunnen gebruikers het desbetreffende rapportexemplaar weergeven wanneer dat nodig is, zonder de database opnieuw te belasten.

Als de benodigde gegevens niet steeds veranderen, kunt u het beste werken met rapportexemplaren. Voor het navigeren door rapportexemplaren of het uitvoeren van een analyse op lager niveau op kolommen of diagrammen is geen directe toegang tot de database nodig. Hiertoe is toegang tot opgeslagen gegevens voldoende. Het gebruik van rapporten met opgeslagen gegevens zorgt dus voor een beperkte gegevensoverdracht via het netwerk en verkleint bovendien de belasting van de databaseserver.

Als de verkoopdatabase bijvoorbeeld eenmaal per dag wordt bijgewerkt, kunt u het rapport ook een keer per dag uitvoeren. Verkopers hebben dan altijd toegang tot actuele verkoopgegevens, maar ze halen die niet steeds op uit de database.

Gebruikers hebben het recht *Weergeven* nodig om rapportexemplaren weer te geven.

7.3.2 Een bestaand toegangsniveau kopiëren

Dit is de beste manier om een toegangsniveau te maken als u een toegangsniveau wilt dat enigszins afwijkt van een bestaand toegangsniveau.

1. Ga naar het gebied *Toegangsniveaus*.
2. Selecteer een toegangsniveau in het venster *Details*.

   > → Tip
   >
   > Selecteer een toegangsniveau met rechten die in grote lijnen overeenkomen met de rechten die u voor het nieuwe toegangsniveau wilt.

3. Klik op *Ordenen* > *Kopiëren*.
   Een kopie van het toegangsniveau dat u hebt geselecteerd, wordt weergegeven in het venster *Details*.

7.3.3 Een nieuw toegangsniveau maken

Dit is de beste manier om een toegangsniveau te maken als u een toegangsniveau wilt dat flink afwijkt van een bestaand toegangsniveau.

1. Ga naar het gebied *Toegangsniveaus*.
2. Klik op *Beheren* > *Nieuw* > *Toegangsniveau maken*.

Het dialoogvenster *Een nieuw toegangsniveau maken* wordt weergegeven.

3. Geef een naam en een beschrijving voor het nieuwe toegangsniveau op en klik op *OK*.
   U gaat terug naar het gebied *Toegangsniveau* en het nieuwe toegangsniveau wordt in het venster *Details* weergegeven.

7.3.4 De naam van een toegangsniveau wijzigen

1. Selecteer het toegangsniveau waarvan u de naam wilt wijzigen in het gebied *Toegangsniveaus* van het venster *Details*.
2. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
3. Geef in het veld *Titel* een nieuwe naam op voor het toegangsniveau en klik op *Opslaan en sluiten*.
   U gaat terug naar het gebied *Toegangsniveaus*.

7.3.5 Een toegangsniveau verwijderen

1. Selecteer het toegangsniveau dat u wilt verwijderen in het gebied *Toegangsniveaus* van het venster *Details*.
2. Klik op *Beheren* > *Toegangsniveau verwijderen*.

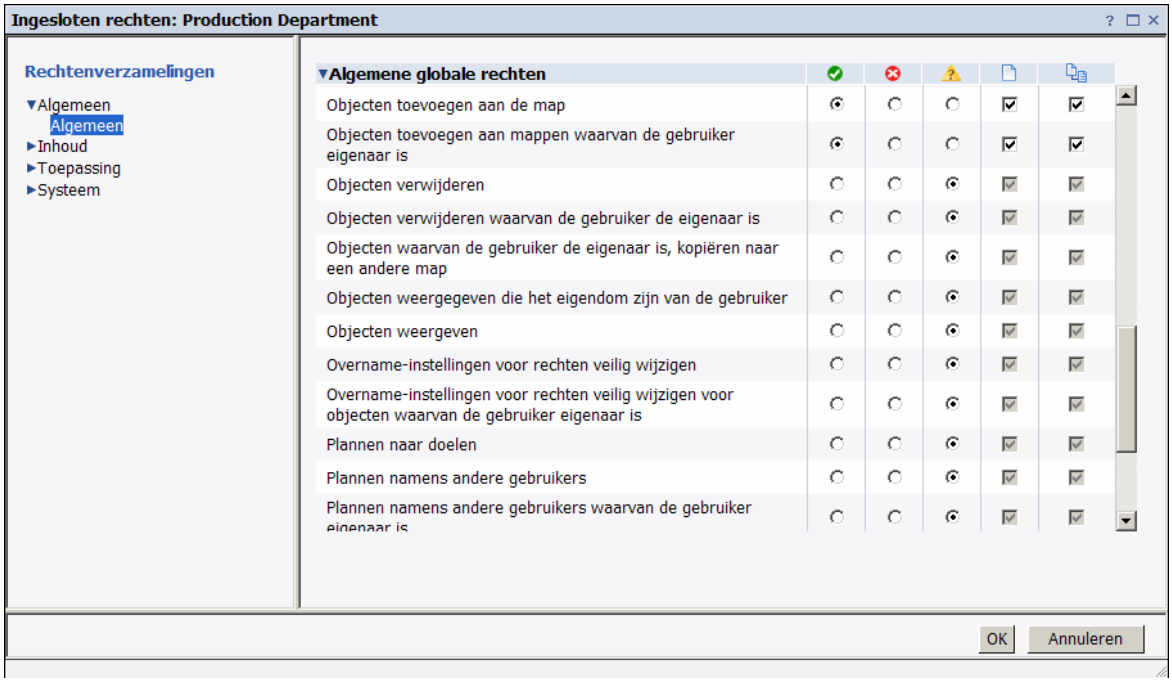
   > **Opmerking**
   >
   > Vooraf gedefinieerde toegangsniveaus kunnen niet worden verwijderd.

   Er wordt een dialoogvenster weergegeven met informatie over de objecten waarop dit toegangsniveau invloed heeft. Als u het toegangsniveau niet wilt verwijderen, klikt u op *Annuleren* om het dialoogvenster te sluiten.
3. Klik op *Verwijderen*.
   Het toegangsniveau wordt verwijderd en u gaat terug naar het gebied *Toegangsniveaus*.

7.3.6 De rechten in een toegangsniveau wijzigen

Als u rechten wilt instellen voor een toegangsniveau, geeft u eerst algemene globale rechten op voor alle objecten (ongeacht het type) en geeft u vervolgens aan wanneer u de algemene instellingen op basis van het specifieke objecttype wilt overschrijven.

1. Selecteer het toegangsniveau waarvan u de rechten wilt wijzigen in het gebied *Toegangsniveaus* van het venster *Details*.
2. Klik op *Acties* > *Ingesloten rechten*.
   Het dialoogvenster *Ingesloten rechten* wordt weergegeven, met daarin een overzicht van effectieve rechten.
3. Klik op *Rechten toevoegen/verwijderen*.



In het dialoogvenster *Ingesloten rechten* worden de rechtenverzamelingen voor het toegangsniveau weergegeven in de navigatielijst. De sectie *Algemene globale rechten* wordt standaard uitgevouwen.

4. Stel de algemene globale rechten in.

   Elk recht kan de status *Toegekend*, *Geweigerd* of *Niet opgegeven* hebben. U kunt ook aangeven of u het recht alleen op het object wilt toepassen, alleen op de subobjecten of beide.

5. Als u typespecifieke rechten voor het toegangsniveau wilt instellen, klikt u in de navigatielijst op de rechtenverzameling en klikt u op de subverzameling die van toepassing is op het objecttype waarvoor u de rechten wilt instellen.

6. Als u gereed bent, klikt u op *OK*.
   U keert terug naar de lijst met effectieve rechten.

7.3.7 De relatie tussen toegangsniveaus en objecten traceren

Voordat u een toegangsniveau wijzigt of verwijdert, is het belangrijk om na te gaan of wijzigingen die u aanbrengt geen negatieve invloed zullen hebben op de objecten in de CMC. U doet dit door een relatiequery op het toegangsniveau uit te voeren

Met relatiequery's worden objecten die door een toegangsniveau worden beïnvloed, op één plek geretourneerd. Deze query's zijn daarom handig bij het beheren van rechten. Neem nu de situatie waarbij een bedrijf haar structuur reorganiseert en twee afdelingen samenvoegt: afdeling A en afdeling B worden samen afdeling C. De beheerder besluit de toegangsniveaus voor afdeling A en afdeling B te verwijderen, omdat deze afdelingen worden opgeheven. De beheerder voert relatiequery's op beide toegangsniveaus uit voordat hij ze verwijdert. In het gebied *Queryresultaten* worden de objecten weergegeven waarop het verdwijnen van de toegangsniveaus invloed zal hebben. In het venster *Details* wordt de locatie van deze objecten in de CMC weergegeven voor het geval de beheerder de rechten van de objecten wil wijzigen voordat de toegangsniveaus worden verwijderd.

> **Opmerking**
>
> u krijgt de lijst met objecten waarop de bewerking invloed heeft alleen te zien als u *weergave*rechten voor de objecten hebt.

> **Opmerking**
>
> De resultaten van een relatiequery voor een toegangsniveau bevatten alleen objecten waarvoor het toegangsniveau expliciet is toegewezen. Als voor een object een toegangsniveau wordt gebruikt vanwege overname-instellingen, wordt dit object niet weergegeven in de queryresultaten.

7.3.8 Toegangsniveaus beheren op meerdere locaties

Toegangsniveaus zijn objecten op een oorspronkelijke locatie die u kunt herhalen op doellocaties. U kunt toegangsniveaus herhalen als ze voorkomen in de ACL (Access Control List) van een herhalingsobject. Als een principal bijvoorbeeld toegangsniveau A heeft voor een Crystal Reports-rapport en dit rapport op meerdere locaties wordt herhaald, wordt toegangsniveau A ook herhaald.

> **Opmerking**
>
> Als op de doellocatie een toegangsniveau met dezelfde naam voorkomt, wordt het toegangsniveau niet herhaald. In dat geval moet u of de beheerder van de doellocatie een van de toegangsniveaus een andere naam geven, zodat de herhaling kan worden uitgevoerd.

Als u een toegangsniveau op meerdere locaties hebt herhaald, dient u rekening te houden met de aanwijzingen voor beheer die in deze sectie zijn beschreven.

Herhaalde toegangsniveaus wijzigen op de oorspronkelijke locatie

Als een herhaald toegangsniveau op de oorspronkelijke locatie wordt gewijzigd, wordt het toegangsniveau op de doellocatie bijgewerkt bij de eerstvolgende keer dat de herhaling volgens planning wordt uitgevoerd. Als u bij herhaling in beide richtingen een herhaald toegangsniveau wijzigt op de doellocatie, wordt het toegangsniveau op de oorspronkelijke locatie ook gewijzigd.

> **Opmerking**
>
> Let erop dat wijzigingen die in een toegangsniveau op de ene locatie zijn aangebracht, geen nadelige invloed hebben op objecten op andere locaties. Vraag de beheerders van de verschillende locaties om relatiequery's voor het herhaalde toegangsniveau uit te voeren voordat u wijzigingen aanbrengt.

Herhaalde toegangsniveaus wijzigen op de doellocatie

> **Opmerking**
>
> Deze functie is uitsluitend van toepassing op herhaling in beide richtingen.

Wijzigingen die zijn aangebracht in herhaalde toegangsniveaus op een doellocatie worden niet doorgevoerd op de oorspronkelijke locatie. De beheerder van een doellocatie kan bijvoorbeeld het planningsrecht voor Crystal Reports-rapporten toekennen in het herhaalde toegangsniveau terwijl dit recht op de oorspronkelijke locatie is geweigerd. Dit heeft tot gevolg dat de namen van toegangsniveaus en de namen van herhaalde objecten ongewijzigd kunnen blijven, terwijl de effectieve rechten die principals voor objecten hebben per doellocatie kunnen verschillen.

Als het herhaalde toegangsniveau op de oorspronkelijke locatie afwijkt van de doellocatie, wordt het verschil in effectieve rechten gedetecteerd bij de eerstvolgende keer dat een herhalingstaak volgens planning wordt uitgevoerd. U kunt afdwingen dat het toegangsniveau op de doellocatie wordt overschreven door het toegangsniveau op de oorspronkelijke locatie of het toegangsniveau op de doellocatie intact laten. Als u het toegangsniveau op de doellocatie echter niet laat overschrijven door het toegangsniveau op de oorspronkelijke locatie, wordt herhaling niet toegepast op objecten die in de wachtij staan voor herhaling en gebruikmaken van dat toegangsniveau.

Als u niet wilt dat gebruikers herhaalde toegangsniveaus op de doellocatie kunnen wijzigen, voegt u gebruikers van doellocaties aan toegangsniveaus toe als principals en kent u aan deze gebruikers alleen *weergave*rechten toe. Dit betekent dat gebruikers van de doellocatie het toegangsniveau kunnen weergeven, maar de rechteninstellingen ervan niet kunnen wijzigen en geen rechten aan andere gebruikers kunnen toekennen.

Verwante informatie

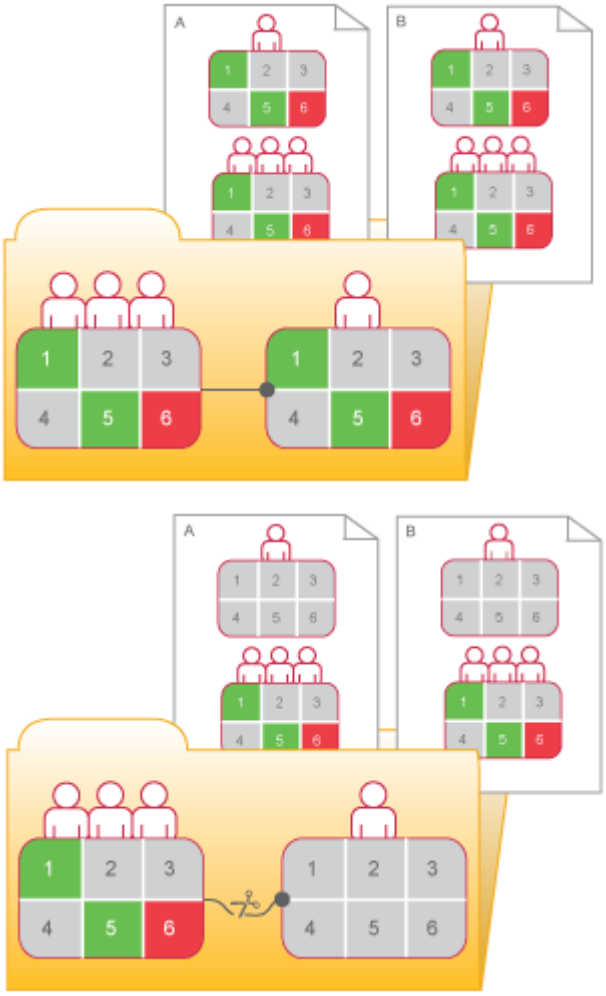
Federatie [pagina 962]
De relatie tussen toegangsniveaus en objecten traceren [pagina 142]

7.4 Overname uitschakelen

Via overname kunt u beveiligingsinstellingen beheren zonder rechten te hoeven opgeven voor elk afzonderlijk object. In bepaalde gevallen wilt u echter niet dat rechten worden overgenomen. Mogelijk wilt u bijvoorbeeld de rechten van elk afzonderlijk object aanpassen. U kunt overname voor een principal uitschakelen in de toegangscontrolelijst van een object. Hierbij kunt u aangeven of u groepsovername, mapovername of beide wilt uitschakelen.

> **Opmerking**
>
> als overname wordt uitgeschakeld, geldt dit voor alle rechten. U kunt niet de overname van bepaalde rechten uitschakelen en van andere niet.

In het diagram “Overname uitschakelen” is de groeps- en mapovername aanvankelijk van toepassing. De rode gebruiker neemt de rechten 1 en 5 over als toegewezen, de rechten 2, 3 en 4 als niet opgegeven en recht 6 als expliciet geweigerd. Deze rechten, ingesteld op mapniveau voor de groep, betekenen dat de rode gebruiker en alle andere leden van de groep deze rechten hebben voor de objecten A en B in de map. Als de overname op mapniveau wordt uitgeschakeld, worden alle rechten van de rode gebruiker voor de objecten in die map gewist totdat een beheerder nieuwe rechten aan deze gebruiker toewijst.



Overname uitschakelen

7.4.1 Overname uitschakelen

Middels deze procedure kunt u groeps- of mapovername, of beide, uitschakelen voor een principal in de ACL (Access Control List) van een object.

1. Selecteer het object waarvoor u overname wilt uitschakelen.
2. Klik op *Beheren* > *Gebruikersbeveiliging*.
   Het dialoogvenster *Gebruikersbeveiliging* wordt weergegeven.
3. Selecteer de principal waarvoor u overname wilt uitschakelen en klik op *Beveiliging toewijzen*.
   Het dialoogvenster *Beveiliging toewijzen* wordt weergegeven.
4. Configureer de gewenste overname-instellingen.

- Als u groepsovername wilt uitschakelen (de rechten die de principal overneemt via groepslidmaatschap), schakelt u het selectievakje *Overnemen van bovenliggende groep* uit.
- Als u mapovername wilt uitschakelen (de rechten die het object overneemt van de map), schakelt u het selectievakje *Overnemen van bovenliggende groep* uit.

5. Klik op *OK*.

7.5 Beheer delegeren met rechten

Met rechten kunt u niet alleen de toegang tot objecten en instellingen beheren, maar ook beheertaken verdelen tussen de functiegroepen in uw organisatie. Zo kan het nuttig zijn om personen uit verschillende afdelingen hun eigen gebruikers en groepen te laten beheren. Of u kunt instellen dat één beheerder op het hoogste niveau zorg draagt voor het beheer van het BI-platform, terwijl de servers door medewerkers van de IT-afdeling worden beheerd.

Als de groepsstructuur en de mappenstructuur overeenkomen met de ingestelde beveiligingsstructuur voor gedelegeerd beheer, moet u de gedelegeerde beheerder alle rechten voor gebruikersgroepen geven, maar minder dan Volledig beheer voor de gebruikers die worden beheerd. Zo kunt u bijvoorbeeld voorkomen dat de gedelegeerde beheerder gebruikersattributen bewerkt of gebruikers lid maakt van andere groepen.

> **Opmerking**
>
> Objectmigraties kunnen het beste worden uitgevoerd door leden van de Beheerdersgroep, met name de gebruikersaccount Beheerder. Als u een object wilt migreren, moeten veel verwante objecten misschien ook worden gemigreerd. Het is misschien niet mogelijk om de vereiste beveiligingsrechten voor alle objecten te verkrijgen voor een gedelegeerde beheerdersaccount.

In de tabel "Rechten voor gedelegeerde beheerders" ziet u een overzicht van de rechten die gedelegeerde bebeerders nodig hebben om veelvoorkomende acties te kunnen uitvoeren.

Rechten voor gedelegeerde beheerders

Actie van gedelegeerde beheerder	Rechten die de gedelegeerde beheerder nodig heeft
Nieuwe gebruikers maken	Het recht *Toevoegen* voor de map *Gebruikers* op het bovenste niveau.
Nieuwe groepen maken	Het recht *Toevoegen* voor de map *Gebruikersgroepen* op het bovenste niveau.
Beheerde groepen verwijderen, plus afzonderlijke gebruikers in die groepen	Het recht *Verwijderen* voor relevante groepen.
Alleen de gebruikers verwijderen die zijn gemaakt door de gedelegeerde beheerder	Het recht *Objecten verwijderen waarvan de gebruiker de eigenaar is* voor de map *Gebruikers* op het bovenste niveau.
Alleen de gebruikers en groepen verwijderen die zijn gemaakt door de gedelegeerde beheerder	Het recht *Objecten verwijderen waarvan de gebruiker de eigenaar is* voor de map *Gebruikersgroepen* op het bovenste niveau.

Actie van gedelegeerde beheerder	Rechten die de gedelegeerde beheerder nodig heeft
Alleen de gebruikers bewerken die zijn gemaakt door de gedelegeerde beheerder (inclusief het toevoegen van deze gebruikers aan deze groepen)	Het recht *Objecten bewerken waarvan de gebruiker de eigenaar is* en *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* voor de map *Gebruikers* op het bovenste niveau.
Alleen de groepen bewerken die de gedelegeerde beheerder maakt (inclusief het toevoegen van gebruikers aan deze groepen)	Het recht *Objecten bewerken waarvan de gebruiker de eigenaar is* en *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* voor de map *Gebruikersgroepen* op het bovenste niveau.
Wachtwoorden wijzigen voor gebruikers in door hen beheerde groepen	Het recht *Wachtwoord bewerken* voor relevante groepen.
Alleen de wachtwoorden wijzigen van principals die de gedelegeerde beheerder heeft gemaakt	Het recht *Gebruikerswachtwoord wijzigen waarvan de gebruiker eigenaar is* voor de map *Gebruikers* op het bovenste niveau of voor relevante groepen. **Opmerking** het toewijzen van het recht *Gebruikerswachtwoord wijzigen waarvan de gebruiker eigenaar is* voor een groep geldt alleen voor een gebruiker als u de gebruiker toevoegt aan de desbetreffende groep.
Gebruikersnamen, beschrijving en andere attributen wijzigen, en gebruikers toewijzen aan andere groepen	Het recht *Bewerken* voor relevante groepen.
Gebruikersnamen, beschrijving en andere attributen wijzigen en gebruikers toewijzen aan andere groepen, maar alleen voor de gebruikers die de gedelegeerde beheerder heeft gemaakt	Het recht *Objecten bewerken waarvan de gebruiker de eigenaar is* voor de map *Gebruikers* op het bovenste niveau of voor relevante groepen. **Opmerking** het toewijzen van het recht *Objecten bewerken die het eigendom zijn van de gebruiker* voor relevante groepen geldt alleen voor een gebruiker als u de gebruiker toevoegt aan de desbetreffende groep.

7.5.1 Kiezen tussen de opties voor "*Rechten van gebruikers voor objecten wijzigen*"

Als u gedelegeerd beheer instelt, geeft u de gedelegeerde beheerder rechten voor het beheer van principals. U kunt de beheerder alle rechten (*Volledig beheer*) geven, maar het is beter om met de instellingen van geavanceerde rechten het recht *Rechten wijzigen* in te trekken en de gedelegeerde beheerder alleen het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* te geven. U kunt de beheerder ook het recht *Overname-instellingen voor rechten veilig wijzigen* geven in plaats van het recht *Overname-instellingen voor rechten wijzigen*. De verschillen tussen deze rechten worden hierna beschreven.

Rechten van gebruikers voor objecten wijzigen

Met dit recht kan een gebruiker elk recht van een andere gebruiker voor dat object wijzigen. Als gebruiker A bijvoorbeeld de rechten *Objecten weergeven* en *Rechten van gebruikers voor objecten wijzigen* voor een object heeft, kan gebruiker A de rechten voor dat object zodanig wijzigen dat deze of andere gebruikers het recht Volledig beheer voor dit object krijgen.

De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen

Met dit recht kan een gebruiker alleen de rechten toekennen, weigeren of instellen op niet-opgegeven die aan de gebruiker zelf zijn toegewezen. Als gebruiker A bijvoorbeeld de rechten *Weergeven* en *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* heeft, kan gebruiker A aan zichzelf niet meer rechten toekennen en kan deze alleen deze twee rechten (*Weergeven* en *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen*) aan andere gebruikers toekennen of weigeren. Daarnaast kan gebruiker A alleen de rechten van gebruikers wijzigen voor objecten waarvoor deze zelf het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* heeft.

Gebruiker A kan in de volgende gevallen de rechten van gebruiker B voor object O wijzigen:

- Gebruiker A heeft het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* voor object O.
- Elk recht of toegangsniveau dat gebruiker A wijzigt voor gebruiker B, moet zijn toegewezen aan gebruiker A.
- Gebruiker A heeft het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* voor gebruiker B.
- Als een toegangsniveau wordt toegewezen, heeft gebruiker A het recht *Toegangsniveau toewijzen* op het toegangsniveau dat wordt gewijzigd voor gebruiker B.

Een rechtenbereik kan de effectieve rechten die een gedelegdeerde beheerder kan toewijzen, verder beperken. Zo kan een gedelegeerde beheerder bijvoorbeeld de rechten *Rechten veilig wijzigen* en *Bewerken* hebben voor een map, maar is het bereik van deze rechten beperkt tot de map en gelden ze niet voor de subobjecten van de map. De gedelegeerde beheerder kan in feite alleen het recht *Bewerken* toewijzen aan de map (maar niet aan de subobjecten van de map), en alleen met het bereik “Toepassen op object”. Aan de andere kant, als aan de gedelegeerde beheerder het recht *Bewerken* met het bereik “Toepassen op subobject” voor een map is toegewezen, kan deze beheerder aan andere principals het recht *Bewerken* met beide bereiken toewijzen voor de subobjecten van de map. Voor de map zelf kan de beheerder echter alleen het recht *Bewerken* met het bereik “Toepassen op subobject” toewijzen.

Daarnaast mag de gedelegeerde beheerder geen rechten wijzigen van groepen voor andere principals waarvoor hij of zijn niet het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* heeft. Dit is handig als u bijvoorbeeld twee gedelegeerde beheerders hebt die rechten toewijzen aan verschillende gebruikersgroepen van dezelfde map, maar niet wilt dat een van de gedelegeerde beheerders de toegang kan weigeren aan groepen die door de andere gedelegeerde beheerder worden beheerd. Dit kunt u regelen met het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen*, omdat gedelegeerde beheerders dit recht meestal niet hebben voor elkaar.

Overname-instellingen voor rechten veilig wijzigen

Met dit recht kan een gedelegeerde beheerder overname-instellingen wijzigen voor andere principals voor de objecten waartoe de gedelegeerde beheerder toegang heeft. Als een gedelegeerde beheerder de overname-instellingen van andere principals wil wijzigen, moet deze beschikken over dit recht voor het object en de gebruikersaccounts van de principals.

7.5.2 Eigendomsrechten

Eigendomsrechten hebben alleen betrekking op de eigenaar van het object waarvoor rechten worden gecontroleerd. In het BI-platform is de eigenaar van een object een principal die het object heeft gemaakt. Als deze principal uit het systeem wordt verwijderd, gaat het eigendom over op de beheerder.

Eigendomsrechten zijn nuttig bij het beheren van beveiliging op basis van eigenaar. U kunt bijvoorbeeld een map of mappenstructuur maken waarin diverse gebruikers documenten kunnen maken en weergeven, maar alleen hun eigen documenten kunnen wijzigen of verwijderen. Ook kunt u met eigendomsrechten gebruikers toestaan te werken met exemplaren die zij zelf maken, maar niet met exemplaren van anderen. Ook met het toegangsniveau Planning kunnen gebruikers alleen hun eigen exemplaren bewerken, verwijderen, onderbreken en opnieuw inplannen.

Eigenaarsrechten werken op dezelfde manier als de overeenkomende normale rechten. Eigendomsrechten zijn echter alleen effectief wanneer aan de principal eigenaarsrechten zijn toegekend en normale rechten zijn geweigerd of niet zijn opgegeven.

7.6 Aanbevelingen voor rechtenbeheer

Houd bij het beheren van rechten rekening met de volgende zaken:

- Maak zo veel mogelijk gebruik van toegangsniveaus. Deze vooraf gedefinieerde groepen rechten vereenvoudigen het beheer, omdat verwante rechten zijn gegroepeerd.
- Stel rechten en toegangsniveaus in voor mappen op het bovenste niveau. Als u overname inschakelt, kunnen deze rechten worden overgenomen in het systeem met minimale tussenkomst van de beheerder.
- Voorkom zo mogelijk dat de overname wordt verbroken. Dit bespaart u tijd die u anders kwijt zou met het beveiligen van toegevoegde inhoud in het BI-platform.
- Stel eerst de juiste rechten in voor gebruikers en groepen op mapniveau en publiceer vervolgens objecten naar deze map. Gebruikers of groepen die rechten voor een map hebben, krijgen standaard dezelfde rechten voor de objecten die u naar die map publiceert.
- Orden gebruikers in gebruikersgroepen, wijs toegangsniveaus en rechten aan de hele groep toe en wijs zo nodig toegangsniveaus en rechten aan specifieke leden toe.
- Maak afzonderlijke Administrator-accounts voor elke beheerder in het systeem en voeg deze toe aan de groep Administrators om de verantwoordelijkheid voor systeemwijzigingen te verbeteren.

- Standaard worden aan de groep Iedereen zeer beperkte rechten toegekend voor mappen op het hoogste niveau in het BI-platform. Na de installatie wordt u aangeraden de rechten van leden van de groep Iedereen te controleren en op basis hiervan de beveiliging in te stellen.

8 Het BI-platform beveiligen

8.1 Overzicht van beveiliging

Deze sectie bevat een beschrijving van de voorzieningen die het BI-platform biedt op het gebied van beveiliging. Beheerders en systeemontwerpers kunnen hier antwoord vinden op veelgestelde vragen over beveiliging.

De architectuur van BI-platform biedt oplossingen voor de vele beveiligingsvereisten die tegenwoordig door bedrijven en instellingen worden gesteld. In de huidige versie worden diverse functies ondersteund, zoals gedistribueerde beveiliging, eenmalige aanmelding, beveiliging van brontoegang, beveiliging met toenemende en afnemende objectrechten, en de externe verificatie voor beveiliging tegen onbevoegde toegang.

Omdat het BI-platform het raamwerk voor een toenemend aantal onderdelen van de Enterprise-reeks van SAP BusinessObjects-producten vormt, wordt in deze sectie uitvoerig ingegaan op de beveiligingsfuncties en verwante functionaliteit om uit te leggen hoe in het raamwerk zelf, beveiliging wordt afgedwongen en onderhouden. Deze sectie bevat geen concrete procedures, maar richt zich op beveiligingsconcepten en bevat koppelingen naar belangrijke procedures.

Na een korte inleiding over beveiligingsconcepten voor het systeem worden details over de volgende onderwerpen gegeven:

- Het gebruik van codering en beveiligingsmodi voor gegevensverwerking om gegevens te beschermen.
- Het instellen van de Secure Sockets Layer voor implementaties van BI-platform.
- Richtlijnen voor het instellen en onderhouden van firewalls voor het BI-platform.
- Omgekeerde proxyserver configureren.

8.2 Veilig gebruik van programmaobjecten

Als een gebruiker planningsrechten heeft voor programmaobjecten, heeft de gebruiker de bevoegdheid om deze uit te voeren.

Voor Java-programma's kunnen gebruikers het volgende doen:

- Gebruikers kunnen de hoofdklasse specificeren. De auteur van het programma moet zorgen hij/zij geen secundaire/testhoofdklasse onbedoeld achterlaat in het programma.
- Gebruikers kunnen het klassepad specificeren. Zij mogen niet bevoegd zijn om `jar` naar het systeem te uploaden. Dit zou kunnen worden gebruikt om speciale code uit te voeren.

Algemene aanbevelingen voor het veilig maken van programmaobjecten

- Geef geen serveraanmeldgegevens aan de gebruiker.

- Geef minimumrechten aan de gebruikersaccount die het programma op de server uitvoert. Geef vooral geen toegang tot het installatiepad van SAP BusinessObjects Business Intelligence Platform.
- Wij raden aan om de optie *Taak laten mislukken* in *Applicaties* > *Central Management Console* > *Rechten voor programmaobjecten*.
- Wij raden aan om mappen te gebruiken voor toegangsbesturing. Programmaobjecten met verschillende beveiligingsniveaus moeten in verschillende mappen worden geplaatst.

8.3 Planning van herstel na uitval

Teneinde de investering van uw organisatie in het BI-platform te beschermen en bij uitval maximale continuïteit in de bedrijfsvoering te garanderen, moeten bepaalde stappen worden genomen. Deze sectie biedt richtlijnen waarmee een plan voor herstel bij uitval kan worden opgesteld voor uw organisatie. U kunt ook deze SAP Note bekijken voor meer informatie.

Algemene richtlijnen

- Voer regelmatige systeemback-ups uit en stuur zo nodig kopieën van back-upmedia naar externe locaties.
- Bewaar alle softwaremedia op een veilige plek.
- Bewaar alle licentiedocumentatie op een veilige plek.

Specifieke richtlijnen

Er zijn drie systeembronnen die specifieke aandacht vereisen bij de planning van herstel bij uitval:

- Inhoud op de servers van de bestandsgegevensopslagruimte: dit omvat eigen inhoud zoals rapporten. Maak regelmatig back-ups van deze inhoud - bij calamiteiten kan dergelijke inhoud niet opnieuw worden gegenereerd als hier geen procedure voor is.
- De systeemdatabase die door de CMS wordt gebruikt: deze bron bevat alle cruciale metagegevens voor uw implementatie zoals gebruikersinformatie, rapporten en andere gevoelige informatie over uw organisatie.
- Sleutelbestand met databasegegevens (.dbinfo-bestand): deze bron bevat de hoofdsleutel tot de systeemdatabase. Als deze sleutel om een bepaalde reden niet beschikbaar is, hebt u geen toegang tot de systeemdatabase. Het wordt sterk aanbevolen om na de implementatie van het BI-platform het wachtwoord voor deze bron op een veilige en bekende locatie te bewaren. Zonder het wachtwoord kunt u het bestand niet opnieuw genereren en hebt u geen toegang meer tot de systeemdatabase.

8.4 Algemene aanbevelingen voor beveiliging van uw implementatie

Aanbevolen richtlijnen voor beveiliging van uw BI-platformimplementaties:

- Gebruik firewalls om de communicatie tussen de CMS en andere systeemonderdelen te beschermen. Verberg uw CMS indien mogelijk altijd achter een firewall. Zorg er op zijn minst voor dat de systeemdatabase zich achter een firewall bevindt.
- Voeg extra codering toe aan de File Repository Servers. Zodra het systeem actief is, wordt eigen inhoud op deze servers opgeslagen. Voeg extra codering toe via het besturingssysteem of gebruik een extern hulpprogramma.
- Implementeer een omgekeerde proxyserver vóór de webtoepassingsservers zodat deze achter één IP-adres kunnen worden verborgen. Door deze configuratie wordt alle internetverkeer dat aan privéwebtoepassingsservers gericht is, via de omgekeerde proxyserver geleid en blijven privé IP-adressen verborgen.
- Zie streng toe op de naleving van het bedrijfsbeleid voor wachtwoorden. Zorg ervoor dat gebruikerswachtwoorden regelmatig worden gewijzigd.
- Als u ervoor hebt gekozen om de systeemdatabase en de webtoepassingsserver te installeren die bij het BI-platform geleverd worden, moet u de relevante documentatie oproepen om ervoor te zorgen dat deze onderdelen met de juiste beveiligingsconfiguraties worden geïmplementeerd.
- Gebruik het SSL-protocol (Secure Sockets Layer) voor alle netwerkcommunicatie tussen clients en servers in uw implementatie.
- Zorg ervoor dat de installatiemap van het platform en submappen zijn beveiligd. Gevoelige tijdelijke gegevens kunnen worden opgeslagen in deze mappen tijdens de systeembewerking.
- Toegang tot de Central Management Console (CMC) moet worden beperkt tot alleen lokale toegang. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor informatie over de implementatieopties voor de CMC.
- Foutberichten van Web Intelligence bevatten standaard informatie over databaseschema's. Als u foutberichten wilt weergeven zonder informatie over databaseschema's, voert u de volgende stappen uit:
  1. Open het configuratiebestand `WebIContainer_ServerDescriptor.xml` voor bewerking.
     Dit bevindt zich standaard in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64config`.
  2. Wijzig de waarde van deze parameter in False: `WebiParamDetailedDbErrorsEnabled = False`.

> **⚠ Let op**
>
> Tijdelijke aanduidingen die niet voor bewerking zijn bedoeld, mogen op geen enkele manier worden gewijzigd. De systeembeheerder moet ervoor zorgen dat alleen de juiste persoon uit de beheerdersgroep (die bedoeld zijn voor het knooppuntbeheer) over de bewerkingsrechten voor het knooppunt beschikt. Alle andere gebruikers, inclusief andere leden van de beheerdersgroep, moeten worden beperkt tot het weergeven/beheren van de knooppuntobjecten door de juiste beveiligingsrechten toe te passen. Als een van de tijdelijke aanduidingen per ongeluk is beschadigd en CMS niet wordt weergegeven, raadpleegt u deze SAP Note: 3269127.

> **ⓘ Opmerking**
>
> Zie SAP Knowledge Base Article 3278916 voor informatie over hoe het wijzigen van plaatsaanduidingen kan worden voorkomen om verstoring van het BI-landschap door kwaadwillenden te voorkomen.

Verwante informatie

Het SSL-protocol configureren [pagina 186]
Wachtwoordbeperkingen [pagina 159]
Beveiliging configureren voor gebundelde externe servers [pagina 154]

8.5 Beveiliging configureren voor gebundelde externe servers

Als u ervoor hebt gekozen om externe serveronderdelen die zijn gebundeld met het BI-platform te installeren, raden we u aan de beveiligingssecties van de officiële documentatie voor SAP SQL Anywhere en Apache Tomcat door te nemen.

8.6 Actieve vertrouwensrelatie

Een vertrouwensrelatie tussen twee domeinen is in een netwerkomgeving meestal een verbinding waarbij het ene domein alle gebruikers herkent die zijn geverifieerd in het andere domein. Door de vertrouwensrelatie kunnen gebruikers toegang krijgen tot bronnen in meerdere domeinen terwijl de beveiliging blijft gehandhaafd en zonder dat de gebruikers steeds opnieuw hun referenties hoeven op te geven.

De actieve vertrouwensrelatie werkt in de omgeving van BI-platform op vergelijkbare wijze om gebruikers probleemloos toegang tot de bronnen in het gehele systeem te verlenen. Nadat de gebruiker is geverifieerd en een actieve sessie heeft gekregen, kunnen alle andere BI-platformonderdelen de aanvragen en acties van de gebruiker verwerken zonder dat de gebruiker referenties hoeft op te geven. De actieve vertrouwensrelatie vormt de basis van de gedistribueerde beveiliging van het BI-platform.

8.6.1 Aanmeldingstokens

Een aanmeldingstoken is een gecodeerde tekenreeks die de eigen gebruiksattributen definieert en sessiegegevens voor een gebruiker bevat. De gebruiksattributen van het aanmeldingstoken worden opgegeven als het aanmeldingstoken wordt gegenereerd. Met deze attributen kunnen beperkingen voor het aanmeldingstoken worden opgegeven om de kans te verminderen dat het aanmeldingstoken wordt misbruikt door onbevoegden. De huidige gebruiksattributen voor aanmeldingstokens zijn:

- *Aantal minuten*
  Met dit attribuut wordt de geldigheid van het aanmeldingstoken beperkt.
- *Aantal aanmeldingen*
  Met dit attribuut wordt het aantal keren beperkt dat het aanmeldingstoken kan worden gebruikt voor aanmelding bij het BI-platform.

Met beide attributen wordt voorkomen dat onbevoegden toegang krijgen tot het BI-platform met behulp van aanmeldingstokens die van geldige gebruikers zijn opgehaald.

> **Opmerking**
>
> het opslaan van een aanmeldingstoken in een cookie vormt een mogelijk beveiligingsrisico als het netwerk tussen de browser en toepassings- of webserver onbeveiligd is, bijvoorbeeld als de verbinding via een openbaar netwerk wordt gemaakt en er geen SSL of Vertrouwde verificatie wordt gebruikt. Het is een goede gewoonte om SSL (Secure Sockets Layer) te gebruiken om beveiligingsrisico tussen de browser en toepassings- of webserver terug te dringen.

Wanneer de aanmeldingscookie is uitgeschakeld en de webserver of de webbrowser een time-out bereikt, wordt het aanmeldingsscherm weergegeven. Als de cookie is ingeschakeld en de webserver of de webbrowser bereikt een time-out, dan wordt de gebruiker automatisch weer bij het systeem aangemeld. Aangezien statusinformatie echter aan de websessie is gekoppeld, gaat de status van de gebruiker verloren. Als de gebruiker bijvoorbeeld een navigatiestructuur had uitgevouwen en een bepaald item had geselecteerd, wordt de structuur opnieuw ingesteld.

Voor het BI-platform zijn aanmeldingstokens standaard ingeschakeld in de webclient, maar u kunt aanmeldingstokens uitschakelen voor BI-startpunt. Wanneer u de aanmeldingstokens in de client uitschakelt, blijft de gebruikerssessie beperkt tot de time-out van de webserver of webbrowser. Wanneer die sessie verloopt, moet de gebruiker zich opnieuw aanmelden bij het BI-platform.

8.6.2 Ticketmechanisme voor gedistribueerde beveiliging

Bij Enterprise-systemen voor grote aantallen gebruikers is meestal een bepaalde vorm van gedistribueerde beveiliging nodig. Een Enterprise-systeem kan gedistribueerde beveiliging nodig hebben voor de ondersteuning van bepaalde functies, zoals de overdracht van vertrouwen (de mogelijkheid om een ander onderdeel toe te staan namens de gebruiker te reageren).

Het BI-platform biedt gedistribueerde beveiliging door de implementatie van een ticketmechanisme (een mechanisme dat vergelijkbaar is met het Kerberos-ticketmechanisme). De CMS verleent tickets die onderdelen machtigen om acties namens een bepaalde gebruiker uit te voeren. In het BI-platform wordt het ticket een aanmeldingstoken genoemd.

Dit aanmeldingstoken wordt het meest gebruikt via het web. Wanneer gebruikers voor het eerst worden geverifieerd door het BI-platform, ontvangen zij een aanmeldingstoken van de CMS. De webbrowser van de gebruiker slaat dit aanmeldingstoken in cache op. Bij nieuwe aanvragen van de gebruiker kunnen andere BI-platformonderdelen het aanmeldingstoken van de webbrowser van de gebruiker lezen.

8.7 Sessies en het bijhouden van sessies

Een sessie is in het algemeen een verbinding tussen een client en een server die gegevensuitwisseling tussen twee computers mogelijk maakt. De status van een sessie is een set gegevens waarmee de attributen van de sessie, de configuratie of de inhoud worden beschreven. Als u via het web een verbinding tussen de client en de server tot stand brengt, wordt door de aard van HTTP de duur van de sessie beperkt tot één pagina met

gegevens. De status van een sessie wordt dus gedurende de weergavetijd van één webpagina in het geheugen van de webbrowser bewaard. Wanneer u naar een andere webpagina gaat, wordt de status van de eerste sessie verwijderd en vervangen door de status van de volgende sessie. Websites en webtoepassingen moeten daarom de status van een sessie ergens opslaan om de gegevens van de sessie later opnieuw te kunnen gebruiken.

In het BI-platform worden twee algemene methoden gebruikt om een sessiestatus op te slaan:

- Cookies - een cookie is een klein tekstbestand waarin de sessiestatus op de client wordt opgeslagen. De cookie wordt voor later gebruik opgeslagen in de webbrowsercache van de gebruiker. Het aanmeldingstoken van BI-platform is een voorbeeld van deze methode.
- Sessievariabelen - een sessievariabele is een deel van het geheugen waarin de sessiestatus op de server wordt opgeslagen. Als het BI-platform aan een gebruiker een actieve identiteit op het systeem toewijst, worden gegevens zoals het verificatietype van de gebruiker in een sessievariabele opgeslagen. Zolang de sessie wordt onderhouden, wordt de gebruiker niet gevraagd de gegevens voor de tweede keer op te geven en hoeft er ook geen taak worden herhaald die nodig is om de volgende aanvraag af te handelen. Voor Java-implementaties wordt de sessie gebruikt voor de verwerking van .jsp-aanvragen, voor .NET-implementaties wordt de sessie gebruikt voor de verwerking van .aspx-aanvragen.

> **Opmerking**
>
> In het ideale geval blijft de sessievariabele tijdens de hele sessie van de gebruiker in het systeem aanwezig. De sessievariabele wordt verwijderd zodra de gebruiker klaar is met werken in het systeem, waardoor de beveiliging blijft gehandhaafd en het gebruik van bronnen wordt geminimaliseerd. Omdat de interactie tussen een webbrowser en een webserver echter statusloos kan zijn, is het soms moeilijk vast te stellen wanneer gebruikers het systeem verlaten als ze zich niet expliciet afmelden. Dit probleem wordt in het BI-platform verholpen door sessies bij te houden.

8.7.1 Sessies bijhouden op de CMS

Sessies worden op de CMS met een eenvoudig algoritme bijgehouden. Een gebruiker die zich aanmeldt, krijgt een CMS-sessie toegewezen. Deze sessie wordt door de CMS gehandhaafd totdat de gebruiker zich afmeldt of totdat de sessievariabele voor de webtoepassingsserver wordt vrijgegeven.

De sessie van de webtoepassingsserver verzendt regelmatig statusmeldingen naar de CMS, zodat de CMS-sessie gehandhaafd blijft zolang de sessie van de webtoepassingsserver bestaat. Als de sessie van de webtoepassingsserver gedurende tien minuten niet meer met de CMS kan communiceren, verwijdert de CMS de CMS-sessie. Deze methode wordt gebruikt in scenario's waar onderdelen op de client onverwachts kunnen worden afgesloten.

8.7.2 Sessies beheren

U kunt sessie weergeven en beëindigen in de CMC.

U kunt sessies weergeven en beëindigen in de Central Management Console (CMC). Bijvoorbeeld: u wilt bekijken welke gebruikers meerdere sessies gebruiken. Of u wilt sessies beëindigen die te veel systeembronnen gebruiken of erg oude sessies beëindigen. Ook moet u mogelijk sessies beëindigen als u uitvaltijd of upgrades voor het systeem voorbereidt.

8.7.2.1 Sessielijst weergeven

Sessies weergeven in de CMC.

U kunt een lijst met sessies weergeven in de Central Management Console.

1. Meld u als beheerder aan bij de CMC.
2. Klik in het gebied *Beheren* op *Sessies*.

De lijst met gebruikerssessies voor het cluster wordt weergegeven. U kunt op de kolomkoppen klikken om de lijst te sorteren op gebruikersnaam, op het aantal geopende sessies of op moment van aanmelding. U kunt ook op de opties voor de gebruikersnaam, het aantal sessies of het moment van aanmelding klikken om details voor de gebruikerssessie weer te geven in het onderste venster.

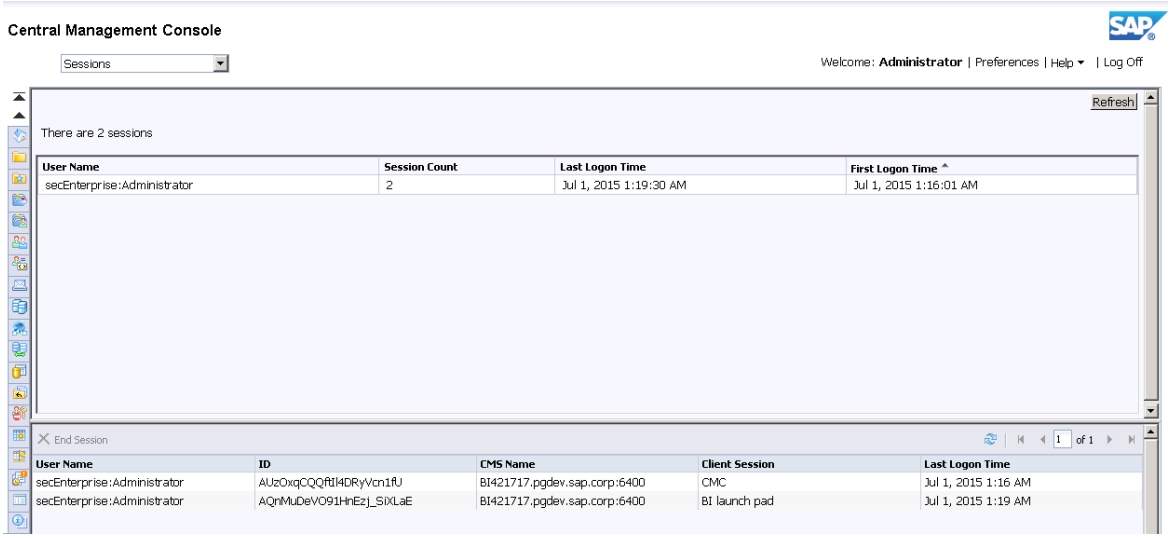
8.7.2.2 Sessies beëindigen

Sessies beëindigen in de CMC.

U kunt afzonderlijke of meerdere sessies beëindigen.

1. Meld u als beheerder aan bij de CMC.
2. Klik in het gebied *Beheren* op *Sessies*.

   De lijst met gebruikerssessies voor het cluster wordt weergegeven.



3. Klik op de opties voor de gebruikersnaam, het aantal sessies of het moment van aanmelding de gebruikerssessie weer te geven in het onderste venster
4. Klik om een afzonderlijke sessie te selecteren of druk op `Ctrl` + `en klik` om meerdere sessies te selecteren.
5. Klik op *Sessie beëindigen*.

> **Opmerking**
>
> De gebruikerssessie wordt vrijgegeven zodra de gebruiker de browser sluit.

> **Opmerking**
>
> Aan u moet het recht “Objecten bewerken” zijn toegewezen voor het CMS-object.

> **Opmerking**
>
> U kunt de huidige beheersessie niet beëindigen.

8.7.3 Script voor het wissen van verouderde sessies

Script

Er is een script toegevoegd voor het wissen van verouderde sessies en het vrijmaken van niet-gebruikte licenties om deze beschikbaar te maken voor gebruikers die wachten om zich te kunnen aanmelden. Dit script wordt uitgevoerd tot het handmatig wordt gesloten en controleert op verouderde sessies en beëindigt deze met een interval van 10 minuten.

- Voor Windows vindt u het script hier: `<BI_Install_Dir>\SAP BusinessObjects Enterprise XI 4.0\java\lib\StaleSessionCleaner.jar`
- Voor Unix vindt u het script hier: `<BI_Install_Dir>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar`

De syntaxis die voor het script wordt gebruikt, is

> **Codesyntaxis**
>
> ```
> java -jar StaleSessionCleaner.jar <username> <password>
> <machine:port><authentication> <logdir>
> ```

8.8 Omgevingsbeveiliging

Met omgevingsbeveiliging wordt de beveiliging bedoeld van de algehele omgeving waarin client- en serveronderdelen met elkaar communiceren. Hoewel het internet en websystemen steeds populairder worden vanwege hun flexibiliteit en uitgebreide functionaliteit, werken ze in een omgeving die moeilijk te beveiligen is. Als u het BI-platform implementeert, wordt de omgevingsbeveiliging in twee communicatiegebieden onderverdeeld: webbrowser naar webserver en webserver naar BI-platform.

8.8.1 Webbrowser naar webserver

Als er tussen de webbrowser en de webserver gegevens worden verzonden, is er meestal een bepaalde mate van beveiliging nodig. Relevante beveiligingsmaatregelen omvatten gewoonlijk twee algemene taken:

- Ervoor zorgen dat de communicatie van gegevens veilig is.
- Ervoor zorgen dat alleen geldige gebruikers gegevens van de webserver kunnen ophalen.

> **Opmerking**
>
> deze taken worden gewoonlijk door webservers uitgevoerd met behulp van diverse beveiligingsmechanismen, waaronder het SSL-protocol (Secure Sockets Layer) en andere soortgelijke mechanismen. Het is een goede gewoonte om SSL te gebruiken om beveiligingsrisico tussen de browser en toepassings- of webserver terug te dringen.

U moet de communicatie tussen de webbrowser en de webserver onafhankelijk van het BI-platform beveiligen. Zie de documentatie bij uw webserver voor meer informatie over het beveiligen van clientverbindingen.

8.8.2 Webserver naar BI-platform

Firewalls worden gewoonlijk gebruikt om de communicatie tussen de webserver en de rest van het bedrijfsintranet (inclusief het BI-platform) te beveiligen. Het platform ondersteunt IP-filters of statistiche NAT (Network Address Translation). Ondersteunde omgevingen kunnen meerdere firewalls, webservers of toepassingsservers bevatten.

8.8.3 Bescherming tegen aanmeldingspogingen van kwaadwillende gebruikers

Hoe veilig een systeem ook is, er is altijd ten minste één locatie die kwetsbaar is voor ongewenste toegang, namelijk de locatie waar gebruikers zich aanmelden bij het systeem. Het is bijna onmogelijk deze locatie volledig te beschermen, omdat er altijd een mogelijkheid bestaat dat er toegang tot het systeem wordt verkregen door eenvoudigweg naar de gebruikersnaam en het wachtwoord te raden.

In het BI-platform zijn diverse technieken geïmplementeerd waarmee de kans wordt verkleind dat kwaadwillende gebruikers toegang tot het systeem krijgen. De beperkingen die hierna worden besproken, zijn alleen van toepassing op Enterprise-accounts. Deze beperkingen zijn dus niet van toepassing op accounts die zijn toegewezen aan een externe gebruikersdatabase (LDAP of Windows Active Directory). U kunt echter meestal wel met het externe systeem zelf soortgelijke beperkingen op de externe accounts toepassen.

8.8.4 Wachtwoordbeperkingen

Wachtwoordbeperkingen zorgen ervoor dat gebruikers die de standaard Enterprise-verificatie uitvoeren, wachtwoorden maken die vrij complex zijn. U kunt de volgende opties inschakelen:

1. Wachtwoorden afdwingen die bestaan uit hoofdletters en kleine letters.
   Deze optie zorgt ervoor dat wachtwoorden ten minste één hoofdletter en één kleine letter bevatten. Deze optie is standaard geselecteerd tenzij gewijzigd door de beheerder.
2. Cijfer(s) in wachtwoorden afdwingen
   Deze optie zorgt ervoor dat wachtwoorden ten minste één numeriek teken bevatten.

3. Speciale tekens in wachtwoorden afdwingen
   Deze optie zorgt ervoor dat wachtwoorden ten minste één speciaal teken bevatten.

Door een minimale complexiteit voor wachtwoorden af te dwingen vermindert u de kans dat kwaadwillende gebruikers toegang krijgen door het wachtwoord van een geldige gebruiker gewoonweg te raden.

8.8.5 Aanmeldingsbeperkingen

Aanmeldingsbeperkingen dienen in de eerste plaats om woordenboekaanvallen te voorkomen (een methode waarbij kwaadwillende gebruikers een geldige gebruikersnaam verkrijgen en achter het bijbehorende wachtwoord proberen te komen door elk woord in een woordenboek te proberen). Met de snelheid van de moderne hardware kunnen er miljoenen wachtwoorden per minuut worden geraden. Om woordenboekaanvallen te voorkomen heeft het BI-platform een intern mechanisme waarmee een vertraging (0,5 tot 1 seconde) tussen aanmeldingspogingen wordt afgedwongen. Verder bevat het platform een aantal aanpasbare opties waarmee u de kans op woordenboekaanvallen kunt verkleinen:

- Account uitschakelen na N mislukte aanmeldingspogingen.
- Aantal mislukte aanmeldingen opnieuw instellen na N minuten.
- Account na N minuten opnieuw inschakelen.

8.8.6 Gebruikersbeperkingen

Gebruikersbeperkingen zorgen ervoor dat gebruikers die de standaard Enterprise-verificatie uitvoeren, regelmatig nieuwe wachtwoorden maken. U kunt de volgende opties inschakelen:

- Wachtwoord moet elke N dagen worden gewijzigd.
- Mag de laatste N wachtwoorden niet opnieuw gebruiken.
- Moet N minuten wachten om wachtwoord te wijzigen.

Deze opties hebben een aantal voordelen. Ten eerste moet een kwaadwillende gebruiker bij elke woordenboekaanval opnieuw beginnen nadat een wachtwoord is gewijzigd. En verder kan een kwaadwillende gebruiker niet gemakkelijk raden wanneer een bepaald wachtwoord wordt gewijzigd, aangezien wachtwoordwijzigingen zijn gekoppeld aan de eerste aanmelding. Bovendien, zelfs al heeft een kwaadwillende gebruiker de referenties van een andere gebruiker geraden of op een andere manier verkregen, dan zijn deze slechts gedurende een beperkte periode geldig.

8.8.7 Beperkingen voor de Guest-account

BI-platform ondersteunt anonieme eenmalige aanmelding voor de Guest-account. Als gebruikers dus verbinding maken met het BI-platform zonder een gebruikersnaam en wachtwoord op te geven, worden ze automatisch aangemeld met de Guest-account. Als u een beveiligd wachtwoord aan de Guest-account toewijst of als u de Guest-account helemaal uitschakelt, schakelt u deze standaardwerking uit.

8.9 Wijzigingen in de beveiligingsconfiguratie controleren

De wijzigingen in de volgende standaard beveiligingsconfiguraties zullen niet worden gecontroleerd door het BI-platform:

- Eigenschappenbestanden voor de webtoepassingen (BOE, webservices)
- TrustedPrincipal.conf
- Aanpassingen die zijn uitgevoerd via BI-startpunt en Open Document

Over het algemeen zullen alle wijzigingen in de beveiligingsconfiguratie die buiten de CMC zijn uitgevoerd niet worden gecontroleerd. Dit geldt tevens voor wijzigingen die buiten de Central Configuration Manager (CCM) zijn uitgevoerd. Wijzigingen die via de CMC zijn ingediend kunnen wel worden gecontroleerd.

8.10 Uitbreidingsmodules

Het BI-platform biedt u de mogelijkheid uw rapportageomgeving verder te beveiligen met aangepaste uitbreidingsmodules. Een programma-uitbreiding is een dynamisch geladen bibliotheek met code waarmee business logic wordt toegepast op bepaalde weergave- of planningsaanvragen in BI-platform voordat deze door het systeem worden verwerkt.

Door de ondersteuning voor programma-uitbreidingen stelt de beheer-SDK van BI-platform in feite een 'greep' beschikbaar waarmee ontwikkelaars een aanvraag kunnen ondervangen. Ontwikkelaars kunnen vervolgens selectieformules aan de aanvraag toevoegen voordat het rapport wordt verwerkt.

Zo wordt voor rapporten vaak een uitbreidingsmodule gebruikt waarmee beveiliging op rijniveau wordt afgedwongen. Bij dit type beveiliging wordt de toegang tot gegevens in een of meer databasetabellen per rij beperkt. De ontwikkelaar schrijft een dynamisch geladen bibliotheek waarmee weergave- of planningsaanvragen voor een rapport worden ondervangen (voordat de aanvragen worden verwerkt op de Job Server, verwerkingsserver of Report Application Server). De ontwikkelaar schrijft code waarmee eerst wordt bepaald welke gebruiker eigenaar is van de verwerkingstaak en waarmee vervolgens in een extern systeem wordt nagegaan welke rechten de gebruiker voor de toegang tot gegevens heeft. Met de code wordt vervolgens een recordselectieformule gegenereerd en aan het rapport toegevoegd om het aantal gegevens te beperken dat uit de database wordt opgehaald. In dit geval wordt de programma-uitbreiding gebruikt om aangepaste beveiliging op rijniveau in de BI-platformomgeving op te nemen.

Als u programma-uitbreidingen inschakelt, kunnen deze tijdens runtime dynamisch op de juiste serveronderdelen van BI-platform worden geladen. In de SDK vindt u een volledig gedocumenteerde API, die ontwikkelaars kunnen gebruiken om uitbreidingsmodules te schrijven. Zie de documentatie voor ontwikkelaars op de product-cd voor meer informatie.

8.11 Virusscaninterface

U kunt verschillende soorten bestanden (Adobe Acrobat, Microsoft Excel, Microsoft Word, Microsoft PowerPoint, Lumira, Crystal Reports, Web Intelligence enz.) via de CMC, het BI-startpunt, REST-webservices

en aangepaste SDK-toepassingen aan het BI-platform toewijzen. Deze bestanden worden onderworpen aan een groottecontrole (om ervoor te zorgen dat de bestandsgrootte niet nul is) en bevoegdheidscontrole op de doelmap. Met de introductie van Virusscaninterface in BI 4.2 SP4 worden de bestanden die u aan het BI-platform toewijst ook aan een virusscan onderworpen om ervoor te zorgen dat de inhoud van dergelijke bestanden niet geïnfecteerd en vrij van virussen is.

Bestanden worden onderworpen aan virusscan wanneer u:

- een nieuw bestand toevoegt
- een document opslaat als
- een document kopieert
- een object naar Postvak IN van BI verzendt
- een exemplaar van een document creëert
- of een willekeurige bewerking uitvoert die een nieuw bestand aan de File Repository Servers toewijst

> **Opmerking**
>
> Alleen bestanden die nieuw zijn toegewezen aan het Bi-platform in BI 4.2 SP$ (nadat u de virusscan hebt ingeschakeld) worden onderworpen aan een virusscan.

8.11.1 Virusscan inschakelen

U kunt virusscan inschakelen voor bestanden die aan het BI-platform zijn toegewezen voor zowel de Input als de Output File Repository Servers.

U hebt de Virusscanadapter (VSA)-bibliotheek van een SAP-gecertificeerde leverancier gedownload. Bezoek http://global.sap.com/community/ebook/2013_09_adpd/enEN/search.html#search=NW-VSI voor een lijst met SAP-gecertificeerde leveranciers.

> **Opmerking**
>
> Als u ondersteuning nodig hebt voor een nieuw platform of nieuwe leverancier, neem dan contact op met de leveranciers hierover.

Voer de volgende stappen uit om virusscan in de Input File Repository Server in te schakelen:

1. Meld u aan bij de CMC.
2. Navigeer naar *Servers* > *Lijst met servers*.
3. Klik met de rechtermuisknop op de Input File Repository Server en selecteer *Eigenschappen* uit de vervolgkeuzelijst.

   Het venster *Eigenschappen* wordt geopend.
4. Selecteer in de sectie *Input Filestore-service* het selectievakje *Virusscan inschakelen*.
5. Voer in het veld *Locatie van bestand voor adapter virusscan* het absolute pad naar het bibliotheekbestand van de virusscanadapter in.
6. Kies *Opslaan en sluiten*.

> **Opmerking**
>
> - Virusscan is standaard ingeschakeld voor alle bestanden die aan het BI-platform zijn toegevoegd in BI 4.2 SP4.
> - U kunt virusscan via de GUI of CLI inschakelen. Het opdrachtregelargument dat u in de File Repository Servers moet opgeven voor het inschakelen van virusscan is `vsaFileLoc`.
> - U kunt dezelfde stappen volgen voor het inschakelen van virusscan in de Output File Repository Server. Als u meerdere Input en Output File Repository Servers hebt, zorg er dan voor dat u virusscan op elke server installeert.
> - Om de wijzigingen van kracht te laten worden, moet u de File Repository Servers opnieuw starten nadat u virusscan hebt ingeschakeld.

8.12 Gegevensbeveiliging op het BI-platform

Beheerders van BI-platformsystemen beheren de beveiliging van vertrouwelijke gegevens als volgt:

- Een beveiligingsinstelling op clusterniveau die bepaalt welke toepassingen en clients toegang hebben tot de CMS. Deze instelling wordt beheerd via de Central Configuration Manager.
- Een cryptografiesysteem met twee sleutels dat toegang tot de CMS-gegevensopslagruimte regelt, en sleutels die gebruikt worden om objecten binnen de gegevensopslagruimte te coderen/decoderen. Toegang tot de CMS-gegevensopslagruimte wordt ingesteld via de Central Configuration Manager, terwijl de Central Management Console een specifiek beheergebied voor cryptografiesleutels heeft.

Met behulp van deze functies kunnen beheerders BI-platformimplementaties instellen op specifieke niveaus voor naleving van gegevensbeveiliging. Bovendien kunnen ze coderingssleutels beheren die worden gebruikt om gegevens in de CMS-gegevensopslagruimte te coderen en decoderen.

8.12.1 Beveiligingsmodi voor gegevensverwerking

Het BI-platform kent twee mogelijke modi voor beveiliging van gegevensverwerking:

- De standaardbeveiligingsmodus voor gegevensverwerking. In bepaalde omstandigheden gebruiken systemen in deze modus hardcoded-coderingssleutels en volgen ze niet een specifieke standaard. De standaardmodus biedt achterwaartse compatibiliteit met eerdere versies van clienthulpprogramma's en toepassingen van het BI-platform.
- Een gegevensbeveiligingsmodus die is ontworpen om aan de richtlijnen te voldoen die zijn voorgeschreven door de Federal Information Processing Standard (FIPS), in het bijzonder FIPS 140-2. In deze modus worden FIPS-compatibele algoritmen en cryptografiemodules gebruikt om vertrouwelijke gegevens te beschermen. Wanneer het platform in FIPS-compatibele modus wordt uitgevoerd, worden alle clienthulpprogramma's en toepassingen die niet aan FIPS-richtlijnen voldoen, automatisch uitgeschakeld. De clienthulpprogramma's en toepassingen van het platform zijn ontworpen om aan de standaard FIPS 140-2 te voldoen. Oudere clients en toepassingen werken niet wanneer het BI-platform in FIPS-compatibele modus wordt uitgevoerd.

De gegevensverwerkingsmodus is transparant voor systeemgebruikers. In beide beveiligingsmodi voor gegevensverwerking worden vertrouwelijke gegevens op de achtergrond gecodeerd en gedecodeerd door een interne coderings-engine.

Het is raadzaam de FIPS-compatibele modus in de volgende omstandigheden te gebruiken:

- Uw BI-platformimplementatie hoeft geen oude clienthulpprogramma's of toepassingen van het BI-platform te gebruiken of hiermee samen te werken.
- De standaarden en richtlijnen van uw organisatie voor de verwerking van gegevens staan het gebruik van hard-coded coderingssleutels niet toe.
- Uw organisatie is verplicht om vertrouwelijke gegevens te beveiligen volgens FIPS 140-2-reglementen.

De beveiligingsmodus voor gegevensverwerking wordt zowel in Windows als op UNIX-platformen ingesteld via de Central Configuration Manager. Alle knooppunten in een geclusterde omgeving moeten op dezelfde modus worden ingesteld.

8.12.1.1 FIPS-compatibele modus inschakelen op Windows

De FIPS-compatibele modus is standaard ingeschakeld wanneer het BI-platform wordt geïnstalleerd.

1. Klik op *Programma's* > *SAP Business Intelligence* > *SAP BusinessObjects BI-platform 4* > *Central Configuration Manager* om de CCM te starten.
2. Klik in de CCM met de rechtermuisknop op de SIA (Server Intelligence Agent) en kies *Stoppen*.

   > ⚠ Let op
   >
   > Ga pas door naar stap 3 als de SIA-status wordt aangeduid met Gestopt.

3. Klik met de rechtermuisknop op de SIA en selecteer *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt geopend met het tabblad *Eigenschappen* geselecteerd.
4. Voeg `-fips` toe aan het veld *Opdracht* en klik op *Toepassen*.
5. Klik op *OK* om het dialoogvenster *Eigenschappen* te sluiten.
6. Start de SIA opnieuw.

De SIA werkt nu in FIPS-compatibele modus.

U moet de FIPS-compatibele modus voor alle SIA's in uw BI-platformimplementatie inschakelen.

8.12.1.2 FIPS-compatibele modus inschakelen op UNIX

Alle knooppunten in uw implementatie van BI-platform moeten worden gestopt voordat u de volgende procedure uitvoert.

De FIPS-compatibele modus is standaard uitgeschakeld nadat het BI-platform is geïnstalleerd. Volg de onderstaande instructies om de FIPS-compatibele modus voor alle knooppunten in uw implementatie in te schakelen.

1. Via de map `<INSTALLATIEMAP>/sap_bobj` opent u het bestand `ccm.config` om het te bewerken.

2. Voeg `-fips` toe aan de startopdrachtparameter van het knooppunt.

   De startopdrachtparameter van het knooppunt wordt met de volgende indeling weergegeven: `<KNOOPPUNTNAAM>LAUNCH`. Voor een knooppunt met de naam “SAP” is de startopdrachtparameter van het knooppunt `SAPLAUNCH`.
3. Sla uw wijzigingen op en klik op *Afsluiten*.
4. Start het knooppunt opnieuw.

Het knooppunt werkt nu in FIPS-compatibele modus.

U moet de FIPS-compatibele modus voor alle knooppunten in uw implementatie van BI-platform inschakelen.

8.12.1.3 FIPS-compatibele modus uitschakelen op Windows

Alle servers in uw BI-platformimplementatie moeten worden gestopt voordat u de volgende procedure uitvoert.

Als uw implementatie in FIPS-compatibele modus wordt uitgevoerd, volgt u deze instructies op om de instelling uit te schakelen.

1. Klik in de CCM met de rechtermuisknop op de Server Intelligence Agent (SIA) en kies *Stoppen*.

   > ⚠ Let op
   >
   > Ga pas door naar stap 2 als de knooppuntstatus wordt aangeduid met *Gestopt*.

2. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven, waarbij het tabblad *Eigenschappen* is geopend.
3. Verwijder `-FIPS` uit het veld *Opdracht* en klik op *Toepassen*.
4. Klik op *OK* om het dialoogvenster *Eigenschappen* te sluiten.
5. Start de SIA opnieuw.

8.12.2 Beheerdersaccounts

Het BI-platform creëert automatisch een eerste beheerdersaccount. We raden u aan voor elke persoon een account in de groep Beheerders te creëren.

Aan de beheerder-gebruiker wordt automatisch het recht *Rechten wijzigen die gebruikers hebben voor objecten* toegewezen. Als u de beheerdersaccount hebt gemaakt, vergeet dan niet om de eerste beheerdersaccount uit te schakelen.

8.12.3 Verbindingsrechten

Standaard hebben beheerders toegang tot verbindingsgegevens, inclusief wachtwoorden, als de verbindingen zijn gedefinieerd met referenties.

In dit gedeelte wordt uitgelegd hoe het principe van de minste bevoegdheden moet worden toegepast op verbindingen als beheerders geen toegang mogen krijgen tot gegevensbronnen.

Het recht 'Verbinding lokaal downloaden' beperken

Het recht *Verbinding lokaal downloaden* is alleen strikt noodzakelijk voor gebruikers die de verbindingen beheren Verbindingsrechten [pagina 1146]). Het moet alleen aan individuele gebruikers worden toegekend, niet aan groepen. Als een groep het recht heeft, kan elke gebruiker die aan die groep is toegevoegd toegang krijgen tot de verbindingsgegevens.

Ga als volgt te werk om de verbindingen volledig te beveiligen:

1. Verleen het recht *Verbinding lokaal downloaden* aan gebruikers die de verbindingen beheren.
2. Weiger het recht *Verbinding lokaal downloaden* in de bovenste map van verbindingen voor de gebruikersgroepen Beheerders en Universeontwerpers.

Zie de onderstaande sectie om te voorkomen dat gebruikers zichzelf het recht toekennen.

De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen

Het standaardrecht *Rechten wijzigen die gebruikers hebben voor objecten* stelt gebruikers in staat een recht toe te kennen, zelfs als ze dat zelf niet hebben. Voor verbindingen moet dit worden vervangen door het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen*. Als beheerders niet beschikken over het recht *Verbinding lokaal downloaden*, mogen ze niet het recht hebben om dit aan andere gebruikers toe te kennen.

Op het hoogste niveau van de map Verbindingen:

1. Verleen de groepen Beheerders en Universeontwerpers het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen*.
2. Verleen het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* aan gebruikers die de verbindingen beheren zoals gedefinieerd in de vorige sectie. Zij hebben het recht om het recht *Verbinding lokaal downloaden* te verlenen.
3. Weiger de groepen Beheerders en Universeontwerpers het recht *Rechten wijzigen die gebruikers hebben voor objecten*.

8.13 Cryptografie in het BI-platform

Vertrouwelijke gegevens

Cryptografie in het BI-platform is ontworpen om vertrouwelijke gegevens te beschermen die worden bewaard in de CMS-gegevensopslagruimte. Vertrouwelijke gegevens zijn gebruikersreferenties, gegevens voor

gegevensbronverbindingen en andere informatieobjecten die wachtwoorden opslaan. Deze gegevens worden gecodeerd om privacy te waarborgen, ervoor te zorgen dat ze niet beschadigd raken en om toegangsbeheer te onderhouden. Alle vereiste coderingsbronnen (waaronder de coderings-engine, RSA-bibliotheken) worden standaard op elke implementatie van het BI-platform geïnstalleerd.

Het systeem van het BI-platform maakt gebruik van een cryptografiesysteem met twee sleutels.

Cryptografiesleutels

Codering en decodering van vertrouwelijke gegevens wordt op de achtergrond verwerkt door de SDK die met de interne coderings-engine communiceert. Systeembeheerders beheren gegevensbeveiliging via symmetrische coderingssleutels zonder specifieke gegevensblokken rechtstreeks te coderen of decoderen.

In het BI-platform worden symmetrische coderingssleutels (genaamd Cryptografiesleutels) gebruikt om vertrouwelijke gegevens te coderen/decoderen. De Central Management Console heeft een specifiek beheergebied voor cryptografiesleutels. Gebruik de *Cryptografiesleutels* om sleutels weer te geven, te genereren, te deactiveren, in te trekken en te verwijderen. Het systeem zorgt dat sleutels die vereist zijn om vertrouwelijke gegevens te decoderen, niet kunnen worden verwijderd.

Clustersleutels

Clustersleutels zijn symmetrische sleutels voor sleuteloverloop die cryptografiesleutels beschermen die worden bewaard in de CMS-gegevensopslagruimte. Via symmetrische sleutelalgoritmen regelen clustersleutels het niveau van toegangsbeheer voor de CMS-gegevensopslagruimte. Elk knooppunt in het BI-platform krijgt tijdens installatie een clustersleutel toegewezen. Systeembeheerders kunnen de CCM gebruiken om de clustersleutel opnieuw in te stellen.

8.13.1 Met clustersleutels werken

Tijdens de installatie van het BI-platform wordt er een clustersleutel van 8 tekens gemaakt voor de Server Intelligence Agent. Deze sleutel wordt gebruikt om alle cryptografiesleutels in de CMS-gegevensopslagruimte te coderen. Zonder de juiste clustersleutel krijgt u geen toegang tot de CMS.

De clustersleutel wordt gecodeerd opgeslagen in een `dbinfo`-bestand. De bestandsnaam `dbinfo` volgt deze conventie: `_boe_<sia_naam>.dbinfo`, waarbij `<sia_naam>` de naam is van de Server Intelligence Agent voor het cluster.

In Windows wordt het bestand in de volgende map opgeslagen: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

Op Unix-systemen wordt het bestand opgeslagen in de platformmap onder `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/`:

Unix-platform	Platformmap
AIX	`<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/aix_rs6000_64/`
Solaris	`<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64/`

> **Opmerking**
>
> U kunt de clustersleutel voor een knooppunt niet ophalen uit het bestand `dbinfo`. Het wordt systeembeheerders aangeraden weloverwogen en gedegen maatregelen te treffen om clustersleutels te beschermen.

Alleen gebruikers met beheerdersbevoegdheden kunnen clustersleutels opnieuw instellen. Indien vereist gebruikt u de CCM om de clustersleutel opnieuw in te stellen voor elk knooppunt in uw implementatie. Nieuwe clustersleutels worden automatisch gebruikt om de cryptografiesleutels in de CMS-gegevensopslagruimte te laten omlopen.

8.13.1.1 De clustersleutel opnieuw instellen op Windows

Voordat u de clustersleutel voor uw knooppunt opnieuw instelt, zorgt u dat alle servers die door de Server Intelligence Agent worden beheerd, zijn gestopt.

1. Ga naar *Programma's* > *SAP Business Intelligence* > *SAP BusinessObjects BI-platform 4* > *Central Configuration Manager* om de CCM te starten.
2. Klik in de CCM met de rechtermuisknop op de SIA (Server Intelligence Agent) en kies *Stoppen*.

   > **Let op**
   >
   > Ga pas door naar stap 3 als de SIA-status Gestopt is.

3. Klik met de rechtermuisknop op de Server Intelligence Agent (SIA) en kies *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Klik op het tabblad *Configuratie*.
5. Klik op *Wijzigen* onder *Configuratie van CMS-clustersleutel*.
   Er wordt een waarschuwingsbericht weergegeven.
6. Klik op *Ja* om verder te gaan.
   Het dialoogvenster *Clustersleutel wijzigen* wordt geopend.
7. Voer dezelfde achtcijferige sleutel in de velden *Nieuwe clustersleutel* en *Nieuwe clustersleutel bevestigen* in.

   > **Opmerking**
   >
   > In Windows moeten clustersleutels uit een combinatie van hoofdletters en kleine letters bestaan. Gebruikers kunnen ook een willekeurige sleutel genereren. Een willekeurige sleutel is vereist om FIPS-compatibel te zijn.

8. Klik op *OK* om de nieuwe clustersleutel bij het systeem in te dienen.
   Er wordt een bericht weergegeven dat de clustersleutel opnieuw is ingesteld.
9. Start de SIA opnieuw.

In een cluster met meerdere knooppunten moet u de clustersleutels voor alle SIA's in uw BI-platformimplementatie opnieuw instellen op de nieuwe sleutel.

8.13.1.2 De clustersleutel opnieuw instellen op UNIX

Voordat u de clustersleutel voor een knooppunt opnieuw instelt, moet u zorgen dat alle servers die door het knooppunt worden beheerd, zijn gestopt.

1. Navigeer naar de map `<INSTALLATIEMAP>/sap_bobj`.
2. Typ **`./cmsdbsetup.sh`** en druk op *Enter*.
   Het venster *Instellingen van CMS-database* wordt weergegeven.
3. Typ de naam van het knooppunt en druk op *Enter*.
4. Typ **2** om de clustersleutel te wijzigen.
   Er wordt een waarschuwingsbericht weergegeven.
5. Selecteer *Ja* om verder te gaan.
6. In het beschikbare veld typt u een nieuwe clustersleutel. Vervolgens drukt u op *Enter*.

   > **Opmerking**
   >
   > Zorg ervoor dat de sleutel minimaal zes tekens lang is en twee van de volgende typen tekens combineert: hoofdletters, kleine letters, cijfers of leestekens. U kunt bijvoorbeeld één kleine letter met een cijfer, een hoofdletter met een leesteken, enzovoort hebben.

7. Voer de nieuwe clustersleutel opnieuw in het opgegeven veld in en druk op *Enter*.
   Er wordt een bericht weergegeven dat de clustersleutel opnieuw is ingesteld.
8. Start het knooppunt opnieuw.

U moet alle knooppunten in uw implementatie van BI-platform opnieuw instellen zodat ze dezelfde clustersleutel gebruiken.

8.13.2 Cryptografie-operators

U moet lid zijn van de groep Cryptografie-operators om cryptografiesleutels in de CMC te kunnen beheren. De standaard beheerdersaccount die voor het BI-platform is aangemaakt, is ook lid van de groep Cryptografie-operators. Gebruik deze account om gebruikers naar wens toe te voegen aan de groep Cryptografie-operators. Het is raadzaam lidmaatschap van de groep te beperken tot een bepaald aantal gebruikers.

> **Opmerking**
>
> Wanneer gebruikers worden toegevoegd aan de groep Beheerders, nemen ze niet de rechten over die vereist zijn om beheertaken uit te voeren op cryptografiesleutels.

8.13.2.1 Een gebruiker toevoegen aan de groep Cryptografie-operators

Er moet een gebruikersaccount in het BI-platform aanwezig zijn voordat de account aan de groep Cryptografie-operators kan worden toegevoegd.

> **Opmerking**
>
> U moet lid zijn van de groepen *Beheerders* en *Cryptografie-operators* om een gebruiker aan de groep Cryptografie-operators te kunnen toevoegen.

1. Selecteer in het beheergebied *Gebruikers en groepen* van de CMC de groep *Cryptografie-operators*.
2. Klik op *Acties* > *Leden toevoegen aan groep*.
   Het dialoogvenster *Toevoegen* wordt weergegeven.
3. Klik op*Lijst met gebruikers*.
   De lijst *Beschikbare gebruikers of groepen* wordt vernieuwd, waarna daarin alle gebruikersaccounts in het systeem worden weergegeven.
4. Verplaats de gebruikersaccount die u aan de groep Cryptografie-operators wilt toevoegen, van de lijst *Beschikbare gebruikers of groepen* naar de lijst *Geselecteerde gebruikers of groepen*.

   > **→ Tip**
   >
   > Gebruik het vak Zoeken als u naar een specifieke gebruiker wilt zoeken.

5. Klik op *OK*.

Als lid van de groep Cryptografie-operators heeft de zojuist toegevoegde account toegang tot het beheergebied voor *Cryptografiesleutels* in de CMC.

8.13.2.2 Cryptografiesleutels weergeven in de CMC

De CMC-toepassing heeft een specifiek beheergebied voor cryptografiesleutels dat wordt gebruikt door het BI-platformsysteem. Toegang tot dit gebied is beperkt tot leden van de groep Cryptografie-operators.

1. Klik op *Programma's* > *SAP Business Intelligence* > *SAP BusinessObjects BI-platform 4* > *SAP BusinessObjects BI-platform Central Management Console* om de CMC te starten.
   De startpagina van CMC wordt geopend.
2. Klik op het tabblad *Cryptografiesleutel*.
   Het beheergebied *Cryptografiesleutels* wordt weergegeven.
3. Dubbelklik op de cryptografiesleutel waarvoor u meer details wilt bekijken.

Verwante informatie

Objecten weergeven die aan een cryptografiesleutel zijn gekoppeld [pagina 172]

8.13.3 Cryptografiesleutels beheren in de CMC

Cryptografie-operators gebruiken het beheergebied *Cryptografiesleutels* om sleutels te controleren, genereren, deactiveren, in te trekken en te verwijderen die worden gebruikt om vertrouwelijke gegevens te beschermen die in de CMS-gegevensopslagruimte worden bewaard.

Alle cryptografiesleutels die momenteel in het systeem zijn gedefinieerd, worden weergegeven in het beheergebied *Cryptografiesleutels*. Onder de koppen die in de volgende tabel worden beschreven, vindt u basisgegevens voor elke sleutel:

Kop	Beschrijving
Titel	Naam-id van de cryptografiesleutel
Status	De huidige status van de sleutel
Laatste statuswijziging	Datum- en tijdstempel voor de laatste wijziging die is uitgevoerd voor de cryptografiesleutel
Objecten	Aantal objecten dat aan de sleutel is gekoppeld

Verwante informatie

Status van cryptografiesleutel [pagina 171]
Een nieuwe cryptografiesleutel maken [pagina 173]
Een cryptografiesleutel verwijderen van het systeem [pagina 174]
Een cryptografiesleutel intrekken [pagina 174]
Objecten weergeven die aan een cryptografiesleutel zijn gekoppeld [pagina 172]
Cryptografiesleutels markeren als beschadigd [pagina 173]

8.13.3.1 Status van cryptografiesleutel

In de volgende tabel worden alle mogelijke statusopties voor cryptografiesleutels op het BI-platform weergegeven:

Status	Beschrijving
Actief	De status *Actief* kan aan slechts één cryptografiesleutel in het systeem worden toegewezen. Deze sleutel wordt gebruikt om huidige vertrouwelijke gegevens te coderen die in de CMS-database worden opgeslagen. De sleutel wordt ook gebruikt om alle objecten in de Lijst met objecten te decoderen. Wanneer er een nieuwe cryptografiesleutel is gemaakt, wordt de huidige status *Actief* teruggezet op *Gedeactiveerd*. U kunt een actieve sleutel niet uit het systeem verwijderen.

Status	Beschrijving
Gedeactiveerd	Een sleutel met de status *Gedeactiveerd* kan niet langer worden gebruikt om gegevens te coderen. U kunt de sleutel echter wel gebruiken om alle objecten te coderen die op de Lijst met objecten voorkomen. Wanneer een sleutel is gedeactiveerd, kunt u deze niet opnieuw activeren. Een sleutel die is gemarkeerd als *Gedeactiveerd* kan niet uit het systeem worden verwijderd. U moet de status van een sleutel eerst wijzigen in *Ingetrokken* voordat deze kan worden verwijderd.
Beschadigd	Een cryptografiesleutel die als onveilig wordt beschouwd, kan als beschadigd worden gemarkeerd. Wanneer u een dergelijke sleutel markeert, kunt u later gegevensobjecten opnieuw coderen die nog aan deze sleutel zijn gekoppeld. Wanneer een sleutel wordt gemarkeerd als beschadigd, moet deze eerst met de status Ingetrokken worden gemarkeerd alvorens de sleutel van het systeem kan worden verwijderd.
Ingetrokken	Wanneer een cryptografiesleutel wordt ingetrokken, wordt er een proces gestart waarin alle objecten die momenteel aan de sleutel zijn gekoppeld, opnieuw worden gecodeerd met de cryptografiesleutel die momenteel de status Actief heeft. Wanneer een sleutel is ingetrokken, kan deze veilig van het systeem worden verwijderd. Dankzij de intrekkingsmethode kunnen gegevens in de CMS-database altijd worden gedecodeerd. Wanneer een sleutel is ingetrokken, kan deze niet opnieuw worden geactiveerd.
Gedeactiveerd: opnieuw versleutelen in voortgang	Hiermee wordt aangegeven dat de cryptografiesleutel op dit moment wordt ingetrokken. Zodra het proces is voltooid, wordt de sleutel gemarkeerd met *Ingetrokken*.
Gedeactiveerd: opnieuw versleutelen uitgesteld	Hiermee wordt aangegeven dat het proces voor het intrekken van een cryptografiesleutel is uitgesteld. Dit gebeurt meestal wanneer het proces opzettelijk is uitgesteld of als een gegevensobject dat aan de sleutel is gekoppeld, niet beschikbaar is.
Ingetrokken-beschadigd	Een sleutel wordt gemarkeerd met Ingetrokken-beschadigd als de sleutel is gemarkeerd als beschadigd en alle gegevens die voorheen aan de sleutel waren gekoppeld, met een andere sleutel zijn gecodeerd. Wanneer een *gedeactiveerde* sleutel is gemarkeerd als beschadigd, kunt u kiezen om geen actie te ondernemen of de sleutel in te trekken. Wanneer een beschadigde sleutel is ingetrokken, kan deze worden verwijderd.

8.13.3.2 Objecten weergeven die aan een cryptografiesleutel zijn gekoppeld

1. Selecteer de sleutel in het beheergebied *Cryptografiesleutels* van de CMC.

2. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* van de cryptografiesleutel wordt geopend.
3. Klik op *Lijst met objecten* in het navigatievenster aan de linkerkant van het dialoogvenster *Eigenschappen*.
   Alle objecten die aan de cryptografiesleutel zijn gekoppeld, worden aan de rechterkant van het navigatievenster weergegeven.

   > → Tip
   >
   > Gebruik de zoekfuncties om naar een specifiek object te zoeken.

8.13.3.3 Een nieuwe cryptografiesleutel maken

> ⚠ Let op
>
> Wanneer u een nieuwe cryptografiesleutel maakt, wordt de *actieve* sleutel automatisch door het systeem gedeactiveerd. Als een sleutel is gedeactiveerd, kan deze niet worden hersteld als de *actieve* sleutel.

1. In het beheergebied *Cryptografiesleutels* van de CMC klikt u op *Beheren* > *Nieuw* > *Cryptografiesleutel*.
   Het dialoogvenster *Nieuwe cryptografiesleutel maken* wordt weergegeven.
2. Klik op *Doorgaan* om de nieuwe cryptografiesleutel te maken.
3. Typ een naam en een beschrijving voor de nieuwe cryptografiesleutel. Klik op *OK* om de gegevens op te slaan.
   De nieuwe sleutel wordt weergegeven als de enige actieve sleutel in het beheergebied *Cryptografiesleutels*.
   De voorgaande *actieve* sleutel wordt nu gemarkeerd als *Gedeactiveerd*.

Alle nieuwe vertrouwelijke gegevens die worden gegenereerd en opgeslagen in de CMS-database, worden nu gecodeerd met de nieuwe cryptografiesleutel. U kunt de vorige sleutel intrekken en alle bijbehorende gegevensobjecten opnieuw coderen met de nieuwe actieve sleutel.

8.13.3.4 Cryptografiesleutels markeren als beschadigd

U kunt een cryptografiesleutel markeren als beschadigd als deze niet langer als veilig wordt beschouwd. Dit is nuttig wanneer u een sleutel wilt traceren, en u kunt vervolgens identificeren welke gegevensobjecten aan de sleutel zijn gekoppeld. Een cryptografiesleutel moet worden gedeactiveerd voordat u deze kunt markeren als beschadigd.

> ⓘ Opmerking
>
> U kunt een sleutel ook markeren als beschadigd wanneer deze is ingetrokken.

1. Ga naar het beheergebied *Cryptografiesleutels* van de CMC.
2. Selecteer de cryptografiesleutel die u wilt markeren als beschadigd.
3. Klik op *Acties* > *Als beschadigd markeren*.
   Het dialoogvenster *Als beschadigd markeren* wordt weergegeven.

4. Klik op *Doorgaan*.
5. Selecteer een van de volgende opties in het dialoogvenster *Als beschadigd markeren*:
   - *Ja*: hiermee wordt het proces gestart om alle gegevensobjecten die aan de beschadigde sleutel zijn gekoppeld, opnieuw te coderen.
   - *Nee*: het dialoogvenster *Als beschadigd markeren* wordt gesloten en de cryptografiesleutel wordt gemarkeerd als *Beschadigd* in het beheergebied *Cryptografiesleutels*.

   > **Opmerking**
   >
   > Als u *Nee* selecteert, blijven vertrouwelijke gegevens gekoppeld aan de beschadigde sleutel. De beschadigde sleutel wordt door het systeem gebruikt om de gekoppelde objecten te decoderen.

Verwante informatie

Een cryptografiesleutel intrekken [pagina 174]
Status van cryptografiesleutel [pagina 171]
Objecten weergeven die aan een cryptografiesleutel zijn gekoppeld [pagina 172]

8.13.3.5 Een cryptografiesleutel intrekken

Een gedeactiveerde cryptografiesleutel kan nog steeds gebruikt worden door gegevensobjecten die eraan zijn gekoppeld. U verbreekt de koppeling tussen de gecodeerde objecten en de gedeactiveerde sleutel door de sleutel in te trekken.

1. Selecteer de sleutel die u wilt intrekken, in de lijst met sleutels die wordt weergegeven in het beheergebied *Cryptografiesleutels*.
2. Klik op *Acties* > *Intrekken*.
   Het dialoogvenster *Intrekken* wordt weergegeven.
3. Klik op *OK*.
   Er wordt een proces gestart om alle objecten van de sleutel met de huidig actieve sleutel te coderen. Als de sleutel aan meerdere gegevensobjecten is gekoppeld, wordt de sleutel gemarkeerd met *Gedeactiveerd: opnieuw coderen in voortgang* tot het hercoderingsproces voltooid is.

Wanneer een cryptografiesleutel is ingetrokken, kan deze veilig worden verwijderd van het systeem, aangezien er geen vertrouwelijke gegevensobjecten zijn die de sleutel nodig hebben voor decodering.

8.13.3.6 Een cryptografiesleutel verwijderen van het systeem

Voordat u een cryptografiesleutel van het BI-platformsysteem verwijdert, moet u controleren of er geen gegevensobjecten op het systeem staan die de sleutel nodig hebben. Deze beperking waarborgt dat alle vertrouwelijke gegevens die in de CMS-gegevensopslagruimte worden opgeslagen, altijd gecodeerd kunnen worden.

Nadat u een cryptografiesleutel hebt ingetrokken, voert u de onderstaande instructies uit om de sleutel van het systeem te verwijderen.

1. Ga naar het beheergebied *Cryptografiesleutels* van de CMC.
2. Selecteer de cryptografiesleutel die u wilt verwijderen.
3. Klik op *Beheren* > *Verwijderen*.
   Het dialoogvenster *Verwijderen* wordt weergegeven.
4. Klik op *Verwijderen* om de cryptografiesleutel van het systeem te verwijderen.
   De verwijderde sleutel wordt niet langer weergegeven in het beheergebied *Cryptografiesleutels* van de CMC.

> **Opmerking**
>
> U kunt een cryptografiesleutel die van het systeem is verwijderd, niet herstellen.

Verwante informatie

Een cryptografiesleutel intrekken [pagina 174]
Status van cryptografiesleutel [pagina 171]

8.14 Gegevensbeveiliging en privacy

Gegevensbeveiliging is geassocieerd aan talloze wettelijke vereisten en privacygevoeligheid. Naast conformiteit met toepasselijke regels over privacy van gegevens, moet er rekening worden gehouden met specifieke wetgeving voor de bedrijfstak in verschillende landen. SAP biedt specifieke onderdelen en functies om conformiteit met betrekking tot wettelijke vereisten te ondersteunen, inclusief gegevensbeveiliging. SAP geeft geen advies over of deze onderdelen en functies de beste methode zijn om bedrijfsspecifieke, bedrijfstakspecifieke, regionale of landspecifieke vereisten te ondersteunen. Verder geeft deze informatie geen advies of aanbeveling met betrekking tot aanvullende onderdelen die in specifieke IT-omgevingen vereist zouden zijn. Beslissingen gerelateerd aan gegevensbeveiliging moeten per geval worden bekeken waarbij rekening wordt gehouden met de specifieke systeemconstellatie en de geldende wettelijke vereisten.

> **Opmerking**
>
> In de meeste gevallen zal conformiteit met toepasselijke gegevensbeveiliging en privacywetten niet door een productonderdeel worden gedekt. SAP-software ondersteunt conformiteit door het aanbieden van beveiligingsonderdelen en specifieke functies die relevant zijn voor gegevensbeveiliging, zoals vereenvoudigde blokkering en verwijdering van persoonlijke gegevens. SAP biedt geen in geen enkel opzicht juridisch advies. Definities en andere termen die in dit document zijn gebruikt, zijn niet overgenomen uit een bepaalde juridische bron.

8.14.1 Woordenlijst

Begrip	Definitie
Persoonlijke gegevens	Alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon ("gegevensonderwerp"). Een identificeerbare persoon is een persoon die, direct of indirect, kan worden geïdentificeerd, met name door te refereren aan een id zoals een naam, een identificatienummer, locatiegegevens, een online-id of aan een of meerdere factoren die specifiek zijn voor de fysieke, fysiologische, genetische, mentale, economische of sociale identiteit van die natuurlijke persoon.
Doel	Een wettelijke, contractuele, of in andere vorm gerechtvaardigde reden voor de verwerking van **persoonlijke gegevens**. De aanname is dat elk doel een einde heeft dat meestal al is gedefinieerd wanneer het doel begint.
Blokkeren	Een methode van het beperken van toegang tot gegevens waarvoor het primaire **zakelijke doel** is beëindigd.
Verwijderen	De onherstelbare vernietiging van **persoonlijke gegevens**.
Periode gegevensopslag	De tijdsperiode tussen het einde van het gebruiksdoel (EoP) voor een gegevensset en wanneer deze gegevensset wordt verwijderd onderhevig aan toepasselijke wetten. Het is een combinatie van de verblijfsperiode en de blokkeerperiode.
Einde van gebruiksdoel (EoP)	Een methode van het identificeren van het tijdstip voor een gegevensset wanneer de verwerking van **persoonlijke gegevens** niet meer vereist is voor het primaire **zakelijke doel**. Nadat de **EoP** is bereikt, worden de gegevens **geblokkeerd** en alleen gebruikers met speciale verificatie hebben toegang tot de gegevens (zoals auditors).

Begrip	Definitie
Gevoelige persoonlijke gegevens	Een categorie van persoonlijke gegevens die meestal de volgende soort informatie bevat: • Speciale categorieën van persoonlijke gegevens zoals gegevens die ras of etnische afkomst, politieke meningen, geloofs- of levensbeschouwelijke overtuigingen of vakbondslidmaatschap prijsgeven en de verwerking van genetische gegevens, biometrische gegevens, gegevens over gezondheid of seksueel gedrag of seksuele geaardheid. • Persoonlijke gegevens onderhevig aan professionele geheimhouding. • Persoonlijke gegevens gerelateerd aan criminele of administratieve overtredingen. • Persoonlijke gegevens met betrekking tot verzekeringen of creditcardrekeningen.
Verblijfsperiode	De tijdsperiode na het einde van gebruiksdoel (EoP) voor een gegevensset tijdens welke de gegevens in de database blijven en kunnen worden gebruikt in geval van volgende processen gerelateerd aan het oorspronkelijke doel. Aan het einde van de langste geconfigureerde verblijfsperiode worden de gegevens geblokkeerd of verwijderd. De verblijfsperiode maakt deel uit van de algehele periode gegevensopslag.
Controle gebruiksinformatie (WUC)	Een proces dat is ontworpen om gegevensintegriteit te garanderen in het geval van potentieel blokkeren van gegevens van zakenpartners. De controle gebruiksinformatie (WUC) van een toepassing bepaalt of er afhankelijke gegevens voor een bepaalde zakenpartner in de database zijn. Als er afhankelijke gegevens zijn, betekent dit dat de gegevens nog steeds vereist zijn voor zakelijke activiteiten. Daarom wordt het blokkeren van zakenpartners gerefereerd in de gegevens voorkomen.
Toestemming	De actie van het gegevensonderwerp die bevestigt dat het gebruik van zijn of haar persoonlijke gegevens voor een bepaald doel zal worden toegestaan. Een toestemmingsfunctionaliteit staat de opslag van een toestemmingsrecord in verband met een specifiek gebruiksdoel toe en geeft weer of een gegevensonderwerp toestemming heeft verleend, ingetrokken of geweigerd.

8.14.2 Gebruikerstoestemming

SAP-toepassingen vragen om toestemming van de gebruiker voordat ze persoonlijke gegevens verzamelen. SAP BusinessObjects Business Intelligence-platform biedt functionaliteit die gegevensonderwerpen toestaat om toestemming te geven om hun persoonlijke gegevens te verzamelen en verwerken. SAP gaat ervan uit dat de gebruiker, bijvoorbeeld een SAP-klant die gegevens verzamelt, toestemming heeft van zijn gegevensonderwerp (een natuurlijke persoon zoals een klant, contactpersoon of account) om gegevens te verzamelen of naar de oplossing over te dragen.

> ⓘ Opmerking
>
> *Bericht gebruikerstoestemming*
>
> Dit product bevat open en vrij configureerbare invoervelden die niet bedoeld zijn om persoonlijke gegevens op te slaan zonder aanvullende technische en organisatorische maatregelen om gegevensbescherming en privacy te waarborgen.

8.14.3 Informatierapport

Iedere persoon heeft het recht om bevestiging te ontvangen over of wel of niet persoonlijke gegevens betreffende hem of haar worden verwerkt. In SAP BusinessObjects Business Intelligence-platform is het mogelijk om alle informatie weer te geven die over een bepaald gegevensonderwerp zijn opgeslagen.

Raadpleeg de sectie 'Accessing your info' in de *Fiorified Business Intelligence Launch Pad User Guide* op SAP Help Portal voor meer informatie over hoe een gebruiker toegang krijgt tot informatie die is opgeslagen over het gevensonderwerp.

> ⓘ Opmerking
>
> Lokaal opgeslagen documenten zijn niet beveiligd door SAP BusinessObjects Business Intelligence-platform. Beveiliging moet worden ingesteld door het betreffende apparatenbeheer (bijv. toegangscontrole, encryptie enz.)

8.14.4 Verslaglegging van leestoegang

Verslaglegging van leestoegang (RAL) wordt gebruikt om leestoegang tot gevoelige gegevens te bewaken en in een verslag op te nemen. Deze gegevens kunnen als gevoelig zijn gecategoriseerd door de wet, door extern ondernemingsbeleid of door intern ondernemingsbeleid. Deze algemene vragen kunnen van belang zijn voor een toepassing die gebruikmaakt van verslaglegging van leestoegang:

- Wie heeft toegang gehad tot de gegevens van een bepaald bedrijfsonderdeel, bijvoorbeeld een bankrekening?
- Wie heeft toegang gehad tot persoonlijke gegevens, bijvoorbeeld van een zakenpartner?
- Welke werknemer heeft toegang gehad tot persoonlijke informatie, bijvoorbeeld religie?
- Welke gebruikers hebben toegang gehad tot welke accounts of zakenpartners?

Deze vragen kunnen worden beantwoord met behulp van informatie over wie binnen een opgegeven tijdsbestek tot bepaalde gegevens toegang heeft gehad. Technisch gezien betekent dit dat alle remote API- en UI-infostructuren (die toegang hebben tot de gegevens) voor verslaglegging moeten worden geactiveerd.

SAP BusinessObjects BI-platform identificeert en verwerkt geen gevoelige persoonsgegevens en slaat deze niet op. Leestoegang tot gegevens wordt om die reden niet vastgelegd in BI-platform.

8.14.5 Verwijderen van persoonlijke gegevens

- Vereenvoudigd blokkeren en verwijderen: Naast conformiteit met toepasselijke regels over privacy van gegevens, moet er rekening worden gehouden met specifieke wetgeving voor de bedrijfstak in verschillende landen. Een typisch potentieel scenario in bepaalde landen is dat persoonlijke gegevens zullen worden verwijderd nadat het opgegeven, expliciete en legitieme gebruiksdoel voor de verwerking van persoonlijke gegevens is beëindigd, maar alleen indien er geen andere perioden voor gegevensopslag zijn gedefinieerd in wetgeving, zoals verblijfsperioden voor financiële documenten. Wettelijke voorschriften in bepaalde scenario's of landen vereisen vaak ook het blokkeren van gegevens waar de opgegeven, expliciete en legitieme gebruiksdoelen voor de verwerking van deze gegevens is beëindigd, maar de gegevens moeten in de database worden bewaard vanwege andere wettelijk gedefinieerde perioden voor gegevensopslag. In sommige scenario's omvatten persoonlijke gegevens ook gerefereerde gegevens. Daarom is de uitdaging voor verwijderen en blokkeren om eerst de gerefereerde gegevens te verwerken en daarna alle andere gegevens, zoals gegevens van zakenpartners.
- Verwijderen van persoonlijke gegevens: De verwerking van persoonlijke gegevens is onderworpen aan toepasselijke wetten die gerelateerd zijn aan het verwijderen van dergelijke gegevens aan het einde van het gebruiksdoel (EoP). Als er niet langer een legitiem gebruiksdoel is dat het gebruik van persoonlijke gegevens vereist, moeten deze worden verwijderd. Wanneer gegevens in een gegevensset worden verwijderd, moeten alle gerefereerde objecten die gerelateerd zijn aan die gegevensset ook worden verwijderd. Het is ook nodig om rekening te houden met bedrijfstakspecifieke wetgeving in verschillende landen naast algemene wetten voor gegevensbeveiliging. Nadat de langste periode voor gegevensopslag is vervallen, moeten de gegevens worden verwijderd.

Persoonlijke gegevens in SAP BusinessObjects BI-platform verwijderen

SAP BusinessObjects BI-platform en de clients ervan identificeren en categoriseren gegevens (uit gegevensbronnen voor analyse en rapportage) niet in persoonsgegevens. Het voorschrift voor het ophalen van deze gegevens en transparantie moet worden beheerd door het systeem dat de gegevens bezit. Het verwijderen van gegevens is een standaardfunctionaliteit van het systeem dat de gegevens bezit. Daarnaast bieden SAP BusinessObjects BI-platform en de clients ervan functionaliteiten (live verbinding met gegevensbronnen) om de gegevens gesynchroniseerd te houden met het systeem dat de gegevens bezit.

Gebruikersgegevens die in het systeem worden verzorgd zijn toegankelijk voor de gebruikers zelf of voor gebruikers die geautoriseerd zijn om deze gegevens voor hen te beheren. Gebruikers die van identiteitsproviders (zoals Windows AD en LDAP) zijn geïmporteerd, blijven gesynchroniseerd en moeten in de identiteitsproviders worden verzorgd.

Enterprise-gebruikers die in SAP BusinessObjects BI-platform zijn gemaakt, kunnen worden verwijderd of uitgeschakeld door gebruikers die geautoriseerd zijn om deze gegevens voor hen te beheren. In dit geval wordt

de gegevensopslag geconfigureerd door de gebruikers uit te schakelen in het systeem. Na de periode voor gegevensopslag kunnen deze gebruikers handmatig worden verwijderd uit het systeem door de gebruikers die geautoriseerd zijn om deze gegevens voor hen te beheren.

Wanneer u een gebruikersaccount verwijdert, worden ook de map Favorieten, de persoonlijke categorieën en het Postvak IN voor die gebruiker verwijderd. De verantwoordelijkheid voor de onderdelen in de openbare map wordt overgeheveld van de verwijderde gebruiker naar de beheerder. Let op: voor de uitgeschakelde gebruiker moet dit handmatig worden uitgevoerd door de gebruikers die geautoriseerd zijn om deze gegevens voor hen te beheren.

De gebruikersobject-id wordt tevens opgeslagen in de controle- en de commentaardatabase. Dit gebeurt echter niet op het moment dat er gebruikers worden verwijderd. De gebruikers-id in controlelogboekbestanden is vereist voor juridische en beveiligingsdoeleinden. Commentaar dat door gebruikers wordt toegevoegd, is vereist voor zakelijke doeleinden en moet dus worden bewaard als gesprekshistorie. Commentaar behoort geen persoonsgegevens te bevatten aangezien de gebruiker van tevoren wordt gevraagd geen persoonsgegevens in te voeren in openstaande velden.

Controle- en commentaardatabasegegevens kunnen handmatig worden verwijderd door gemachtigde gebruikers.

Zie Een gebruikersaccount wijzigen [pagina 103] voor meer informatie over hoe u een gebruiker uitschakelt.

Zie Toepassingsinstellingen beheer BI Commentary [pagina 721] voor meer details over hoe commentaargegevens van gebruikers kunnen worden verwijderd.

8.14.6 Wijzigingsverslag

Wijzigingsverslag in SAP BusinessObjects Business Intelligence-platform verwerkt persoonlijke gegevens van zakenpartners die betrokken zijn bij wijzigingsaanvragen en -activiteiten. Als er wijzigingen worden aangebracht met betrekking tot de zakenpartner, legt het systeem de volgende informatie vast over persoonlijke gegevens per wijzigingsaanvraag en -activiteit:

- De gebruiker die de gegevens heeft gewijzigd
- Datum en tijd van de wijziging
- Het type wijziging (update, invoeging, verwijderen, documentatie afzonderlijk veld)
- De identificerende sleutels en hun waarden van de gegevensrecords
- De oude en de nieuwe waarde van het attribuut dat is gewijzigd
- De kopnaam voor het attribuut dat is gewijzigd

U kunt de in het verslag op te nemen velden definiëren.

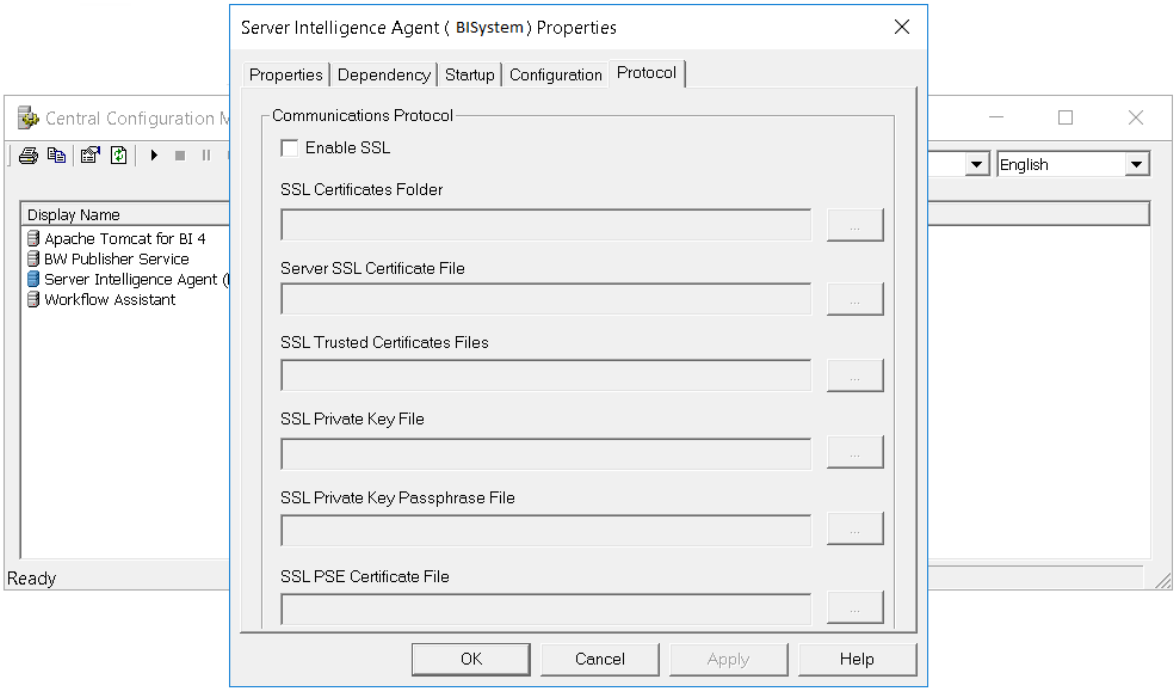
Raadpleeg voor meer informatie over logboeken voor gebruikersaccountupdates eventtype-id: 1007 in Audit events and details [pagina 909].

8.15 Back-endservers configureren voor SSL

U kunt het SSL-protocol (Secure Sockets Layer) gebruiken voor alle netwerkcommunicatie tussen BI-clients en BI-servers in uw implementatie van BI-platform.

Als u SSL wilt instellen voor alle servercommunicatie, moet u de volgende stappen uitvoeren:

- Het BI-platform implementeren met SSL ingeschakeld.
- Key- en certificaatbestanden maken voor elke computer in uw implementatie.
- De locatie van deze bestanden configureren in de Central Configuration Manager (CCM) en uw webtoepassingsserver.
- U kunt SSL ook configureren voor certificaten die zelfondertekend zijn of door een certificeringsinstantie worden beheerd.



> **Opmerking**
>
> Als u thick clients gebruikt, zoals Crystal Reports, moet u hiervoor SSL configureren als u verbinding maakt met de CMS. Als u dit niet doet, treden er fouten op wanneer u verbinding probeert te maken met een CMS die is geconfigureerd voor SSL vanuit een thick-client die niet op dezelfde manier is geconfigureerd.

8.15.1 Het standaardconfiguratiebestand maken

U kunt een standaardconfiguratiebestand maken om niet steeds dezelfde waarden te hoeven invoeren tijdens het genereren van certificaten of certificaatondertekeningsverzoeken.

> **Opmerking**
>
> U moet de onderstaande regels volgen tijdens het maken van het standaardconfiguratiebestand.
>
> - U moet de waarden aan de linkerkant toevoegen, zoals hieronder wordt vermeld.
> - De waarden aan de linkerkant zijn hoofdlettergevoelig.
> - Er mag maar één spatie zijn tussen een waarde en het teken 'gelijk aan' (=). Er is bijvoorbeeld maar één spatie tussen *CA_Common_Name* en het teken 'gelijk aan'.
> - U moet ervoor zorgen dat er geen spatie volgt na de waarden aan de rechterkant.

Volg de onderstaande stappen uit om een standaardconfiguratiebestand te maken met de naam **Name.cnf**:

1. Open een nieuw document in een teksteditor.
2. Voeg de waarden toe zoals hieronder wordt aangegeven:

```
CA_Common_Name = rootnm
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. Sla het bestand op met de naam **Name.cnf** op `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows en `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64` in de Unix-omgeving.

8.15.2 Key- en certificaatbestanden maken

Als u het SSL-protocol wilt instellen voor uw servercommunicatie, gebruikt u het opdrachtregelprogramma GENPSE om een key-bestand en een certificaatbestand te maken voor elke computer in uw implementatie.

> **Opmerking**
>
> U moet certificaten opnieuw maken voor alle computers in de implementatie, met inbegrip van computers waarop thick-clientonderdelen, zoals Crystal Reports, worden uitgevoerd. Gebruik het opdrachtregelprogramma `sslconfig` om deze clientcomputers te configureren.

> **Opmerking**
>
> Voor een maximale beveiliging moeten alle privé-sleutels zijn beveiligd en mogen deze sleutels niet worden verzonden via onbeveiligde communicatiekanalen.

8.15.2.1 Key- en certificaatbestanden maken voor een computer

Deze sectie gaat over het genereren van zelfondertekende keys en certificaten die vereist zijn voor het beveiligen van de communicatie tussen servers, of server en client. U kunt de certificaten genereren met behulp van het hulpprogramma GENPSE, een opdrachtregelprogramma voor het uitvoeren van verschillende taken die gerelateerd zijn aan de openbare key-infrastructuur. Het hulpprogramma GENPSE wordt gebruikt om X.509-certificaten, certificaatondertekeningsverzoeken en PSE-bestanden te genereren die worden gebruikt in de CORBA SSL-workflow. Het programma is gebaseerd op de cryptografische bibliotheek **CommonCryptoLib** van SAP en biedt ondersteuning voor het SHA-2-hashingmechanisme.

Volg de onderstaande stappen om de vereiste certificaten voor beveiligde communicatie te maken:

> **Opmerking**
>
> U kunt het standaardconfiguratiebestand **Name.cnf** maken met de standaardwaarden voor de gegevens die worden gevraagd tijdens het genereren van certificaten. Als u het standaardconfiguratiebestand gebruikt, hoeft u niet telkens dezelfde gegevens in te vullen voor elk certificaat. Raadpleeg Het standaardconfiguratiebestand maken [pagina 181] voor meer informatie.

1. Ga naar `<INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows en `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64` in Unix.
2. Voer de volgende opdracht uit:
   - In Windows: `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - In Unix: `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

   Raadpleeg de onderstaande tabel voor informatie over de opdracht:

Opdracht	Functie
GenPSE.exe of GenPSE.sh	Het hulpprogramma voor cryptografie starten
selfsigned	Zelfondertekende certificaten genereren
<Name.pse>	Bestandsnaam server-PSE
<Name.der>	Bestandsnaam servercertificaat
<root Cert.der>	Certificaatnaam certificeringsinstantie
<Name.key>	Bestandsnaam privé-key server
<private key password.txt>	Wachtwoordzin voor openbaar keybestand server
< path to Name.cnf >	Bestandspad van het standaardconfiguratiebestand

3. Voer de volgende gegevens in om de hoofdcertificeringsinstantie, de server en het clientcertificaat te genereren.

- *Landnaam*
- *Naam staat of provincie*
- *Locatienaam*
- *Organisatienaam*
- *Naam organisatie-eenheid*
- *Voer uw naam in*
- *Algemene naam*
- *E-mailadres*
- *Voer de vervaldatum in de indeling JJMMDD in*

4. Uw PSE-bestanden en de certificaten worden gegenereerd en opgeslagen op `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows en `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64` in Unix.

> → Tip
>
> Tijdens het genereren van een gebruikerscertificaat is er een aanvullende parameter *User Certificate type* (Type gebruikerscertificaat) waarmee het hulpprogramma het certificaat voor server- of clientverificatie kan identificeren en maken. Momenteel heeft de keuze die wordt gemaakt voor deze parameter geen effect op de CORBA SSL-instellingen.

> ⓘ Opmerking
>
> - De certificaatbestanden van de server-PSE en certificeringsinstantie moeten verschillende namen hebben.
> - De vervaldatum wordt ondersteund tot 2049.

8.15.3 SSL instellen wanneer het certificaat wordt beheerd door een certificeringsinstantie

U moet een certificaatondertekeningsverzoek genereren voor een externe certificeringsinstantie om de certificaten te ondertekenen. Het hulpprogramma GENPSE genereert een certificaatondertekeningsverzoek door eenvoudige opdrachten uit te voeren en de benodigde informatie te verstrekken als daarom wordt gevraagd.

Volg de onderstaande stappen om een certificaatondertekeningsverzoek te genereren:

> ⓘ Opmerking
>
> U kunt het standaardconfiguratiebestand `Name.cnf` maken met de standaardwaarden voor de gegevens die worden gevraagd tijdens het genereren van certificaten. Als u het standaardconfiguratiebestand gebruikt, hoeft u niet telkens dezelfde gegevens in te vullen voor elk certificaat. Raadpleeg Het standaardconfiguratiebestand maken [pagina 181] voor meer informatie.

1. Ga naar `<INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows en `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64` in Unix.
2. Voer de volgende opdracht uit:

- In Windows: `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
- In Unix: `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

Opdracht	Functie
GenPSE.exe of GenPSE.sh	Het hulpprogramma voor cryptografie starten
gencsr	Het certificaatondertekeningsverzoek genereren
<csrname.p10>	Bestandsnaam van certificaatondertekeningsverzoek
<Name.key>	Bestandsnaam privé-key server
<private key password.txt>	Wachtwoordzin voor openbaar key-bestand server
<path to Name.cnf>	Pad van het standaardconfiguratiebestand

3. Geef de volgende gegevens op:
   - *Voer de wachtwoordzin voor de privé-key in die moet worden ingesteld*
   - *Voer ter bevestiging de wachtwoordzin voor de privé-key opnieuw in*
   - *Landnaam*
   - *Naam staat of provincie*
   - *Locatienaam*
   - *Naam organisatie-eenheid*
   - *Algemene naam*
   - *E-mailadres*
4. Uw CSR-bestand in p10-formaat, de privésleutel van de server en het wachtwoordenbestand worden gegenereerd en opgeslagen in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` in Windows en `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64` in Unix. Het gegenereerde CSR-bestand wordt verzonden naar de certificeringsinstantie om een ondertekend certificaat te genereren.

8.15.3.1 Een pse-bestand genereren

Als uw certificaten worden beheerd door een externe certificeringsinstantie, moet u een PSE-bestand genereren. Volg de onderstaande stappen om een PSE-bestand te genereren:

1. Open `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Start een opdrachtregelconsole en voer `set SECUDIR=.` voor Windows en `export SECUDIR=.` voor Linux uit.
3. Voer `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>` uit.

   Raadpleeg de onderstaande tabel voor meer informatie over de opdracht:

Opdracht	Beschrijving
sapgenpse	Het hulpprogramma voor cryptografie starten
import_p8	Een nieuw PSE-bestand maken met een privésleutel in PKCS#8-formaat (optioneel bescherm met een op PKCS#5-wachtwoord gebaseerde encryptie), samen met alle X.509-certificaten.
-p <file_path_PSE>	Bestandspad van het nieuwe PSE-bestand.
-c <file_path_server_certificate>	Bestandspad van het servercertificaat.
-r <file_path_CA_certificate>	Bestandspad van het CA-certificaat.
-z <file_path_passphrase_text_file>	Bestandspad van het tekstbestand met wachtwoordzinnen.
<file_path_server_key>	Bestandspad van privésleutelbestand server.

Voorbeeld

sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key

4. Geef een leeg wachtwoord op door op Enter te drukken als om het wachtwoord wordt gevraagd.
5. Voeg de gebruikersreferenties aan het gemaakte pse-bestand toe.

→ Tip

Als SIA met account LocalSystem wordt uitgevoerd, moet u de volgende opdracht uitvoeren: `sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM` om de gebruikersreferenties aan het pse-bestand toe te voegen.

Opmerking

U kunt elke naam van uw keuze voor het pse-bestand gebruiken.

8.15.4 Het SSL-protocol configureren

Nadat u voor elke computer in uw implementatie sleutels en certificaten hebt gemaakt en deze op een beveiligde locatie hebt opgeslagen, moet u deze beveiligde locatie kenbaar maken aan de Central Configuration Manager (CCM) en uw webtoepassingsserver.

U moet ook specifieke stappen implementeren voor de configuratie van het SSL-protocol voor de webtoepassingsserver en voor elke computer waarop een thick client-toepassing wordt uitgevoerd.

FIPS in op Unix gebaseerd platform voor het configureren van SSL inschakelen

FIPS wordt standaard ingeschakeld voor een volledige installatie van 4.2 SP04 of een hogere versie maar u moet het handmatig inschakelen voor de hieronder vermelde scenario's:

- Patchupdate van 4.1 SPXX naar 4.2 SP04
- Patchupdate van 4.1 SPXX naar 4.2 SP02 of SP03 en later bijwerken naar 4.2 SP04

> **Opmerking**
>
> In Windows werkt CORBA SSL zelfs wanneer FIPS niet is ingeschakeld, terwijl het in op Unix gebaseerde platformen nodig is om ervoor te zorgen dat FIPS is ingeschakeld voor servers voordat CORBA SSL wordt geconfigureerd.

Stappen om FIPS in te schakelen:

- Ga naar `<INSTALLDIR>/sap_bobj.`
- Voer `./stopservers` uit
- Open het bestand ccm.config.
- Voeg de tekst '-FIPS' toe uit de eigenschappenlijst van het SIA-knooppunt.
- Voer `./startservers` uit

8.15.4.1 Het SSL-protocol configureren in de CCM

1. Klik in de CCM met de rechtermuisknop op de Server Intelligence Agent en kies *Eigenschappen*.
2. Klik in het dialoogvenster Eigenschappen op het tabblad *Protocol*.
3. Zorg dat *SSL inschakelen* is geselecteerd.
4. Geef het pad op voor de map waarin u de key- en certificaatbestanden hebt opgeslagen.

Veld	Beschrijving
Map met SSL-certificaten	Map waarin alle vereiste SSL-certificaten en -bestanden zijn opgeslagen. Bijvoorbeeld: `d:\ssl`
Bestand met SSL-certificaat voor server	Naam van het bestand waarin het SSL-certificaat voor de server wordt opgeslagen. Dit is standaard `servercert.der`
Bestand met vertrouwde SSL-certificaten	Naam van het bestand met het vertrouwde SSL-certificaat. Standaardnaam: `cacert.der`
Bestand met SSL-privésleutel	Naam van het SSL-privésleutelbestand dat gebruikt wordt om het certificaat op te roepen. Standaardnaam: `server.key`
Wachtwoordbestand met SSL-privésleutel	Naam van het tekstbestand met het wachtwoord voor toegang tot de privésleutel. Standaardnaam: `passphrase.txt`

Veld	Beschrijving
Bestand met pse-certificaat	Naam van het pse-bestand dat informatie bevat over de vertrouwde en servercertificaten.

> **Opmerking**
>
> Zorg ervoor dat u de map opgeeft voor de computer waarop de server wordt uitgevoerd.

8.15.4.2 Het SSL-protocol op Unix configureren

U moet het script `serverconfig.sh` gebruiken om het SSL-protocol voor een SIA te configureren. Voer het script uit om een tekstprogramma te starten waarmee u servergegevens kunt bekijken en servers kunt toevoegen aan of verwijderen uit uw installatie. Het script `serverconfig.sh` wordt geïnstalleerd in de map `sap_bobj` in uw installatie.

1. Met het script `ccm.sh` kunt u de SIA en alle SAP BusinessObjects-servers stoppen.
2. Voer het script `serverconfig.sh` uit.
3. Selecteer *3 - Knooppunt wijzigen* en druk op `Enter`.
4. Geef de doel-SIA op en druk op `Enter`.
5. Selecteer *1 - SSL-configuratie van Server Intelligence Agent wijzigen*.
6. Selecteer *ssl*.
   Geef de locaties van de SSL-certificaten op als u hierom wordt gevraagd.
7. Herhaal stap 1 t/m 6 voor elke SIA als uw BI-platformimplementatie een SIA-cluster is.
8. Start de SIA met het script `ccm.sh` en wacht tot de servers worden gestart.

8.15.4.3 Het SSL-protocol configureren voor de webtoepassingsserver

1. Als u een J2EE-webtoepassingsserver hebt, voert u de Java SDK uit met de volgende systeemeigenschappen ingesteld. Bijvoorbeeld:

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

   De volgende tabel bevat de beschrijvingen van deze voorbeelden:

Voorbeeld	Beschrijving
`<DcertDir>=d:\ssl`	De map waarin alle certificaten en sleutels worden opgeslagen.

Voorbeeld	Beschrijving
`<DtrustedCert>=cacert.der`	Vertrouwd certificaatbestand. Als u meerdere bestanden opgeeft, scheidt u deze door puntkomma's.
`<DsslCert>=clientcert.der`	Het certificaat dat door de SDK wordt gebruikt.
`<DsslKey>=client.key`	De privé-sleutel van het SDK-certificaat.
`<Dpassphrase>=passphrase.txt`	Het bestand waarin het wachtwoord voor de privé-sleutel wordt opgeslagen.
`<Dpsecert>=cert.pse`	Een PSE is een repository die keys en certificaten voor het beveiligen van communicatie bevat. Zie 3026364 voor meer informatie.

2. Als u een IIS-webtoepassingsserver hebt, voert u het hulpprogramma `sslconfig` uit vanaf de opdrachtregel en volgt u de configuratiestappen.

8.15.4.4 Thick-clients configureren

Voordat u de volgende procedure uitvoert, moet u alle vereiste SSL-bronnen (bijvoorbeeld certificaten en privésleutels) maken en opslaan in een bekende map.

In de onderstaande procedure wordt aangenomen dat u de instructies voor het maken van SSL-bronnen hebt gevolgd:

SSL-bron	
SSL-certificatenmap	`d:\ssl`
Naam van SSL-certificaatbestand voor server	`servercert.der`
Bestandsnaam van vertrouwd SSL-certificaat of hoofdcertificaat	`cacert.der`
Naam van SSL-privésleutelbestand	`server.key`
Bestand met wachtwoord voor toegang tot het SSL-privésleutelbestand	`passphrase.txt`
Naam van bestand met SSL pse-certificaat	cert.pse

Wanneer u de bovenstaande bronnen hebt gemaakt, gebruikt u de volgende instructies om thick-clienttoepassingen zoals de Central Configuration Manager (CCM) te configureren.

1. Controleer of de thick client-toepassing niet wordt uitgevoerd.

   > **Opmerking**
   >
   > Let op dat u de map opgeeft voor de computer waarop de server wordt uitgevoerd.

2. Voer het opdrachtregelprogramma `sslconfig.exe` uit. Let op dat u, afhankelijk van uw configuratie, het hulpprogramma uitvoert vanuit win32_x86 voor 32-bits clients of win64_x64 voor 64-bits clients.

Het hulpprogramma SSLC wordt met uw BI-platformsoftware geïnstalleerd. (In Windows wordt dit standaard geïnstalleerd in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

3. Typ de volgende opdracht:

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey
server.key
-passphrase     passphrase.txt -psecert cert.pse -protocol ssl
```

4. Start de thick client-toepassing opnieuw.

Verwante informatie

Key- en certificaatbestanden maken voor een computer [pagina 183]

8.15.4.4.1 SSL-aanmelding bij het hulpprogramma voor vertaalbeheer configureren

Als u wilt dat gebruikers zich met SSL kunnen aanmelden bij het hulpprogramma voor vertaalbeheer, moet informatie over de SSL-bronnen worden toegevoegd aan het configuratiebestand (`.ini`) van het hulpprogramma.

1. Zoek het bestand `TransMgr.ini`in de volgende map: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. Open het bestand `TransMgr.ini` in een teksteditor.
3. Voeg de volgende parameters toe:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Sla het bestand op en sluit de teksteditor af.

Gebruikers hebben nu via SSL toegang tot het hulpprogramma voor vertaalbeheer.

8.15.4.4.2 SSL configureren voor hulpprogramma van rapportconversie

RCT is uit gebruik genomen in de BI 4.3-release. Zie **2801797** voor meer informatie.

8.16 Communicatie tussen BI-platformonderdelen begrijpen

Als uw gehele BI-platformsysteem zich in één beveiligd subnet bevindt, is er geen speciale configuratie van de firewalls nodig. Het kan echter zijn dat u bepaalde onderdelen op verschillende subnetten wilt implementeren, gescheiden door één of meer firewalls.

Het is van belang om goed inzicht te hebben in de communicatie tussen BI-platformservers, Rich Clients en de webtoepassingsserver die als host dient voor de SAP BusinessObjects SDK, voordat u uw systeem configureert voor firewalls.

Verwante informatie

Het BI-platform voor firewalls configureren [pagina 204]
Voorbeelden van veelvoorkomende scenario's met firewalls [pagina 208]

8.16.1 Overzicht van BI-platformservers en communicatiepoorten

Als het systeem is geïmplementeerd met firewalls is het belangrijk hun BI-platformservers en communicatiepoorten te kennen.

8.16.1.1 Elke BI-platformserver wordt aan een aanvraagpoort gebonden

Een BI-platformserver, zoals de Input File Repository Server, wordt bij het starten aan een aanvraagpoort gebonden. Deze aanvraagpoort kan door andere BI-platformonderdelen, waaronder servers, Rich Clients en de SDK die op de webtoepassingsserver wordt gehost, worden gebruikt voor communicatie met de server.

Servers selecteren het nummer van de aanvraagpoort dynamisch wanneer de server (opnieuw) gestart wordt, tenzij er een specifiek poortnummer is gedefinieerd. Voor servers die met andere BI-platformonderdelen communiceren via een firewall, moet er handmatig een specifiek nummer voor de aanvraagpoort worden opgegeven.

8.16.1.2 Elke BI-platformserver wordt bij de CMS geregistreerd

BI-platformservers worden bij de CMS geregistreerd wanneer ze gestart worden. Bij de registratie van een server wordt het volgende in de CMS vastgelegd:

- De hostnaam (of het IP-adres) van de hostcomputer van de server.
- Het nummer van de aanvraagpoort van de server.

8.16.1.3 De CMS gebruikt twee poorten

De CMS gebruikt twee poorten: de aanvraagpoort en de Name Server-poort. De aanvraagpoort wordt standaard dynamisch geselecteerd. De Name Server-poort is standaard 6400.

Alle BI-platform™servers en clienttoepassingen maken in eerste instantie verbinding met de CMS via de Name Server-poort. De CMS™ reageert op dit eerste contact door de waarde van de aanvraagpoort te retourneren. Deze aanvraagpoort wordt door de servers gebruikt voor verdere communicatie met de CMS™.

8.16.1.4 CMS-map (Central Management Server) met geregistreerde services

De CMS bevat een map met de services die bij de CMS zijn geregistreerd. Andere BI-platformonderdelen zoals webservices, rich clients en de SDK die op de webtoepassingsserver worden gehost, kunnen verbinding maken met de CMS en een verwijzing naar een bepaalde service aanvragen. Een serviceverwijzing bevat het nummer van de aanvraagpoort van de service, de hostnaam (of het IP-adres) van de computer waarop de server wordt gehost en de service-id.

BI-platformonderdelen kunnen zich in een ander subnet bevinden dan de server waarvan ze gebruikmaken. De hostnaam (of het IP-adres) in de serviceverwijzing moet kunnen worden gerouteerd vanaf de computer waarop het onderdeel zich bevindt.

> **Opmerking**
>
> De verwijzing naar een BI-platformserver bevat standaard de hostnaam van de servercomputer. (Als een computer meer dan een hostnaam heeft, wordt de primaire hostnaam gekozen.) U kunt een server zo configureren dat de verwijzing niet de hostnaam bevat, maar het IP-adres.

Verwante informatie

Communicatie tussen BI-platformonderdelen [pagina 193]

8.16.1.5 Server Intelligence Agents (SIA) communiceren met de CMS (Central Management Server)

De implementatie is alleen functioneel als de Server Intelligence Agent (SIA) en de CMS (Central Management Server) met elkaar kunnen communiceren. Controleer of de poorten van de firewall zodanig zijn geconfigureerd dat er communicatie tussen alle SIA's en CMS'en in het cluster mogelijk is.

8.16.1.6 Onderliggende processen van Job Server communiceren met gegevenslaag en CMS

De meeste Job Servers maken een onderliggend proces om een taak te verwerken, bijvoorbeeld het genereren van een rapport. De Job Server maakt een of meer onderliggende processen. Elk onderliggend proces heeft een eigen aanvraagpoort.

Een Job Server selecteert op dynamische wijze een aanvraagpoort voor elk onderliggend proces. U kunt een reeks poortnummers opgeven, waaruit de Job Server een keuze kan maken.

Alle onderliggende processen communiceren met de CMS. Als deze communicatie een firewall passeert, moet u het volgende doen:

- Geef het bereik van poortnummers op waaruit de taakserver kan kiezen door de parameters `-requestJSChildPorts <laagstepoort>-<hoogstepoort>` en `-requestPort <poort>` in te voeren op de opdrachtregel van de server. Houd rekening ermee dat het poortbereik groot genoeg moet zijn om ondersteuning te bieden aan het maximum aantal onderliggende processen dat met `-maxJobs` is gedefinieerd.
- Het opgegeven poortbereik in de firewall openen.

Veel onderliggende processen communiceren met de gegevenslaag. Zo kan door een onderliggend proces bijvoorbeeld verbinding worden gemaakt met een rapportdatabase, gegevens worden opgehaald en waarden worden berekend voor een rapport. Als de onderliggende processen van de Job Server via een firewall met de gegevenslaag communiceren, moet u het volgende doen:

- Een communicatiepad in de firewall openen vanaf elke gewenste poort op de Job Server-computer naar de luisterpoort van de database op de computer waarop de databaseserver zich bevindt.

Verwante informatie

Overzicht van opdrachtregels [pagina 1104]

8.16.2 Communicatie tussen BI-platformonderdelen

BI-platformonderdelen, zoals browserclients, Rich Clients, servers en de SDK die op de webtoepassingsserver wordt gehost, communiceren via het netwerk met elkaar tijdens speciale werkstromen. U hebt inzicht in deze werkstromen nodig om SAP Business Objects-producten te kunnen implementeren in een aantal verschillende subnetten die door een firewall worden gescheiden.

8.16.2.1 Vereisten voor de communicatie tussen BI-platformonderdelen

Implementaties van het BI-platform moeten voldoen aan deze algemene vereisten.

1. Elke server moet communicatie kunnen starten met elke andere BI-platformserver via de aanvraagpoort van die server.
2. De Central Management Server gebruikt twee poorten. Elke BI-platformserver, rich client en de webtoepassingsserver waarop de SDK wordt gehost, moeten communicatie met de CMS via beide poorten kunnen starten.
3. Elk onderliggend proces van de Job Server moet met de CMS kunnen communiceren.
4. Thick clients moeten communicatie kunnen initiëren met de aanvraagpoort van de Input File Repository Server en de Output File Repository Server.
5. Als de controlefunctie is ingeschakeld voor thick clients en webtoepassingen, moeten deze communicatie kunnen initiëren met de aanvraagpoort van de Adaptive Processing Servers waarop de proxyservice voor clientcontrole wordt gehost.
6. In het algemeen geldt dat de webtoepassingsserver waarop de SDK wordt gehost, communicatie moet kunnen initiëren met de aanvraagpoort van elke BI-platformserver.

   > **Opmerking**
   >
   > De webtoepassingsserver hoeft alleen te communiceren met BI-platformservers die in de implementatie worden gebruikt. Als Crystal Reports bijvoorbeeld niet wordt gebruikt, hoeft de webtoepassingsserver niet met de Crystal Reports Cache Servers te communiceren.

7. Voor taakservers worden de poortnummers gebruikt die u kunt opgeven met de opdracht `-requestJSChildPorts <laagstepoort>-<hoogstepoort>`. Als er geen bereik is opgegeven op de opdrachtregel, worden voor de servers willekeurige poortnummers gebruikt. Als u communicatie tussen een Job Server en een CMS, FTP-, SFTP-, of e-mailserver op een andere computer wilt toestaan, opent u alle poorten in het bereik dat is opgegeven via `-requestJSChildPorts` voor de firewall.
8. De CMS moet kunnen communiceren met de luisterpoort van de CMS-database.
9. De verbindingsserver, de meeste onderliggende processen van de Job Server en alle systeemdatabases en controlerende Processing Servers moeten communicatie kunnen initiëren met de luisterpoort van de rapportdatabase.

Verwante informatie

Poortvereisten voor BI-platform [pagina 194]

8.16.2.2 Poortvereisten voor BI-platform

In deze sectie vindt u de communicatiepoorten die worden gebruikt door BI-platformservers, thick clients, de webtoepassingsserver waarop de SDK wordt gehost en externe softwaretoepassingen. Als u het BI-platform implementeert met firewalls, kunt u aan de hand van deze informatie het minimum aantal poorten in de firewalls openen.

8.16.2.2.1 Poortvereisten voor BI-platformtoepassingen

In deze tabel vindt u de servers en de poortnummers die door BI-platformtoepassingen worden gebruikt.

Product	Clienttoepassing	Ondersteunde servers	Vereiste serverpoort
Crystal Reports	SAP Crystal Reports 2020-ontwerper	CMS Input FRS Output FRS Crystal Reports 2020 Report Application Server (RAS) Crystal Reports 2020-verwerkingsserver Crystal Reports-cacheserver	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort Output FRS-aanvraagpoort Aanvraagpoort voor Crystal Reports 2020 Report Application Server Aanvraagpoort voor Crystal Reports 2020-verwerkingsserver Aanvraagpoort voor Crystal Reports-cacheserver
Crystal Reports	SAP Crystal Reports voor Enterprise-ontwerper	CMS Input FRS Output FRS Crystal Reports-verwerkingsserver Crystal Reports-cacheserver	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort Output FRS-aanvraagpoort Aanvraagpoort voor Crystal Reports-verwerkingsserver Aanvraagpoort voor Crystal Reports-cacheserver
Live Office	Live Office-client:	Toepassing van webserviceprovider (`dswsbobje.war`) waarmee de Live Office-webservice wordt gehost	HTTP-poort (standaard: 80)
SAP Analysis voor Microsoft Office	SAP Analysis voor Microsoft Office	CMS Adaptive Processing Server host de Multi Dimensional Analysis Service Input FRS Output FRS	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Adaptive Processing Server-aanvraagpoort Input FRS-aanvraagpoort Output FRS-aanvraagpoort
BI-platform	SAP BusinessObjects Web Intelligence Rich Client	CMS Input FRS	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort

Product	Clienttoepassing	Ondersteunde servers	Vereiste serverpoort
BI-platform	Universe-ontwerpprogramma	CMS Input FRS Verbindingsserver	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort Verbindingsserverpoort
BI-platform	Business Views-beheer	CMS Input FRS	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort
BI-platform	Central Configuration Manager (CCM)	CMS SIA (Server Intelligence Agent)	De volgende poorten moeten geopend zijn, zodat externe BI-platformservers door de CCM kunnen worden beheerd: CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort De volgende poorten moeten geopend zijn, zodat externe SIA-processen door de CCM kunnen worden beheerd: Microsoft Directory Services (TCP-poort 445) NetBIOS Session Service (TCP-poort 139) NetBIOS Datagram Service (UDP-poort 138) NetBIOS Name Service (UDP-poort 137) DNS (TCP/UDP-poort 53) (Sommige van de bovenvermelde poorten zijn mogelijk niet vereist. Raadpleeg de Windows-beheerder.)
BI-platform	SIA (Server Intelligence Agent)	Elke BI-platformserver inclusief de CMS	SIA-aanvraagpoort (standaard: 6410) CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort
BI-platform	Diagnostisch hulpprogramma voor gegevensopslagruimten	CMS Input FRS Output FRS	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Input FRS-aanvraagpoort Output FRS-aanvraagpoort

Product	Clienttoepassing	Ondersteunde servers	Vereiste serverpoort
BI-platform	SDK van BI-platform gehost op de webtoepassingsserver	Alle BI-platformservers die vereist worden door de geïmplementeerde producten Communicatie met de aanvraagpoort voor de Crystal Reports 2020-verwerkingsserver is vereist als de SDK communiceert met Crystal Reports-rapporten en deze ophaalt uit de CMS.	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Aanvraagpoort van elke vereiste server De aanvraagpoort voor de Crystal Reports 2020-verwerkingsserver bijvoorbeeld.
BI-platform	Webserviceprovider (`dswsbobje.war`)	Alle BI-platformservers die vereist worden door de producten die webservices oproepen. Communicatie met de aanvraagpoorten voor de Dashboards-cacheserver en -verwerkingsserver is vereist als SAP BusinessObjects Dashboards Enterprise-gegevensbronverbindingen oproept via de webserviceprovider.	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Aanvraagpoort van elke vereiste server Bijvoorbeeld aanvraagpoorten voor de Dashboards-cacheserver en -verwerkingsserver.
BI-platform	SAP BusinessObjects Analysis, editie voor OLAP	CMS Adaptive Processing Server host de Multi Dimensional Analysis Service Input FRS Output FRS	CMS Name Server-poort (standaard: 6400) CMS-aanvraagpoort Adaptive Processing Server-aanvraagpoort Input FRS-aanvraagpoort Output FRS-aanvraagpoort

8.16.2.2.2 Poortvereisten voor externe toepassingen

Deze tabel bevat een overzicht van externe software die door SAP BusinessObjects-producten worden gebruikt. U vindt hier specifieke voorbeelden van bepaalde softwareleveranciers; voor elke leverancier gelden echter andere poortvereisten.

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
CMS-systeemdatabase	Central Management Server (CMS)	Luisterpoort van databaseserver	De CMS is de enige server die met de CMS-systeemdatabase communiceert.

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
CMS-controledatabase	Central Management Server (CMS)	Luisterpoort van databaseserver	De CMS is de enige server die met de CMS-controledatabase communiceert.
Rapportdatabase	Verbindingsserver Alle onderliggende processen van Job Server Alle verwerkingsservers	Luisterpoort van databaseserver	Deze servers halen gegevens op uit de rapportdatabase.
webtoepassingsserver	Alle SAP BusinessObjects-webservices en -webtoepassingen inclusief het BI-startpunt en de CMC	HTTP-poort en HTTPS-poort. Voorbeeld: op Tomcat is de standaard HTTP-poort 8080 en de standaard HTTPS-poort 443.	De HTTPS-poort is alleen vereist als er beveiligde HTTP-communicatie wordt gebruikt.
FTP-server	Alle Job Servers	FTP In (poort 21) FTP Out (poort 22)	De Job Servers gebruiken de FTP-poort ter ondersteuning van *verzending naar FTP*.

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
SFTP-server	Alle Job Servers	SFTP (poort 22)	De Job Servers gebruiken de SFTP-poort ter ondersteuning van *verzending naar SFTP*. **Opmerking** Er wordt een vingerafdruk van de hostsleutel gebruikt om een SSH-verbinding te beveiligen en man-in-the-middle-aanvallen te voorkomen. Het is een verplichte niet-nullparameter die is vereist om SFTP te configureren. Het proces waarmee de vingerafdruk van de hostsleutel wordt gegenereerd, verschilt per gebruikte SFTP-server. De beheerder/gebruiker moet de SHA-2-vingerafdruk configureren om SFTP in te schakelen. De beheerder/gebruiker kan de productdocumentatie bij de SSH-/SFTP-serverimplementaties raadplegen om de SHA-2-vingerafdruk te genereren. **Voorbeeld** Gangbare SFTP-clients zoals PuTTY en WinSCP gebruiken MD5-vingerafdrukken voor de unieke identificatie van SFTP-servers. MD5-vingerafdrukken werken niet. Raadpleeg de SFTP-serverdocumentatie voor instructies hoe u SHA-2-vingerafdrukken ophaalt. Hieronder wordt een voorbeeldmethode beschreven waarbij een bepaald openbaar sleutelbestand en Unix-hulpprogramma's voor OpenSSH worden gebruikt. Uitgaande van een openbaar sleutelbestand met de naam RSA-Key.pub met de volgende gegevens: `ssh-rsa <base64 encoded key>`, voert u het

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
			volgende script uit: `cut -d ' ' -f 2 < RSAKey.pub | base64 -d | openssl dgst -c -sha256`. De uitvoer is bijvoorbeeld: `(stdin)= 00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`, waarbij de uitvoer van 20 cijfers afhankelijk is van de waarde van de base64-gecodeerde openbare sleutel. Gebruik de waarde van 20 cijfers `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` als vingerafdruk van de hostsleutel. → Aanbeveling De aanbevolen procedure is dat u SFTP-configuratie inschakelt op de serverpagina's van de CMC in BOE en de standaardinstellingen gebruikt als u de gegevens verzendt naar SFTP-servers.

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
E-mailserver	Alle Job Servers	SMTP (poort volgens SMTP-server)	U kunt dezelfde poort gebruiken voor SMTPS en SMTP. Zorg er bij SMTP's echter voor dat SSL/TLS is ingeschakeld voor de server met de SMTP-opdracht STARTTLS. De Job Servers gebruiken de SMTP-poort ter ondersteuning van *verzending naar e-mail*. **Adaptive Job Server configureren:** Voer de onderstaande stappen uit om de Adaptive Job Server te configureren: 1. Start de CMC (Central Management Console) 2. Selecteer *Servers* in de vervolgkeuzelijst. 3. Klik met de rechtermuisknop op **AdaptiveJobServer** en selecteer *Doel* 4. Selecteer *E-mail* in de vervolgkeuzelijst. Als u E-mailserver niet al als doel hebt toegevoegd, dan moet u eerst E-mailserver als doel toevoegen voordat u doorgaat. 5. Voer de benodigde gegevens in. 6. Selecteer de optie *SSL inschakelen* indien vereist. 7. Klik op *Opslaan en sluiten*. **SMTP via SSL instellen:** Om SMTP via SSL in te stellen moet het SMTP-servercertificaat aanwezig zijn in de server en het BOE-systeem. Volg de volgende stappen om SMTP via SSL in te stellen: 1. Genereer een certificaat vanaf de SMTP-server. 2. Schakel in het venster *Doel* het selectievakje *SSL inschakelen* in.

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
			3. Voer het absolute pad naar het SMTP-certificaat in. **Opmerking** Voer een absoluut pad naar het SMTP-certificaat in. Als u geen absoluut pad naar het SMTP-certificaat invoert, kunt u een tijdelijke aanduiding invoeren (%SI_DEFAULT_CERT_LOC%) en het systeem leest dit als de standaardlocatie, d.w.z. `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` of `\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` en zoekt het certificaat (standaardnaam van het certificaat is certificate.crt). 4. Selecteer de gewenste *Beveiliging verbinding*. **Opmerking** Standaard is de optie *StartTLS* geselecteerd. U kunt ervoor kiezen *SSL/TLS* te selecteren. 5. Selecteer de gewenste TLS-versie. **Opmerking** Standaard is TLS v1.0 geselecteerd. U kunt ervoor kie-

Externe toepassing	SAP BusinessObjects-onderdeel dat het externe product gebruikt	Poortvereiste voor externe toepassing	Beschrijving
			zen TLS v1.1 of TLS v1.2 te selecteren. 6. Kies *Opslaan en sluiten*. SMTP via SSL in nu ingesteld. **Opmerking** Als u een patchupdate van BI 4.1 SP6 naar een willekeurige hogere versie uitvoert, wordt standaard de optie StartTLS en TLSv1.0 geselecteerd. **Opmerking** • Als de gebruiker het selectievakje *SSL inschakelen* inschakelt, wordt er een beveiligd kanaal ingeschakeld. Dit maakt beveiligde SMTP-communicatie via SSL mogelijk. • U kunt slechts één SMTP-certificaat per Adaptive Job Server configureren. U kunt niet meerdere certificaten voor één jobserver configureren. • De optie *SSL inschakelen* is alleen beschikbaar in de Adaptive Job Server en niet op documentniveau.
Unix-servers waarnaar de Job Servers inhoud kunnen sturen	Alle Job Servers	rexec out (poort 512) (alleen Unix) rsh out (poort 514)	(alleen Unix) De Job Servers gebruiken deze poorten ter ondersteuning van verzending naar schijf.
Verificatieserver	CMS™ webtoepassingsserver waarop de SDK wordt gehost elke thick client, zoals Live Office.	Verbindingspoort voor externe verificatie Voorbeeld: de verbindingsserver voor de Oracle LDAP-server wordt door de gebruiker gedefinieerd in het bestand Ldap.ora.	Gebruikersreferenties worden opgeslagen op de externe verificatieserver. De CMS™, SDK en thick clients die hier worden vermeld, moeten met de externe verificatieserver kunnen communiceren wanneer een gebruiker zich aanmeldt.

8.17 Het BI-platform voor firewalls configureren

Deze sectie bevat praktische stapsgewijze instructies voor het configureren van BI-platformsysteem voor een firewallomgeving.

8.17.1 Het systeem configureren voor firewalls

1. Bepaal welke BI-platformonderdelen via een firewall moeten communiceren.
2. Configureer handmatig de aanvraagpoort voor elke BI-platformserver die via een firewall moet communiceren.
3. Configureer een poortbereik voor de onderliggende processen van de Job Server die door een firewall moeten communiceren door de parameters `-requestJSChildPorts<laagstepoort>-<hoogstepoort> en -requestPort <poort>` toe te voegen aan de opdrachtregel van de server.
4. Configureer de firewall zodanig dat communicatie mogelijk is met de aanvraagpoorten en het poortbereik van taakservers van de BI-platformservers die u in de vorige stap hebt geconfigureerd.
5. (Optioneel) Configureer het hosts-bestand op elke computer die als host fungeert voor een BI-platformserver die via een firewall moet communiceren.

Verwante informatie

Communicatie tussen BI-platformonderdelen [pagina 193]
Poortnummers configureren [pagina 463]
Overzicht van opdrachtregels [pagina 1104]
Firewallregels opgeven [pagina 204]
Configureer het hostbestand voor firewalls die gebruikmaken van NAT. [pagina 206]

8.17.1.1 Firewallregels opgeven

Configureer de firewall zodanig dat het nodige verkeer tussen BI-platformonderdelen mogelijk is. Raadpleeg de documentatie bij de firewall voor meer informatie over het instellen van de juiste regels.

Geef een toegangsregel voor inkomend verkeer op voor elk communicatiepad in de firewall. Mogelijk hoeft u geen afzonderlijke toegangsregel op te geven voor elke BI-platformserver die zich achter de firewall bevindt.

Gebruik het poortnummer dat u opgeeft in het vak *Aanvraagpoort* van de server op de pagina Eigenschappen van de server in de CMC. Let erop dat u voor elke server op een computer een uniek poortnummer opgeeft. Bepaalde SAP Business Objects-servers gebruiken meerdere poorten.

> **Opmerking**
>
> Als het BI-platform wordt geïmplementeerd met een firewall die gebruikmaakt van NAT, is er voor elke server op alle computers een uniek nummer voor de aanvraagpoort vereist. Dit betekent dat niet twee servers in de gehele implementatie hetzelfde poortnummer kunnen hebben.

> **Opmerking**
>
> U hoeft geen toegangsregels voor uitgaand verkeer op te geven. BI-platformservers kunnen geen communicatie initiëren met de webtoepassingsserver of met clienttoepassingen. BI-platformservers kunnen communicatie initiëren met andere platformservers in hetzelfde cluster. Implementaties met geclusterde servers in een omgeving met een uitgaande firewall worden niet ondersteund.

Voorbeeld

In dit voorbeeld ziet u de toegangsregels voor inkomend verkeer voor een firewall die tussen de webtoepassingsserver en de BI-platformservers is geïnstalleerd. Er zijn hier twee poorten nodig voor de CMS, een poort voor de Input FRS (File Repository Server) en een poort voor de Output FRS. De nummers voor de aanvraagpoort zijn de nummers die u hebt opgegeven in het vak *Aanvraagpoort* op de CMC-configuratiepagina voor een server.

Broncomputer	Poort	Doelcomputer	Poort	Actie
webtoepassingsserver	Willekeurig	CMS	6400	Toestaan
webtoepassingsserver	Willekeurig	CMS	<nummer aanvraag-poort>	Toestaan
webtoepassingsserver	Willekeurig	Input FRS	<nummer aanvraag-poort>	Toestaan
webtoepassingsserver	Willekeurig	Output FRS	<nummer aanvraag-poort>	Toestaan
Willekeurig	Willekeurig	CMS	Willekeurig	Weigeren
Willekeurig	Willekeurig	Andere platformser-vers	Willekeurig	Weigeren

Verwante informatie

Communicatie tussen BI-platformonderdelen [pagina 193]

8.17.1.2 Configureer het hostbestand voor firewalls die gebruikmaken van NAT.

Deze stap is alleen vereist als de BI-platformservers via een firewall moeten communiceren waarop NAT (Network Address Translation) is ingeschakeld. Met deze stap kunnen de clientcomputers de hostnaam van een server toewijzen aan een routeerbaar IP-adres.

> ⓘ Opmerking
>
> Het BI-platform kan worden geïmplementeerd op computers die DNS (Domain Name System) gebruiken. In dit geval kunnen de hostnamen van de servercomputers worden toegewezen aan een extern routeerbaar IP-adres op de DNS-server in plaats van aan het `host`bestand van elke computer.

NAT (Network Address Translation)

Een firewall beschermt een intern netwerk tegen ongewenste toegang. Firewalls die gebruikmaken van NAT wijzen de IP-adressen van het interne netwerk toe aan een ander adres dat door het externe netwerk wordt gebruikt. Deze adresconversie versterkt de beveiliging, doordat de interne IP-adressen worden afgeschermd van het externe netwerk.

BI-platformonderdelen zoals servers, thick clients en de webtoepassingsserver die als host dient voor de SDK, gebruiken een serviceverwijzing om verbinding te maken met een server. De serviceverwijzing bevat de hostnaam van de servercomputer. Deze hostnaam moet routeerbaar zijn vanaf de computer waarop BI-platformonderdeel zich bevindt. Dit betekent dat het `host`bestand op de computer waarop het onderdeel zich bevindt, de hostnaam van de servercomputer moet toewijzen aan het externe IP-adres van de servercomputer. Het externe IP-adres van de servercomputer is buiten de firewall routeerbaar, in tegenstelling tot het interne IP-adres.

De procedure voor het configureren van het `Hosts`-bestand is verschillend voor Windows en Unix.

8.17.1.2.1 Het Hosts-bestand configureren in Windows

1. Zoek elke computer waarop zich een BI-platformonderdeel bevindt dat moet communiceren via een firewall waarvoor Network Address Translation (NAT is ingeschakeld.
2. Open op elke computer die u in de vorige stap hebt gevonden het bestand `Hosts` in een teksteditor, bijvoorbeeld Kladblok. U vindt het `hosts`-bestand in `\Windows\System32\drivers\etc\hosts`.
3. Volg de instructies in het `host`bestand om een vermelding toe te voegen voor elke computer achter de firewall waarop een of meer BI-platformservers worden uitgevoerd. Wijs de hostnaam van de servercomputer of de FQDN (Fully Qualified Domain Name) toe aan het externe IP-adres van de servercomputer.
4. Sla het bestand `Hosts` op.

8.17.1.2.2 De hostbestanden configureren op UNIX

> **Opmerking**
>
> Het UNIX-besturingssysteem moet zo worden geconfigureerd dat eerst het bestand Hosts wordt geraadpleegd voor omzetting van domeinnamen en daarna pas de DNS. Raadpleeg de documentatie bij het UNIX-systeem voor meer informatie.

1. Zoek elke computer waarop zich een BI-platformonderdeel bevindt dat moet communiceren via een firewall waarvoor Network Address Translation (NAT is ingeschakeld.
2. Open het Hosts-bestand met een editor, bijvoorbeeld `Vi`. Het `Hosts`-bestand bevindt zich in de map `\etc`.
3. Volg de instructies in het `host`bestand om een vermelding toe te voegen voor elke computer achter de firewall waarop een of meer BI-platformservers worden uitgevoerd. Wijs de hostnaam van de servercomputer of de FQDN (Fully Qualified Domain Name) toe aan het externe IP-adres van de servercomputer.
4. Sla het bestand `Hosts` op.

8.17.2 Fouten opsporen in een implementatie met firewalls

Als een of meer van uw BI-platformservers niet werken wanneer uw firewall is ingeschakeld, zelfs als de verwachte poorten zijn geopend in de firewall, kunt u de gebeurtenislogboeken gebruiken om te bepalen welke servers op welke poorten of IP-adressen proberen te luisteren. U kunt deze poorten dan openen in uw firewall of de Central Management Console (CMC) gebruiken om de poortnummers of IP-adressen te wijzigen waarop deze servers proberen te luisteren.

Wanneer een BI-platformserver gestart wordt, schrijft de server de volgende informatie naar het gebeurtenislogboek voor elke aanvraagpoort waarmee de server verbinding probeert te maken.

- *Server* - De naam van de server en of deze gestart is.
- *Gepubliceerd(e) adres(sen)* - Een lijst met IP-adressen en poortcombinaties die gepost zijn naar de naamservice die andere servers gebruiken om met deze server te communiceren.

Als de server aan een poort gebonden wordt, geeft het logbestand ook *Luisteren op poorten* weer met het IP-adres en de poort waarop de server luistert. Als de server niet aan een poort gebonden kan worden, geeft het logbestand *Kan niet luisteren op poort(en)* weer met het IP-adres en de poort waarop de server niet kan luisteren.

Wanneer een Central Management Server wordt gestart, legt deze ook informatie vast als Gepubliceerd(e) adres(sen), Luisteren op poorten en Luisteren mislukt op voor de Name Service-poort van de server.

> **Opmerking**
>
> Als de server geconfigureerd is voor gebruik van een automatisch toegewezen poort en een ongeldige hostnaam en een ongeldig IP-adres, geeft het gebeurtenislogboek aan dat de server niet kan luisteren op de hostnaam of het IP-adres en poort “0”. Als de opgegeven hostnaam of het IP-adres ongeldig is, mislukt de server voordat het besturingssysteem van de host een poort kan toewijzen.

Voorbeeld

In het volgende voorbeeld wordt een vermelding van een Central Management Server weergegeven, die luistert op twee aanvraagpoorten en een Name Service-poort.

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

8.17.2.1 Fouten opsporen in een implementatie met firewalls

1. Lees het gebeurtenislogboek om te bepalen of de server aan de opgegeven poort gebonden is.

   Als de server niet aan een poort is gebonden, is er waarschijnlijk sprake van een poortconflict tussen de server en een ander proces dat op dezelfde computer wordt uitgevoerd. De vermelding *Luisteren mislukt op* geeft aan op welke poort de server probeert te luisteren. Voer een hulpprogramma zoals netstat uit om te bepalen welk proces gebruikmaakt van de poort en configureer dan het andere proces of de server om op een andere poort te luisteren.
2. Als de aan server een poort gebonden is, geeft *Luisteren op* aan op welke poort de server luistert. Als een server op een poort luistert en nog steeds niet juist werkt, zorg er dan voor dat de poort open is in de firewall of configureer de server zodat deze op een open poort luistert.

Als alle Central Management Servers in uw implementatie proberen te luisteren op poorten of IP-adressen die niet beschikbaar zijn, worden de CMS'en niet gestart en kunt u zich niet aanmelden bij de CMC. Als u het poortnummer of IP-adres wilt wijzigen waarop de CMS probeert te luisteren, moet u de Central Configuration Manager (CCM) gebruiken om een geldig poortnummer of IP-adres op te geven.

Verwante informatie

Poortnummers configureren [pagina 463]

8.18 Voorbeelden van veelvoorkomende scenario's met firewalls

Deze sectie bevat voorbeelden van veelvoorkomende scenario's waarin firewalls zijn geïmplementeerd.

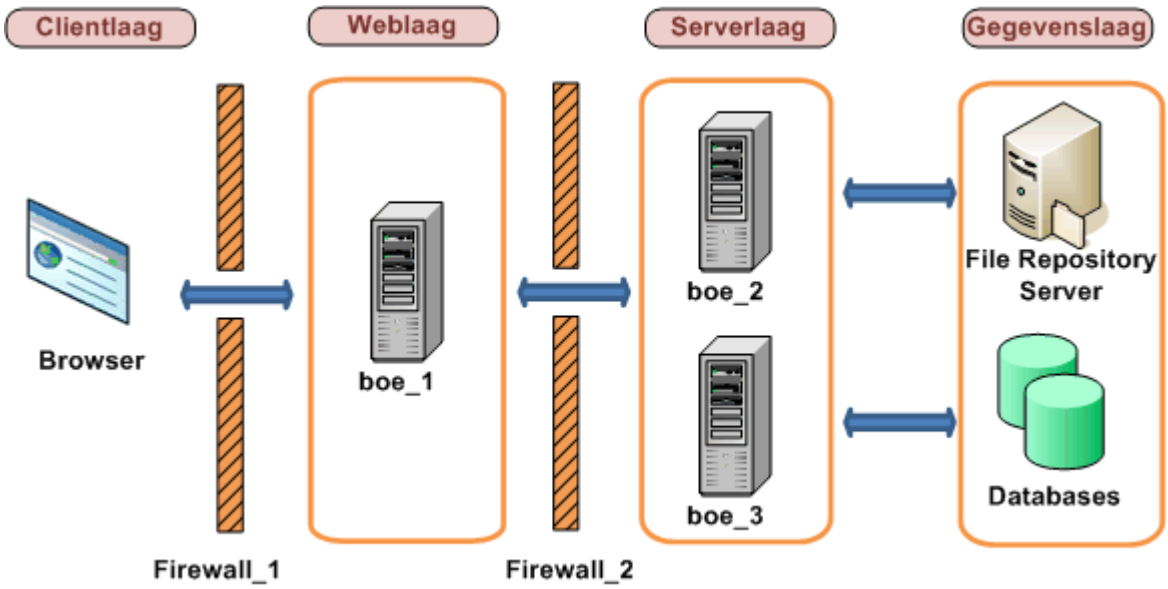
8.18.1 Voorbeeld: de toepassingslaag bevindt zich op een afzonderlijk netwerk.

In dit voorbeeld ziet u hoe u een firewall en het BI-platform configureert voor interoperabiliteit in een implementatiescenario waarin de firewall de webtoepassingsserver van andere BI-platformservers scheidt.

De BI-platformonderdelen zijn in dit voorbeeld verspreid over deze computers:

- Computer `boe_1` is host voor de webtoepassingsserver en de SDK.
- Computer `boe_2` is host voor de servers van de intelligence-laag, waaronder de Central Management Server, de Input File Repository Server, de Output File Repository Server en Event Server.
- Computer `boe_3` is host voor de servers van de verwerkingslaag, waaronder de Adaptive Job Server, de Web Intelligence-verwerkingsserver, de Report Application Server, the Crystal Reports-cacheserver en de Crystal Reports-verwerkingsserver.

Toepassingslaag op afzonderlijk netwerk



8.18.1.1 Toepassingslaag op afzonderlijk netwerk configureren

In de volgende stappen wordt aangegeven hoe u de configuratie in dit voorbeeld definieert.

1. Voor dit voorbeeld gelden deze communicatievereisten:
   - De webtoepassingsserver waarop de SDK wordt gehost, moet via beide poorten met de CMS kunnen communiceren.
   - De webtoepassingsserver waarop de SDK wordt gehost, moet met alle BI-platformservers kunnen communiceren.
   - De browser moet toegang hebben tot de HTTP- of de HTTPS-aanvraagpoort op de webtoepassingsserver.

2. De webtoepassingsserver moet kunnen communiceren met alle BI-platformservers op de computers `boe_2` en `boe_3`. Configureer de poortnummers voor elke server op deze computers. U kunt elke beschikbare poort tussen 1.025 en 65.535 opgeven.
   U vindt de poortnummers die in dit voorbeeld zijn gebruikt in de tabel hieronder:

Server	Poortnummer
Central Management Server	6400
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event Server	6425
Adaptive Job Server	6435
Crystal Reports Cache Server	6440
Web Intelligence-verwerkingsserver	6460
Report Application Server	6465
Crystal Reports-verwerkingsserver	6470

3. Configureer de firewalls `Firewall_1` en `Firewall_2` zodanig dat communicatie mogelijk is met de vaste poorten van de BI-platformservers en de webtoepassingsserver die u in de vorige stap hebt geconfigureerd.

   In dit voorbeeld wordt de HTTP-poort voor de Tomcat-toepassingsserver geopend.

   Configuratie voor Firewall_1

Poort	Doelcomputer	Poort	Actie
Willekeurig	boe_1	8080	Toestaan

   Configuratie voor Firewall_2

Broncomputer	Poort	Doelcomputer	Poort	Actie
boe_1	Willekeurig	boe_2	6400	Toestaan
boe_1	Willekeurig	boe_2	6411	Toestaan
boe_1	Willekeurig	boe_2	6415	Toestaan
boe_1	Willekeurig	boe_2	6420	Toestaan
boe_1	Willekeurig	boe_2	6425	Toestaan
boe_1	Willekeurig	boe_3	6435	Toestaan
boe_1	Willekeurig	boe_3	6440	Toestaan
boe_1	Willekeurig	boe_3	6460	Toestaan
boe_1	Willekeurig	boe_3	6465	Toestaan
boe_1	Willekeurig	boe_3	6470	Toestaan

4. Deze firewall biedt geen ondersteuning voor NAT, waardoor het `hosts`-bestand niet hoeft te worden geconfigureerd.

Verwante informatie

Poortnummers configureren [pagina 463]
Communicatie tussen BI-platformonderdelen begrijpen [pagina 191]

8.18.2 Voorbeeld: thick client en databaselaag door firewall gescheiden van BI-platformservers

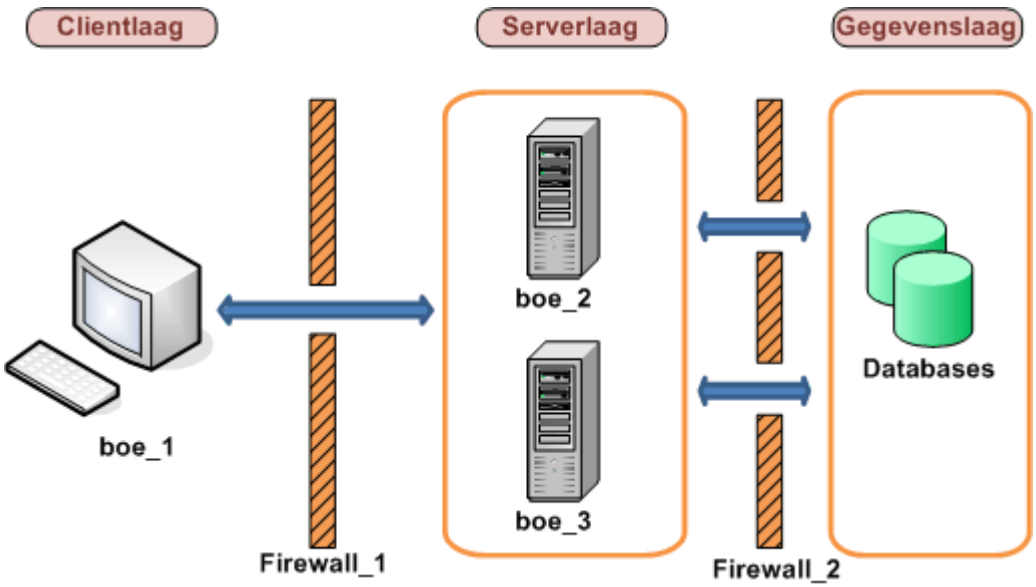
In dit voorbeeld ziet u hoe u een firewall en het BI-platform configureert voor interoperabiliteit in een implementatie waarbij het volgende geldt:

- Eén firewall scheidt een thick client van de BI-platformservers.
- Eén firewall scheidt de BI-platformservers van de databaselaag.

De BI-platformonderdelen zijn in dit voorbeeld verspreid over deze computers:

- Computer `boe_1` is host voor de wizard Publiceren. De wizard Publiceren is een thick client van BI-platform
- Computer `boe_2` is host voor de servers van de intelligencelaag, waaronder de Central Management Server (CMS), de Input File Repository Server, de Output File Repository Server en Event Server.
- Computer `boe_3` is host voor de servers van de verwerkingslaag, waaronder de Adaptive Job Server, de Web Intelligence-verwerkingsserver, de Report Application Server, de Crystal Reports-verwerkingsserver en de Crystal Reports-cacheserver.
- Computer `Databases` is host voor de systeem- en controledatabase van de CMS en de rapportdatabase. U kunt beide databases op dezelfde databaseserver implementeren of elk op een afzonderlijke databaseserver. In dit voorbeeld bevinden alle CMS-databases en de rapportdatabase zich op dezelfde databaseserver.

Rich Client en databaselaag op afzonderlijke netwerken



8.18.2.1 Lagen configureren die van BI-platformservers worden gescheiden door een firewall

In de volgende stappen wordt aangegeven hoe u de configuratie in dit voorbeeld definieert.

1. Voor dit voorbeeld gelden deze communicatievereisten:
   - De wizard Publiceren moet communicatie met de CMS™ kunnen initiëren via beide poorten.
   - De wizard Publiceren moet communicatie met de Input File Repository Server en de Output File Repository Server kunnen initiëren.
   - De verbindingsserver, alle onderliggende processen van de Job Server en alle Processing Servers moeten toegang hebben tot de luisterpoort van de server waarop de rapportdatabase zich bevindt.
   - De CMS™ moet toegang hebben tot de databaseluisterpoort van de CMS™-databaseserver.
2. Configureer een specifieke poort voor de CMS™, de Input FRS en de Output FRS. U kunt elke beschikbare poort tussen 1.025 en 65.535 opgeven.
   U vindt de poortnummers die in dit voorbeeld zijn gebruikt in de tabel hieronder:

Server	Poortnummer
Central Management Server ™	6411
Input File Repository Server	6415
Output File Repository Server	6416

3. Het is niet nodig om een poortbereik voor de onderliggende processen van de Job Server te configureren, omdat de firewall tussen de Job Servers en de databaseservers zodanig zal worden geconfigureerd dat vanuit elke poort communicatie kan worden geïnitieerd.
4. Configureer `<Firewall_1 >` zodanig dat communicatie mogelijk is met de vaste poorten van de platformservers die u in de vorige stap hebt geconfigureerd. Poort 6400 is de standaardpoort voor de CMS™ Name Server-poort en hoefde in de vorige stap niet expliciet te worden geconfigureerd.

Poort	Doelcomputer	Poort	Actie
Willekeurig	boe_2	6400	Toestaan
Willekeurig	boe_2	6411	Toestaan
Willekeurig	boe_2	6415	Toestaan
Willekeurig	boe_2	6416	Toestaan

Configureer `<Firewall_2>` zodanig dat communicatie mogelijk is met de luisterpoort van de databaseserver. De CMS™ (op *boe_2*) moet toegang hebben tot de systeem- en controledatabase van de CMS™, en de Job Servers (op *boe_3*) moeten toegang hebben tot de systeem- en controledatabase. Het is niet nodig om een poortbereik voor de onderliggende processen van de Job Server te configureren, omdat hun communicatie met de CMS de firewall niet hoeft te passeren.

Broncomputer	Poort	Doelcomputer	Poort	Actie
boe_2	Willekeurig	Databases	3306	Toestaan
boe_3	Willekeurig	Databases	3306	Toestaan

5. Deze firewall biedt geen ondersteuning voor NAT, waardoor het `hosts`-bestand niet hoeft te worden geconfigureerd.

Verwante informatie

Communicatie tussen BI-platformonderdelen begrijpen [pagina 191]
Het BI-platform voor firewalls configureren [pagina 204]

8.19 Firewallinstellingen voor geïntegreerde omgevingen

Deze sectie biedt een gedetailleerde beschrijving van specifieke overwegingen en poortinstellingen voor BI-platformsystemen die met de volgende ERP-omgevingen kunnen worden geïntegreerd.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI-platform bevat onderdelen zoals browserclients, rich clients, servers en de SDK die op de webtoepassingsserver worden gehost. Systeemonderdelen kunnen op meerdere computers worden geïnstalleerd. Het is handig als u de communicatie tussen het BI-platform en de ERP-onderdelen in grote lijnen begrijpt, voordat u uw systeem configureert voor firewalls.

Poortvereisten voor BI-platformservers

De volgende poorten zijn vereist voor de desbetreffende servers in het BI-platform:

Vereiste serverpoort
• Central Management Server - naamserverpoort • Central Management Server - aanvraagpoort • Aanvraagpoort voor invoer-FRS • Aanvraagpoort voor uitvoer-FRS • Report Application Server - aanvraagpoort • Crystal Reports Cache Server - aanvraagpoort • Crystal Reports Page Server - aanvraagpoort • Crystal Reports-verwerkingsserver - aanvraagpoort

8.19.1 Specifieke firewallrichtlijnen voor SAP-integratie

Uw BI-platformimplementatie moet de volgende communicatieregels in acht nemen:

- De CMS moet de communicatie met het SAP-systeem op de gatewaypoort voor het SAP-systeem kunnen initiëren.
- De Adaptive Job Server en Crystal Reports-verwerkingsserver (met de onderdelen voor gegevenstoegang) moeten de communicatie met het SAP-systeem op de gatewaypoort voor het SAP-systeem kunnen initiëren.
- Het BW Publisher-onderdeel moet de communicatie met het SAP-systeem op de gatewaypoort voor het SAP-systeem kunnen initiëren.
- BI-platformonderdelen die zijn geïmplementeerd op de SAP Enterprise-portal (zoals iView en KMC), moeten communicatie met webtoepassingen van BI-platform op HTTP/HTTPS-poorten kunnen initiëren.
- De webtoepassingsserver moet de communicatie voor de service van de SAP-systeemgateway kunnen initiëren.
- Crystal Reports moet de communicatie met de SAP-host op de gatewaypoort en de dispatcherpoort voor het SAP-systeem kunnen initiëren.

De poort waarop de SAP-gatewayservice luistert, is dezelfde poort die voor de installatie is opgegeven.

> **Opmerking**
>
> Als een onderdeel een SAP-router vereist voor verbinding met een SAP-systeem, kunt u het onderdeel met behulp van de SAP-routertekenreeks configureren. Wanneer u bijvoorbeeld een SAP-machtigingssysteem configureert om rollen en gebruikers te importeren, kan de SAP-routerreeks vervangen worden door de naam van de toepassingsserver. Zo wordt verzekerd dat CMS via de SAP-router met het SAP-systeem communiceert.

Verwante informatie

Lokale SAP-gateways installeren [pagina 1018]

8.19.1.1 Gedetailleerde poortvereisten

Poortvereisten voor SAP

Het BI-platform gebruikt de SAP Java Connector (SAP JCO) voor communicatie met SAP NetWeaver. U moet de beschikbaarheid van de volgende poorten controleren en deze configureren:

- Luisterpoort voor SAP-gatewayservice (bijvoorbeeld 3300).
- Luisterpoort voor SAP-dispatcherservice (bijvoorbeeld 3200).

De volgende tabel bevat een overzicht van de specifieke poortconfiguraties die u nodig hebt.

Broncomputer	Poort	Doelcomputer	Poort	Actie
SAP	Willekeurig	Webtoepassingsserver van BI-platform	Webservice-HTTP/ HTTPS-poort	Toestaan
SAP	Willekeurig	CMS	CMS Name Server-poort	Toestaan
SAP	Willekeurig	CMS	CMS-aanvraagpoort	Toestaan
Webtoepassingsserver	Willekeurig	SAP	Gatewayservicepoort voor SAP-systeem	Toestaan
Central Management Server (CMS)	Willekeurig	SAP	Gatewayservicepoort voor SAP-systeem	Toestaan
Crystal Reports™	Willekeurig	SAP	Gatewayservicepoort voor SAP-systeem en dispatcherpoort voor SAP-systeem	Toestaan

8.19.2 Firewall-configuratie voor JD Edwards EnterpriseOne-integratie

Implementaties van het BI-platform die met JD Edwards-software communiceren, moeten aan deze algemene communicatievereisten voldoen:

- Central Management Console-webtoepassingen moeten communicatie met JD Edwards EnterpriseOne kunnen initiëren via de JDENET-poort en een willekeurig geselecteerde poort.
- Crystal Reports met het clientonderdeel Gegevensconnectiviteit moet communicatie met JD Edwards EnterpriseOne via de JDNET-poort kunnen initiëren. Voor het ophalen van gegevens moet de JD Edwards EnterpriseOne-zijde kunnen communiceren met het stuurprogramma via een willekeurige poort die niet kan worden gecontroleerd.
- De Central Management Server moet communicatie met JD Edwards EnterpriseOne kunnen initiëren via de JDENET-poort en een willekeurig geselecteerde poort.
- Het JDENET-poortnummer staat in het configuratiebestand voor de toepassingsserver van JD Edwards EnterpriseOne (`JDE.INI`) in de sectie JDENET.

Poortvereisten voor BI-platformservers

Product	Vereiste serverpoort
SAP BusinessObjects Business Intelligence-platform	Poort van aanmeldingsserver voor BI-platform.

Poortvereisten voor JD Edwards EnterpriseOne

Product	Poortvereiste	Beschrijving
JD Edwards EnterpriseOne	JDENET-poort en een willekeurig geselecteerde poort	Gebruikt voor communicatie tussen het BI-platform en JD Edwards EnterpriseOne-toepassingsserver.

De webtoepassingsserver configureren voor communicatie met JD Edwards

In deze sectie ziet u hoe u een firewall en het BI-platform configureert voor interoperabiliteit in een implementatiescenario waarin de firewall zich tussen de webtoepassingsserver en andere platformservers bevindt.

Voor firewallconfiguratie met BI-platformservers en clients raadpleegt u de sectie *Poortvereisten voor BI-platformservers* van deze handleiding. Naast de standaardfirewallconfiguratie moet voor communicatie met JD Edwards-servers een aantal extra poorten worden geopend.

Voor JD Edwards EnterpriseOne Enterprise

Broncomputer	Poort	Doelcomputer	Poort	Actie
CMS met de functie Beveiligingsconnectiviteit voor JD Edwards EnterpriseOne	Willekeurig	JD Edwards EnterpriseOne	Willekeurig	Toestaan
BI-platformservers met Gegevensconnectiviteit voor JD Edwards EnterpriseOne	Willekeurig	JD Edwards EnterpriseOne	Willekeurig	Toestaan
Crystal Reports met Gegevensconnectiviteit aan clientzijde voor JD Edwards EnterpriseOne	Willekeurig	JD Edwards EnterpriseOne	Willekeurig	Toestaan
Webtoepassingsserver	Willekeurig	JD Edwards EnterpriseOne	Willekeurig	Toestaan

8.19.3 Specifieke firewallrichtlijnen voor Oracle EBS

Uw implementatie van het BI-platform moet de volgende onderdelen toestaan om communicatie te initiëren met de luisterpoort van de Oracle-database.

- Webonderdelen van BI-platform
- CMS (met name de Oracle EBS-beveiligingsinvoegtoepassing)
- Back-endservers van BI-platform (met nam het onderdeel EBS-gegevenstoegang)
- Crystal Reports (met name het EBS Data Access-onderdeel)

> **Opmerking**
>
> De standaardwaarde van de listener-poort van de Oracle-database in alle bovenstaande vereisten is 1521.

8.19.3.1 Gedetailleerde poortvereisten

In aanvulling op de standaardfirewallconfiguratie voor het BI-platform moet een aantal extra poorten worden geopend om in een geïntegreerde Oracle EBS-omgeving te werken:

Broncomputer	Poort	Doelcomputer	Poort	Actie
Webtoepassingsserver	Willekeurig	Oracle EBS	Oracle-databasepoort	Toestaan
CMS met beveiligingsconnectiviteit voor Oracle EBS	Willekeurig	Oracle EBS	Oracle-databasepoort	Toestaan
BI-platformservers met gegevensconnectiviteit op de server voor Oracle EBS	Willekeurig	Oracle EBS	Oracle-databasepoort	Toestaan
Crystal Reports met gegevensconnectiviteit op de client voor Oracle EBS	Willekeurig	Oracle EBS	Oracle-databasepoort	Toestaan

8.19.4 Firewall-configuratie voor PeopleSoft Enterprise-integratie

Implementaties van het BI-platform die met PeopleSoft Enterprise communiceren, moeten aan de volgende algemene communicatieregels voldoen:

- De Central Management Server (CMS) met het onderdeel Beveiligingsconnectiviteit moet de communicatie met de PeopleSoft QAS-webservice (Query Access) kunnen starten.
- BI-platformservers met een Gegevensconnectiviteit-onderdeel moeten de communicatie met de PeopleSoft QAS-webservice kunnen starten.
- Crystal Reports met Gegevensconnectiviteit-clientonderdelen moet de communicatie met de PeopleSoft QAS-webservice kunnen starten.
- De Enterprise Management (EPM) Bridge moet met de CMS en de Input File Repository Server kunnen communiceren.
- De EPM Bridge moet kunnen communiceren met de PeopleSoft-database via een ODBC-verbinding.

Het poortnummer van de webservice is hetzelfde als de poort die in de domeinnaam van PeopleSoft Enterprise is opgegeven.

Poortvereisten voor BI-platformservers

Product	Vereiste serverpoort
SAP BI-platform	Poort van aanmeldingsserver voor BI-platform.

Poortvereisten voor PeopleSoft

Product	Poortvereiste	Beschrijving
PeopleSoft Enterprise: People Tools 8.46 of hoger	Webservice-HTTP/HTTPS-poort	Deze poort is vereist wanneer u een SOAP-verbinding voor PeopleSoft Enterprise met PeopleTools 8.46 en nieuwere oplossingen gebruikt

BI-platform en PeopleSoft voor firewalls configureren

In deze sectie ziet u hoe u het BI-platform en PeopleSoft Enterprise configureert voor interoperabiliteit in een implementatiescenario waarin de firewall zich tussen de webtoepassingsserver en andere BI-platformservers bevindt.

Raadpleeg de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor firewallconfiguratie met BI-platformservers en clients.

Naast de firewallconfiguratie met het BI-platform moet u extra configuraties uitvoeren.

Voor PeopleSoft Enterprise: PeopleTools 8.46 of hoger

Broncomputer	Poort	Doelcomputer	Poort	Actie
CMS met functie Beveiligingsconnectiviteit voor PeopleSoft	Willekeurig	PeopleSoft	HTTP-/HTTPS-poort voor PeopleSoft-webservice	Toestaan
BI-platformservers met Gegevensconnectiviteit voor PeopleSoft	Willekeurig	PeopleSoft	HTTP-/HTTPS-poort voor PeopleSoft-webservice	Toestaan
Crystal Reports met Gegevensconnectiviteit voor PeopleSoft aan clientzijde	Willekeurig	PeopleSoft	HTTP-/HTTPS-poort voor PeopleSoft-webservice	Toestaan
EPM-brug	Willekeurig	CMS	Poort voor CMS-naamserver	Toestaan
EPM-brug	Willekeurig	CMS	CMS-aanvraagpoort	Toestaan
EPM-brug	Willekeurig	Input File Repository Server	Poort voor invoer-FRS	Toestaan
EPM-brug	Willekeurig	PeopleSoft	PeopleSoft-database-poort	Toestaan

8.19.5 Firewall-configuratie voor Siebel-integratie

In deze sectie ziet u welke poorten gebruikt worden voor de communicatie tussen BI-platform en Siebel eBusiness Application-systemen wanneer deze door firewalls worden gescheiden.

- De webtoepassing moet communicatie met de aanmeldingsserver van BI-platform voor Siebel kunnen starten. Voor de BusinessObjects Enterprise-aanmeldingsserver voor Siebel zijn drie poorten vereist:
  1. de echopoort (TCP) 7 voor toegangscontrole tot de aanmeldingsserver,
  2. de poort voor de aanmeldingsserver van het BI-platform voor Siebel (standaard 8448) voor CORBA IOR-luisterpoort
  3. en een willekeurige POA-poort voor CORBA-communicatie die niet gecontroleerd kan worden, zodat alle poorten moeten openstaan.
- De CMS moet communicatie met de aanmeldingsserver van BI-platform voor Siebel kunnen starten. CORBA IOR-luisterpoort voor elke aanmeldingsserver (bijvoorbeeld: 8448). U moet ook een willekeurig POA-poortnummer openen dat pas na installatie van BI-platform bekend wordt gemaakt.
- De aanmeldingsserver van BI-platform voor Siebel moet communicatie kunnen starten met de SCBroker-poort (Siebel connection broker), bijvoorbeeld 2321.
- De backend-servers van BI-platform (onderdeel voor Siebel-gegevenstoegang) moeten communicatie kunnen starten met de SCBroker-poort (Siebel connection broker), bijvoorbeeld 2321.
- Crystal Reports-rapporten (onderdeel voor Siebel-gegevenstoegang) moeten communicatie kunnen starten met de SCBroker-poort (Siebel connection broker), bijvoorbeeld 2321.

Gedetailleerde beschrijving van poorten

In deze sectie ziet u de poorten die door BI-platform worden gebruikt. Als u het BI-platform implementeert met firewalls, kunt u aan de hand van deze informatie het minimumaantal poorten in de firewalls openen dat is vereist voor specifieke integratie met Siebel.

Poortvereisten voor BI-platformservers

Product	Vereiste serverpoort
SAP BI-platform	Poort van aanmeldingsserver voor BI-platform.

Poortvereiste voor Siebel

Product	Poortvereiste	Beschrijving
Siebel eBusiness-toepassing	2321	Standaard SCBroker-poort (Siebel connection broker)

BI-platformfirewalls configureren voor integratie met Siebel

In deze sectie ziet u hoe u een firewall voor Siebel en het BI-platform configureert voor interoperabiliteit in een implementatiescenario waarin de firewall zich tussen de webtoepassingsserver en andere platformservers bevindt.

Broncomputer	Poort	Doelcomputer	Poort	Actie
Webtoepassingsserver	Willekeurig	Aanmeldingsserver van BI-platform voor Siebel	Willekeurig	Toestaan

Broncomputer	Poort	Doelcomputer	Poort	Actie
CMS	Willekeurig	Aanmeldingsserver van BI-platform voor Siebel	Willekeurig	Toestaan
Aanmeldingsserver van BI-platform voor Siebel	Willekeurig	Siebel	SCBroker-poort	Toestaan
BI-platformservers met gegevensconnectiviteit aan serverzijde voor Siebel	Willekeurig	Siebel	SCBroker-poort	Toestaan
Crystal Reports met gegevensconnectiviteit aan clientzijde voor Siebel	Willekeurig	Siebel	SCBroker-poort	Toestaan

8.20 Het BI-platform en omgekeerde proxyservers

Het BI-platform kan worden geïmplementeerd in een omgeving met een of meer omgekeerde proxyservers. Een omgekeerde proxyserver wordt meestal vóór de webtoepassingsserver geïmplementeerd, zodat deze één IP-adres kunnen gebruiken. Door deze configuratie wordt alle internetverkeer dat gericht is aan privéwebtoepassingsservers via de omgekeerde proxyserver geleid en blijven privé IP-adressen verborgen.

Omdat de omgekeerde proxyserver openbare URL's omzet in interne URL's, moet de server worden geconfigureerd met de URL's van de webtoepassingen van BI-platform die in het interne netwerk zijn geïmplementeerd.

8.20.1 Inzicht in de implementatie van webtoepassingen

Webtoepassingen van BI-platform worden geïmplementeerd op een webtoepassingsserver. De toepassingen worden automatisch tijdens de installatie geïmplementeerd via het WDeploy-hulpprogramma. Het hulpprogramma kan ook worden gebruikt om de toepassingen handmatig te implementeren nadat het BI-platform geïmplementeerd is. Op een standaard Windows-installatie bevinden de webtoepassingen zich in de volgende map:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps
```

WDeploy wordt gebruikt om dergelijke WAR-bestanden te implementeren:

- `BOE`: bevat de CMC (Central Management Console), BI-startpunt en Open Document
- `dswsbobje`: bevat de toepassing Webservices

Als de webtoepassingsserver zich achter een omgekeerde proxyserver bevindt, moet u de juiste contextpaden van de WAR-bestanden opgeven in de configuratie van de omgekeerde proxyserver. Configureer een contextpad voor elk geïmplementeerd WAR-bestand van BI-platform om alle functies van BI-platform beschikbaar te maken.

8.21 Omgekeerde proxyserver configureren voor webtoepassingen van BI-platform

In implementaties waar webtoepassingen van BI-platform zich achter een omgekeerde proxyserver bevinden, moet de omgekeerde proxyserver worden geconfigureerd om inkomende URL-aanvragen toe te wijzen aan de juiste webtoepassing.

Deze sectie bevat specifieke configuratievoorbeelden voor een aantal ondersteunde omgekeerde proxyservers. Raadpleeg de documentatie bij de omgekeerde proxyserver voor meer informatie.

8.21.1 Gedetailleerde instructies voor de configuratie van omgekeerde proxyservers

De WAR-bestanden configureren

Webtoepassingen van BI-platform worden als WAR-bestanden geïmplementeerd op een webtoepassingsserver. Configureer op de omgekeerde proxyserver een instructie voor het WAR-bestand dat door de implementatie wordt vereist. U kunt WDeploy gebruiken om de `BOE` of `dswsbobje` WAR-bestanden te implementeren. Zie de *Implementatiehandleiding voor BI-platformwebtoepassingen* voor meer informatie over WDeploy.

BOE-eigenschappen opgeven in de aangepaste configuratiemap

Het `BOE.war`-bestand bevat algemene en toepassingsspecifieke eigenschappen. Gebruik de aangepaste configuratiemap als u een van deze eigenschappen moet wijzigen. De map bevindt zich standaard in: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **⚠ Let op**
>
> Wijzig de eigenschappen in de map `config\default` niet om te voorkomen dat bestanden in de standaardmap worden overschreven. Gebruikers moeten de `aangepaste` map gebruiken.

> **ⓘ Opmerking**
>
> Op sommige webtoepassingsservers zoals de Tomcat-versie die is gebundeld met het BI-platform, kunt u het `BOE.war`-bestand rechtstreeks openen. In deze situatie kunt u aangepaste instellingen rechtstreeks configureren, zonder de implementatie van het WAR-bestand te verwijderen. Kunt u `BOE.war` niet openen, dan moet u de implementatie ongedaan maken, het bestand aanpassen en het opnieuw implementeren.

Consistent gebruik van slashes (/)

Definieer de contextpaden voor de omgekeerde proxyserver op dezelfde manier als in de URL van een browser. Als de instructie bijvoorbeeld het teken / (slash) aan het einde van het gespiegelde pad op de omgekeerde proxyserver bevat, geeft u / ook op aan het einde van de URL van de browser.

Zorg ervoor dat het teken / consistent voorkomt in de bron-URL en de doel-URL in de instructie voor de omgekeerde proxyserver. Als het teken / wordt toegevoegd aan het einde van de bron-URL, moet het ook worden toegevoegd aan het einde van de doel-URL.

8.21.2 De omgekeerde proxyserver configureren

De onderstaande stappen zijn vereist voor de werking van de webtoepassingen van BI-platform achter een ondersteunde omgekeerde proxyserver.

1. Zorg ervoor dat de omgekeerde proxyserver is geconfigureerd conform de aanwijzingen van de leverancier en de netwerktopologie van de implementatie.
2. Bepaal welk WAR-bestand van BI-platform vereist is.
3. Configureer de reverse-proxyserver voor elk WAR-bestand van BI-platform. Let op: op elk type omgekeerde proxyserver worden de regels anders opgegeven.
4. Geef zo nodig speciale configuratie-instellingen op. Sommige webtoepassingen vereisen speciale configuratie wanneer ze op bepaalde webtoepassingsservers worden geïmplementeerd.

8.21.3 De reverse-proxyserver van Apache 2.2 configureren voor het BI-platform

Deze sectie biedt een werkstroom voor de configuratie van interoperabiliteit tussen het BI-platform en Apache 2.2.

1. Het BI-platform en Apache 2.2 moeten elk op een andere computer zijn geïnstalleerd.
2. Apache 2.2 moet als een omgekeerde proxyserver zijn geïnstalleerd en geconfigureerd, zoals beschreven in de documentatie van de leverancier.
3. Configureer `ProxyPass` voor elk WAR-bestand dat zich achter de omgekeerde proxyserver bevindt.
4. Open het bestand *httpd.conf* dat zich onder de proxyinstallatiemap Apache Reverse bevindt.
5. Configureer `ProxyPassReverseCookiePath` voor elke webtoepassing die zich achter de omgekeerde proxyserver bevindt. Bijvoorbeeld:

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.21.4 De omgekeerde proxyserver van WebSEAL 6.0 configureren voor het BI-platform

In deze sectie wordt uitgelegd hoe u het BI-platform en WebSeal 6.0 configureert voor interoperabiliteit.

De aanbevolen configuratiemethode is om één standaardkoppeling te maken waarmee alle webtoepassingen van BI-platform die op een interne webtoepassingsserver of webserver worden gehost, aan één koppelpunt worden toegewezen.

1. Het BI-platform en WebSEAL 6.0 moeten elk op een andere computer zijn geïnstalleerd.

   Hoewel het mogelijk is het BI-platform en WebSEAL 6.0 op dezelfde computer te implementeren, maar dit wordt niet aanbevolen. Raadpleeg de documentatie bij WebSEAL 6.0 voor aanwijzingen bij de configuratie van dit implementatiescenario.
2. Zorg ervoor dat WebSEAL 6.0 geïnstalleerd en geconfigureerd is zoals beschreven in de documentatie van de leverancier.
3. Start het WebSEAL-opdrachtregelprogramma *pdadmin*. Meld u als gebruiker met beheerdersrechten aan bij een beveiligd domein, bijvoorbeeld *sec_master*.
4. Geef de volgende opdracht op bij de aanwijzing *pdadmin sec_master*:

   ```
   server task <instance_name-webseald-host_name> create -t
   <type> -h <host_name> -p <port> <junction_point>
   ```

   waarbij

   - `<naam_exemplaar-webseald-naam_host>` de volledige servernaam is van het geïnstalleerde WebSEAL-exemplaar. Gebruik voor deze volledige servernaam dezelfde notatie die ook is gebruikt in de uitvoer van de opdracht `server list`.
   - `<type>` is het type koppelingspunt. Geef `tcp` op als het koppelingspunt verwijst naar een interne HTTP-poort. Geef `ssl` op als het koppelingspunt verwijst naar een interne HTTPS-poort.
   - `<naam_host>` is de DNS-hostnaam of het IP-adres van de interne server waar de aanvragen worden ontvangen.
   - `<poort>` is de TCP-poort van de interne server waar de aanvragen worden ontvangen.
   - `<koppelingspunt>` is de map in de door WebSEAL beveiligde objectruimte waar de documentruimte van de interne server zich bevindt.

Voorbeeld

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.21.5 Microsoft ISA 2006 configureren voor het BI-platform

In deze sectie wordt uitgelegd hoe u het BI-platform en ISA 2006 configureert voor interoperabiliteit.

De aanbevolen configuratiemethode is om één standaardkoppeling te maken waarmee alle WAR-bestanden van BI-platform die op een interne webtoepassingsserver of webserver worden gehost, aan één koppelpunt

worden toegewezen. Afhankelijk van uw webtoepassingsserver is er extra configuratie vereist voor de toepassingsserver, zodat deze kan worden gebruikt met ISA 2006.

1. Het BI-platform en ISA 2006 moeten elk op een andere computer zijn geïnstalleerd.

   Hoewel het mogelijk is het BI-platform en ISA 2006 op dezelfde computer te implementeren, wordt dit niet aanbevolen. Raadpleeg de documentatie bij ISA 2006 voor instructies bij de configuratie van dit implementatiescenario.
2. ISA 2006 moet worden geïnstalleerd en geconfigureerd zoals wordt beschreven in de documentatie van de leverancier.
3. Start het serverbeheerprogramma voor ISA.
4. Gebruik het navigatievenster om een nieuwe publicatieregel te starten.
   a. Ga naar

      Matrices > *Computernaam* > *Firewallbeleid* > *Nieuw* > *Publicatieregel voor websites*

      > **→ Onthouden**
      >
      > Vervang `Computernaam` door de naam van de computer waarop ISA 2006 is geïnstalleerd.

   b. Typ een regelnaam bij *Regelnaam Web-publicaties* en klik op *Volgende*.
   c. Selecteer *Toestaan* als regelactie en klik op *Volgende*.
   d. Selecteer *Eén website of taakverdeling publiceren* als publicatietype en klik op *Volgende*.
   e. Selecteer een verbindingstype tussen de ISA-server en de gepubliceerde website en klik op *Volgende*.

      Selecteer bijvoorbeeld *Niet-beveiligde verbindingen gebruiken voor het maken van verbinding met de gepubliceerde server-farm*.
   f. Typ de interne naam van de website die u publiceert (bijvoorbeeld computernaam waarop BI-platform wordt gehost) in *Interne naam website* en klik op *Volgende*.

      > **ⓘ Opmerking**
      >
      > Als de computer waarop ISA 2006 wordt gehost, geen verbinding kan maken met de doelserver, selecteert u *Een computernaam of IP-adres gebruiken om verbinding te maken met de gepubliceerde server* en typt u de naam of het IP-adres in het desbetreffende veld.

   g. Selecteer de domeinnaam in *Openbare naamgegevens* (bijvoorbeeld *Een domeinnaam*) en geef interne publicatiegegevens op (bijvoorbeeld `/*`). Klik op *Volgende*.
      U moet nu een nieuwe web-listener maken om te controleren op inkomende webaanvragen.
5. Klik op *Nieuw* om de wizard Definitie van nieuwe web-listener te starten.
   a. Typ een naam in *Naam web-listener* en klik op *Volgende*.
   b. Selecteer een verbindingstype tussen de ISA-server en de gepubliceerde website en klik op *Volgende*.

      Selecteer bijvoorbeeld *Beveiligde SSL-verbindingen met clients niet vereist*.
   c. Selecteer de volgende optie in de sectie *IP-adressen web-listener* en klik op *Volgende*.
      - Interne
      - Extern
      - Lokale host
      - Alle netwerken

      De ISA-server is nu geconfigureerd voor publicaties alleen via HTTP.
   d. Selecteer een optie bij *Verificatie-instelling*, klik op *Volgende* en dan op *Voltooien*.
      De nieuwe listener is nu geconfigureerd voor de webpublicatieregel.

6. Klik op *Volgende* in *Gebruikerssets* en klik op *Voltooien*.
7. Klik op *Toepassen* om alle instellingen voor de webpublicatieregel op te slaan en de ISA 2006-configuratie bij te werken.
   U moet nu de eigenschappen van de webpublicatieregel bijwerken om paden toe te wijzen aan de webtoepassingen.
8. Klik in het navigatievenster met de rechtermuisknop op het geconfigureerde firewallbeleid en selecteer *Eigenschappen*.
9. Klik in het tabblad *Paden* op *Toevoegen* om routes toe te wijzen aan SAP BusinessObjects-webtoepassingen.
10. Selecteer op het tabblad *Openbare naam* de optie *Aanvraag voor de volgende websites* en klik op *Toevoegen*.
11. Voer in het dialoogvenster *Openbare naam* de servernaam voor ISA 2006 in en klik op *OK*.
12. Klik op *Toepassen* om alle instellingen voor de webpublicatieregel op te slaan en de ISA 2006-configuratie bij te werken.
13. Controleer de verbindingen door de volgende URL te openen:

    `http://<Hostnaam ISA-server>:<poortnummer web-listener>/<Extern pad van de toepassing>`

    Bijvoorbeeld: **`http://mijnISAserver:80/Product/BOE/CMC`**

    > **Opmerking**
    >
    > U moet de browser mogelijk een aantal keer vernieuwen.

U moet het HTTP-beleid wijzigen voor de regel die u zojuist hebt geconfigureerd om ervoor te zorgen dat u zich kunt aanmelden bij de CMC. Klik met de rechtermuisknop op de regel die u in het serverbeheerprogramma van ISA hebt gemaakt en selecteer *HTTP configureren*. Schakel nu *Normalisatie verifiëren* uit in het gebied *URL-beveiliging*.

Als u extern toegang wilt krijgen tot het BI-platform, moet u een toegangsregel maken.

8.22 Speciale configuratie voor het BI-platform in implementaties met omgekeerde proxy's

Bepaalde BI-platformproducten vereisen aanvullende configuratie om correct te functioneren in implementaties met omgekeerde proxyservers. In deze sectie vindt u aanwijzingen voor het uitvoeren van deze aanvullende configuratie.

8.22.1 Omgekeerde proxy voor webservices inschakelen

In deze sectie worden de vereiste procedures beschreven voor het inschakelen van omgekeerde proxy's voor webservices.

8.22.1.1 Reverse proxy inschakelen op Tomcat

Als u omgekeerde proxy's wilt inschakelen op de Tomcat-webtoepassingsserver, past u het bestand `Server.xml` aan. Vereiste wijzigingen zijn onder meer het instellen van `proxyPort` als luisterpoort voor de reverseproxyserver en het toevoegen van een nieuwe `proxyName`. In deze sectie wordt de procedure beschreven.

1. Stop Tomcat.
2. Open het bestand `Server.xml` voor Tomcat.

   In Windows bevindt `server.xml` zich in: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   In Unix `server.xml` bevindt zich in `<CATALINA_HOME>/conf`. De standaardwaarde van `<CATALINA_HOME>` is `<INSTALLATIEMAP>/sap_bobj/tomcat`.
3. Zoek deze sectie in het bestand Server.xml:

```
<!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

4. Behandel het connectorelement als sourcecode door `<!--` en `-->` te verwijderen.
5. Wijzig de waarde van `proxyPort` in de luisterpoort van de reverseproxyserver.
6. Voeg een nieuw `proxyName`-attribuut toe aan de attribuutlijst van de connector. De waarde van de `proxyName` moet de naam van de proxyserver zijn, die door Tomcat moet kunnen worden geconverteerd in het juiste IP-adres.

   Voorbeeld:

```
<!--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" />
```

   Waarbij `my_reverse_proxy_server.domain.com` en `ReverseProxyServerPort` moeten worden vervangen door de juiste naam en luisterpoort van de reverseproxyserver.
7. Sla het bestand `server.xml` op en sluit het.
8. Start Tomcat opnieuw.

9. Zorg ervoor dat het virtuele pad van de omgekeerde proxyserver wordt toegewezen aan de juiste Tomcat-verbindingspoort. In het bovenstaande voorbeeld is dit poort 8082.

   Hieronder ziet u een voorbeeldconfiguratie voor Apache HTTP Server 2.2, waarmee een omgekeerde proxy wordt ingesteld voor SAP BusinessObjects™-webservices die zijn geïmplementeerd op Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/
dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Als u webservices wilt inschakelen, moeten de proxynaam en het poortnummer worden aangegeven voor de connector.

8.22.1.2 Omgekeerde proxy inschakelen voor webservices op andere webtoepassingsservers dan Tomcat

Voor de volgende procedure is het vereist dat webtoepassingen van BI-platform juist zijn geconfigureerd voor de gekozen webtoepassingsserver. Bij `wsresources` wordt onderscheid gemaakt tussen hoofdletters en kleine letters.

1. Stop de webtoepassingsserver.
2. Geef de externe URL van de webservices op in het bestand `dsws.properties`.

   Dit bestand bevindt zich in de webtoepassing `dswsbobje`. Als de externe URL bijvoorbeeld `http://my_reverse_proxy_server.domain.com/dswsbobje/` is, werkt u de eigenschappen bij in het bestand 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. Sla het bestand `dsws.properties` op en sluit het.
4. Start de webtoepassingsserver opnieuw.
5. Zorg ervoor dat het virtuele pad van de omgekeerde proxyserver wordt toegewezen aan de juiste verbindingspoort van de webtoepassingsserver. In het volgende voorbeeld wordt een voorbeeldconfiguratie weergegeven voor de Apache HTTP-server 2.2 om een omgekeerde proxy uit te voeren op webservices van BI-platform die zijn geïmplementeerd op de gekozen webtoepassingsserver:

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<luisterpoort> /dswsbobje
   ```

   ```
   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

Hierbij is `<luisterpoort>` de luisterpoort van de webtoepassingsserver.

8.22.2 Het basispad voor sessiecookies inschakelen voor ISA 2006

In deze sectie wordt beschreven hoe u specifieke webtoepassingsservers zo kunt configureren dat u het basispad voor sessiecookies kunt gebruiken met ISA 2006 als reverse-proxyserver.

8.22.2.1 Apache Tomcat configureren

Voeg het volgende toe aan het element `<Connector>` element in `server.xml` om het basispad voor sessiecookies te configureren voor gebruik met ISA 2006 als reverse-proxyserver:

```
emptySessionPath="true"
```

1. Stop Tomcat.
2. Open server.xml, dat zich bevindt in:

   `<HOOFDMAP_CATALINA>\conf`
3. Zoek naar de volgende sectie in het bestand 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. Hef de opmerking bij het verbindingselement op door `<!--` en `-->` te verwijderen.
5. Voeg het volgende toe aan het element `<Connector>` element in `server.xml` om het basispad voor sessiecookies te configureren voor gebruik met ISA 2006 als reverse-proxyserver:

   ```
   emptySessionPath="true"
   ```
6. Stel de waarde van `proxyPort` in op de luisterpoort van de omgekeerde proxyserver.
7. Voeg een nieuw attribuut `proxyName` toe aan de attribuutlijst van de connector. De waarde moet de naam van de proxyserver zijn die via Tomcat moet kunnen worden omgezet in een juist IP-adres.

   Bijvoorbeeld:

   ```
   <!--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. Sla het bestand `Server.xml` op en sluit het.
9. Start Tomcat opnieuw.

Zorg ervoor dat het virtuele pad van de omgekeerde proxyserver wordt toegewezen aan de juiste Tomcat-verbindingspoort. In het bovenstaande voorbeeld is dit poort 8082.

8.22.2.2 Sun Java 8.2 configureren

U moet het bestand `sun-web.xml` wijzigen voor elke webtoepassing van BI-platform.

1. Ga naar `<SUN_WEBAPP_DOMAIN>`\generated\xml\j2ee-modules\webapps\BOE\WEB-INF
2. Open `sun-web.xml`.
3. Voeg het volgende toe na de container `<context-root>`:

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
        </session-config>
   <property name="reuseSessionID" value="true"/>
```

4. Sla `sun-web.xml` op en sluit het.
5. Herhaal stap 1-4 voor elke webtoepassing.

8.22.2.3 Oracle Application Server 10gR3 configureren

U moet het bestand `global-web-application.xml` of `orion-web.xml` wijzigen voor elke implementatiemap van de webtoepassingen van BI-platform.

1. Ga naar `<ORACLE_HOME>\j2ee\home\config\`
2. Open `global-web-application.xml` of `orion-web.xml`.
3. Voeg de volgende regel toe aan de container `<orion-web-app>`:

```
<session-tracking cookie-path="/" />
```

4. Sla het configuratiebestand op en sluit het.
5. Meld u aan bij de beheerconsole van Oracle:
   a. Ga naar *OC4J:home* > *Beheer* > *Servereigenschappen*.
   b. Selecteer *Opties* onder *Opdrachtregelopties*.
   c. Klik op *Nog een rij toevoegen* en typ het volgende:

```
Doracle.useSessionIDFromCookie=true
```

6. Start de Oracle-server opnieuw op.

8.22.2.4 WebSphere Community Edition 2.0 configureren

1. Open de beheerconsole van WebSphere Community Edition 2.0.
2. Zoek naar *Server* in het linkernavigatievenster en selecteer *Webserver*.
3. Selecteer de connectors en klik op *Bewerken*.
4. Schakel het selectievakje *emptySessionPath* in en klik op *Opslaan*.
5. Typ de ISA-servernaam in *ProxyName*.
6. Typ het ISA-luisterpoortnummer in *ProxyPort*.
7. Stop de connector en start deze opnieuw.

8.22.3 Omgekeerde proxy inschakelen voor SAP BusinessObjects Live Office

Als u de functie Object weergeven in webbrowser van SAP BusinessObjects Live Office wilt inschakelen voor omgekeerde proxy's, moet u de standaardviewer-URL aanpassen. U kunt dit doen in de Central Management Console (CMC) of via Live Office-opties.

> **Opmerking**
>
> In deze sectie wordt ervan uitgegaan dat de omgekeerde proxy's voor het BI-startpunt en de webservices van BI-platform zijn ingeschakeld.

8.22.3.1 De standaardviewer-URL aanpassen in de CMC

1. Meld u aan bij de CMC.
2. Klik op de pagina *Toepassingen* op *Central Management Console*.
3. Selecteer *Acties* > *Verwerkingsinstellingen*.
4. Selecteer de juiste URL van de standaard-URL in het veld *URL* en klik op *Opslaan en sluiten*.
   Bijvoorbeeld:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   Hierbij zijn `ReverseProxyServer` en `ReverseProxyServerPort` de juiste naam van de omgekeerde proxyserver en de luisterpoort.

9 Verificatie

9.1 Verificatieopties in het BI-platform

Verificatie is het proces waarbij de identiteit wordt gecontroleerd van een gebruiker die probeert toegang tot het systeem te krijgen, en rechtenbeheer is het proces waarbij wordt gecontroleerd of de gebruiker voldoende rechten heeft om de gevraagde actie voor het opgegeven object uit te voeren.

Met beveiligingsinvoegtoepassingen kunt u de manier waarop het BI-platform gebruikers verifieert uitbreiden en aanpassen. Beveiligingsinvoegtoepassingen vergemakkelijken de aanmaak en het beheer van accounts doordat u gebruikersaccounts en groepen van externe systemen kunt toewijzen in het platform. U kunt externe gebruikersaccounts of groepen toewijzen aan bestaande BI-platformgebruikersaccounts of -groepen, of u kunt nieuwe Enterprise-gebruikersaccounts of -groepen maken die overeenkomen met alle toegewezen vermeldingen in het externe systeem.

De huidige versie ondersteunt de volgende verificatiemethoden:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Omdat het BI-platform volledig aanpasbaar is, kunnen de verificatie en processen per systeem verschillen.

9.1.1 Primaire verificatie

De primaire verificatie vindt plaats wanneer een gebruiker voor het eerst probeert toegang tot het systeem te krijgen. Tijdens primaire verificatie kan een van de volgende twee dingen gebeuren:

- Als eenmalige aanmelding niet is geconfigureerd, geeft de gebruiker zijn of haar referenties op, zoals gebruikersnaam, wachtwoord en verificatietype.
  Deze gegevens worden door de gebruikers ingevoerd op het aanmeldingsscherm.

  > **Opmerking**
  >
  > Standaard wordt alleen de wachtwoordinstelling dat wachtwoorden mogen bestaan uit hoofd- en kleine letters gecontroleerd, tenzij deze is gewijzigd door de beheerder. Hiervoor moet het wachtwoord uit ten minste één hoofdletter en één kleine letter bestaan. Zo nodig kan de beheerder aanvullende wachtwoordinstellingen afdwingen.

- Als er een methode voor eenmalige aanmelding is geconfigureerd, worden de referenties voor de gebruikers in stilte verspreid.
  Deze gegevens worden opgehaald via andere methoden, zoals Kerberos of SiteMinder.

De verificatietypen die kunnen worden opgegeven zijn Enterprise, LDAP, Windows AD, SAP, Oracle, EBS, Siebel, JD Edwards Enterprise One en PeopleSoft Enterprise, afhankelijk van de typen die u hebt ingesteld in het beheergebied Verificatie van de CMC (Central Management Console). De gegevens worden via HTTP door de webbrowser van de gebruiker naar uw webserver verzonden. De gegevens worden vervolgens vanaf de webserver via de webconnector naar de juiste platformserver verzonden.

De webtoepassingsserver stuurt de gegevens van de gebruiker door naar een script op de server. Dit script communiceert intern met de SDK en uiteindelijk met de juiste beveiligingsinvoegtoepassing om de gegevens van de gebruiker te verifiëren in de gebruikersdatabase.

Als de gebruiker zich bijvoorbeeld bij het BI-startpunt aanmeldt en daarbij Enterprise-verificatie opgeeft, zorgt de SDK ervoor dat de verificatie wordt uitgevoerd door de beveiligingsinvoegtoepassing van BI-platform. De CMS (Central Management Server) gebruikt de beveiligingsinvoegtoepassing om de gebruikersnaam en het wachtwoord te verifiëren met behulp van de systeemdatabase. Als de gebruiker echter een andere verificatiemethode opgeeft, gebruikt de SDK de overeenkomstige beveiligingsinvoegtoepassing om de gebruiker te verifiëren.

Wanneer door de beveiligingsinvoegtoepassing wordt doorgegeven dat de referenties kloppen, krijgt de gebruiker door de CMS een actieve systeemidentiteit toegewezen en voert de CMS de volgende acties uit:

- De CMS maakt een Enterprise-sessie voor de gebruiker. Terwijl de sessie actief is, is er voor deze sessie één gebruikerslicentie in het systeem nodig.
- De CMS genereert en codeert een aanmeldingstoken en verzendt dit naar de webtoepassingsserver.
- De webtoepassingsserver slaat de gegevens van de gebruiker op in een sessievariabele in het geheugen. Een actieve sessie slaat gegevens op die in BI-platform worden gebruikt om te reageren op aanvragen van de gebruiker.

  > ⓘ Opmerking
  >
  > De sessievariabele bevat niet het wachtwoord van de gebruiker.

- De webtoepassingsserver slaat de aanmeldingstoken op in een cookie op de browser van de client. Dit wordt uitsluitend gedaan omwille van failover, zoals wanneer u een geclusterde CMS hebt of wanneer BI-startpunt is geclusterd voor sessieaffiniteit.

  > ⓘ Opmerking
  >
  > Het aanmeldingstoken kan worden uitgeschakeld Als u het aanmeldingstoken uitschakelt, wordt ook failover uitgeschakeld.

9.1.2 Beveiligingsinvoegtoepassingen

Met beveiligingsinvoegtoepassingen kunt u de manier waarop het BI-platform gebruikers verifieert, uitbreiden en aanpassen. Het BI-platform wordt momenteel geleverd met de volgende invoegtoepassingen:

- Enterprise
- LDAP

- Windows Active Directory
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Beveiligingsinvoegtoepassingen vereenvoudigen de aanmaak en het beheer van accounts doordat u gebruikersaccounts en groepen van externe systemen kunt toewijzen in het BI-platform. U kunt externe gebruikersaccounts of groepen toewijzen aan bestaande BI-platformgebruikersaccounts of -groepen, of u kunt nieuwe Enterprise-gebruikersaccounts of -groepen maken die overeenkomen met alle toegewezen vermeldingen in het externe systeem.

De externe gebruikers en groepen worden door de beveiligingsinvoegtoepassingen dynamisch onderhouden. Zodra u een externe groep aan het BI-platform toewijst, kunnen alle gebruikers in die groep zich aanmelden bij het BI-platform. Als u het lidmaatschap van de externe groep later wijzigt, hoeft u de groep niet nogmaals in het BI-platform bij te werken of te vernieuwen. Als u bijvoorbeeld een LDAP-groep in het BI-platform toewijst en vervolgens een nieuwe gebruiker aan de groep toevoegt, maakt de beveiligingstoepassing dynamisch een alias voor deze nieuwe gebruiker wanneer deze zich voor het eerst met geldige LDAP-referenties aanmeldt bij het BI-platform.

U kunt bovendien met beveiligingsinvoegtoepassingen op een consistente manier rechten toewijzen aan gebruikers en groepen, omdat voor de toegewezen gebruikers en groepen in Crystal Enterprise dezelfde regels gelden. U kunt bijvoorbeeld enkele gebruikersaccounts of groepen uit Windows AD en uit een LDAP-adreslijstserver toewijzen. Als u vervolgens in het BI-platform rechten wilt toekennen of nieuwe, aangepaste groepen wilt maken, kunt u alle instellingen opgeven in de CMC.

Elke beveiligingsinvoegtoepassing werkt als een verificatieprovider die de gebruikersreferenties in de juiste gebruikersdatabase controleert. Als gebruikers zich aanmelden bij het BI-platform, kunnen ze kiezen uit de beschikbare verificatietypen die u hebt ingesteld in het beheergebied Verificatie van de CMC.

> ⓘ Opmerking
>
> Gebruikers kunnen niet worden geverifieerd met de Windows AD-beveiligingsinvoegtoepassing als de serveronderdelen van BI-platform worden uitgevoerd op UNIX.

9.1.3 Eenmalige aanmelding bij het BI-platform

Eenmalige aanmelding bij het BI-platform wil zeggen dat gebruikers, wanneer ze zich eenmaal hebben aangemeld bij het besturingssysteem, toegang hebben tot toepassingen die SSO (Single Sign On: eenmalige aanmelding) ondersteunen zonder dat ze hun aanmeldingsgegevens opnieuw hoeven op te geven. Wanneer een gebruiker zich aanmeldt, wordt er een beveiligingscontext voor die gebruiker gemaakt. Deze context kan naar het BI-platform worden overgebracht om SSO uit te voeren.

De term “anonieme eenmalige aanmelding” heeft ook betrekking op eenmalige aanmelding bij het BI-platform, maar dan specifiek op eenmalige aanmelding voor de gebruikersaccount Guest. Wanneer de Guest-gebruikersaccount standaard is ingeschakeld, kan iedereen zich als gast aanmelden bij het BI-platform en heeft dan toegang tot het systeem.

9.1.3.1 Ondersteuning voor eenmalige aanmelding

De term eenmalige aanmelding wordt voor verschillende scenario's gebruikt. In de eerste plaats verwijst deze term naar een situatie waarin gebruikers slechts eenmaal hun aanmeldingsgegevens hoeven op te geven om toegang te krijgen tot twee of meer toepassingen of systemen. Hierdoor wordt het voor gebruikers gemakkelijker om met het systeem te werken.

Eenmalige aanmelding bij BI-startpunt is mogelijk via het BI-platform of via verschillende verificatiehulpprogramma's, afhankelijk van uw type toepassingsserver en besturingssysteem.

Deze methoden voor eenmalige aanmelding zijn beschikbaar wanneer u een Java-toepassingsserver onder Windows gebruikt:

- Windows Active Directory met Kerberos
- Windows AD met SiteMinder

De volgende methoden voor eenmalige aanmelding zijn beschikbaar als u de IIS gebruikt onder Windows:

- Windows Active Directory met Kerberos
- Windows Active Directory met NTLM
- Windows AD met SiteMinder

Deze methoden voor ondersteuning van eenmalige aanmelding zijn beschikbaar in Windows of UNIX, met een van de ondersteunde webtoepassingsservers voor het platform.

- LDAP met SiteMinder
- Vertrouwde verificatie
- Windows Active Directory met Kerberos
- LDAP via Kerberos op SUSE 11
- SAP NetWeaver SSO via Vertrouwde verificatie

> **Opmerking**
>
> Windows Active Directory met Kerberos wordt ondersteund als de Java-toepassing in UNIX wordt uitgevoerd. BI-platformservices moeten echter op een Windows-server worden uitgevoerd.

In de tabel hieronder vindt u de methoden voor eenmalige aanmelding die worden ondersteund door het BI-startpunt.

Verificatiemodus	CMS-server	Opties	Opmerkingen
Windows AD	Alleen Windows	Alleen Windows Active Directory met Kerberos	Windows Active Directory-verificatie voor het BI-startpunt en de CMC is standaard beschikbaar.
LDAP	Alle ondersteunde platforms	Alleen ondersteunde LDAP-directoryservers met SiteMinder	LDAP-verificatie voor het BI-startpunt en de CMC is standaard beschikbaar. Voor SSO bij BI-startpunt en CMC is SiteMinder vereist.
Enterprise	Alle ondersteunde platforms	Vertrouwde verificatie	Enterprise-verificatie voor het BI-startpunt en de CMC is standaard

Verificatiemodus	CMS-server	Opties	Opmerkingen
			beschikbaar. SSO met Enterprise-verificatie voor BI-startpunt en de CMC vereist Vertrouwde verificatie.

9.1.3.1.1 Eenmalige aanmelding voor CMC inschakelen

Volg de volgende stappen om SSO voor CMC in te schakelen:

De cache aan de clientzijde moet worden leeggemaakt voordat de eerste CMC-installatie wordt gestart. Anders wordt de Enterprise-verificatiemethode in de cache opgenomen.

Voer op de Tomcat-server de volgende stappen uit:

1. Ga in een systeem dat al is geconfigureerd voor SSO voor BILP naar `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom`.
2. Maak een bestand met de naam CmcApp.properties en vermeld hierin
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   .
3. Start Tomcat opnieuw op.

   SSO voor CMC is nu ingeschakeld.

> **Opmerking**
>
> Na een sessietime-out in het BI-startpunt of CMC (als SSO is ingeschakeld in beide gevallen) wordt de gebruiker gevraagd zich aan te melden. Als de wordt vernieuwd, wordt de gebruiker opnieuw aangemeld zonder dat deze opnieuw een wachtwoord moet opgeven. De ping-functie moet niet worden uitgeschakeld tijdens het proces.

9.1.3.2 Eenmalige aanmelding bij de database

Nadat gebruikers zijn aangemeld bij het BI-platform, kunnen ze via eenmalige aanmelding bij de database acties uitvoeren waarvoor databasetoegang nodig is, met name het weergeven en vernieuwen van rapporten, zonder dat ze opnieuw hun aanmeldingsgegevens hoeven op te geven. Eenmalige aanmelding bij de database kan met eenmalige aanmelding bij het BI-platform worden gecombineerd om gebruikers nog gemakkelijker toegang te bieden tot de bronnen die ze nodig hebben.

9.1.3.3 Eenmalige end-to-end-aanmelding

Eenmalige end-to-end-aanmelding verwijst naar een configuratie waarin gebruikers eenmalige toegang hebben tot zowel het BI-platform als tot de databases. Gebruikers hoeven in dit geval slechts eenmaal hun aanmeldingsgegevens op te geven, namelijk wanneer ze zich bij het besturingssysteem aanmelden, om toegang te krijgen tot het BI-platform en om acties te kunnen uitvoeren waarvoor databasetoegang nodig is, zoals het weergeven van rapporten.

In het BI-platform wordt eenmalige end-to-end-aanmelding ondersteund via Windows Active Directory en Kerberos.

9.2 Enterprise-verificatie

9.2.1 Enterprise-verificatie (overzicht)

Enterprise-verificatie is de standaardverificatiemethode voor het BI-platform. Het wordt automatisch ingeschakeld wanneer u het systeem voor de eerste keer installeert (het kan niet worden uitgeschakeld). Wanneer u gebruikers en groepen toevoegt en beheert, slaat het platform de gebruikers- en groepsgegevens op in een database.

> → Tip
>
> Gebruik de standaard Enterprise-verificatie van het systeem als u het liefst afzonderlijke accounts en groepen maakt voor gebruik met het BI-platform, of als u nog geen hiërarchie van gebruikers en groepen hebt gemaakt op een externe adreslijstserver.
>
> U hoeft Enterprise-verificatie niet te configureren of in te schakelen. U kunt de instellingen voor Enterprise-verificatie echter wel afstemmen op de specifieke beveiligingsbehoeften van uw onderneming. U kunt verificatie-instellingen van Enterprise alleen aanpassen via de CMC (Central Management Console).

9.2.2 Instellingen voor Enterprise-verificatie

Instellingen	Opties	Beschrijving
Wachtwoordbeperkingen	*Wachtwoorden afdwingen die bestaan uit hoofdletters en kleine letters*	Deze optie zorgt ervoor dat wachtwoorden ten minste één hoofdletter en één kleine letter bevatten. ⓘ Opmerking Standaard is deze optie ingeschakeld. Indien nodig kan

Instellingen	Opties	Beschrijving
		deze door de beheerder worden uitgeschakeld.
	Cijfer(s) in wachtwoord afdwingen	Deze optie zorgt ervoor dat wachtwoorden ten minste één numeriek teken bevatten.
	Specia(a)l(e) teken(s) in wachtwoord afdwingen	Deze optie zorgt ervoor dat wachtwoorden ten minste één speciaal teken bevatten.
	Moet ten minste N tekens bevatten, waarbij N is	De optie zorgt ervoor dat wachtwoorden ten minste N tekens lang zijn.
	Mag niet langer zijn dan N tekens, waarbij N is	Deze optie zorgt ervoor dat wachtwoorden niet langer mogen zijn dan N tekens.
	Mag niet de volgende tekenvolgorden bevatten	Deze optie zorgt ervoor dat het wachtwoord geen beperkte tekenvolgorden mag bevatten. De standaardwaarde hiervoor is als volgt: Wachtwoord 12345678 beheerder.
Gebruikersbeperkingen	*Moet wachtwoord elke N dag(en) wijzigen*	Met deze optie zorgt u ervoor dat wachtwoorden geen risico vormen en regelmatig vernieuwd worden.
	De laatste N wachtwoorden kunnen niet opnieuw worden gebruikt	Met deze optie zorgt u ervoor dat wachtwoorden niet routineus herhaald worden.
	Moet N minuten wachten voor wachtwoord kan worden gewijzigd	Met deze optie zorgt u ervoor dat nieuwe wachtwoorden niet direct nadat ze in het systeem zijn ingevoerd, kunnen worden gewijzigd.
	Moet wachtwoord na N dag(en) inactiviteit wijzigen	Deze optie zorgt ervoor dat het wachtwoord moet worden gewijzigd na N dagen van inactiviteit.
	Moet initieel wachtwoord na N dag(en) wijzigen	Deze optie zorgt ervoor dat het initiële wachtwoord moet worden gewijzigd na N dagen.
Aanmeldbeperkingen	*Account uitschakelen na N mislukte aanmeldingspogingen*	Met deze beveiligingsoptie bepaalt u hoeveel pogingen een gebruiker heeft om zich bij het systeem aan te melden voordat diens account wordt uitgeschakeld.
	Aantal mislukte aanmeldingspogingen na N minuten op nul stellen	Met deze optie geeft u aan na hoeveel tijd de teller voor aanmeldpogingen opnieuw wordt ingesteld.

Instellingen	Opties	Beschrijving
	Account na N minuten opnieuw inschakelen	Met deze optie geeft u aan hoe lang een account geblokkeerd blijft na N mislukte aanmeldpogingen.
Gegevensbronreferenties synchroniseren met aanmelding	*Gegevensbronreferenties van de gebruiker bij de aanmelding inschakelen en bijwerken*	Met deze optie worden gegevensbronreferenties ingeschakeld nadat de gebruiker is aangemeld.
Vertrouwde verificatie	*Vertrouwde verificatie is ingeschakeld*	Hier vindt u de instellingen voor vertrouwde verificatie.
OpenID Connect-verificatie	*OpenID Connect-verificatie is ingeschakeld*	Om *OpenID Connect-verificatie* in te schakelen, dient u het selectievakje *OpenID Connect-verificatie is ingeschakeld* in te schakelen. Wanneer u een verificatie uitvoert via OpenID Connect, wordt er een interne Enterprise-sessie gemaakt op het BI-platform.

9.2.3 Enterprise-instellingen wijzigen

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Enterprise*.
   Het dialoogvenster *Enterprise* wordt weergegeven.
3. Wijzig de instellingen.

   > → Tip
   >
   > Als u alle instellingen wilt terugzetten op hun standaardwaarden, klikt u op *Opnieuw instellen*.

4. Klik op *Bijwerken* om de wijzigingen op te slaan.

9.2.3.1 Algemene wachtwoordinstellingen wijzigen

> ⓘ Opmerking
>
> Accounts die langere tijd niet worden gebruikt, worden niet automatisch gedeactiveerd. Beheerders moeten inactieve accounts handmatig verwijderen.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Enterprise*.
   Het dialoogvenster *Enterprise* wordt weergegeven.
3. Schakel het selectievakje in voor elke wachtwoordinstelling die u wilt gebruiken en geef indien nodig een waarde op.

In de volgende tabel vindt u de minimum- en maximumwaarden voor de wachtwoordinstellingen die u kunt configureren.

Wachtwoordinstelling	Standaard	Minimum	Aanbevolen maximum
Mag niet de volgende tekenvolgorden bevatten	wachtwoord 12345678 beheerder	1 teken	25550 tekens
Moet ten minste N tekens bevatten	8 tekens	6 tekens	255 tekens
Mag niet langer zijn dan N tekens, waarbij N is:	255 tekens	13 tekens	255 tekens
Moet wachtwoord elke N dag(en) wijzigen	30 dagen	2 dagen	100 dagen
Mag de laatste N wachtwoorden niet opnieuw gebruiken	3 wachtwoorden	1 wachtwoord	100 wachtwoorden
Moet N minuten wachten voor wachtwoord kan worden gewijzigd	0 minuten	0 minuten	100 minuten
Moet wachtwoord na N dag(en) inactiviteit wijzigen	20 dagen	2 dagen	365 dagen
Moet initieel wachtwoord na N dag(en) wijzigen	7 dagen	2 dagen	15 dagen
Account uitschakelen na N mislukte aanmeldingspogingen	10 mislukte poging	1 mislukte poging	100 mislukte pogingen
Aantal mislukte aanmeldingspogingen na N minuten op nul stellen	5 minuten	1 minuut	100 minuten
Account na N minuten opnieuw inschakelen	5 minuten	0 minuten	100 minuten

4. Klik op *Bijwerken*.

9.2.4 SAML 2.0-verificatie

9.2.4.1 Eenmalige aanmelding uitvoeren via SAML 2.0

Het Business Intelligence-platform kan nu worden geïntegreerd als verificatiemechanisme voor eenmalige aanmelding met alle voor SAML ingeschakelde portals of toepassingen. Dit betekent dat u zich nu kunt

aanmelden bij een cloudtoepassing zoals Analytics Hub of SAP Analytics Cloud, en de bronnen tijdens dezelfde aanmeldingssessie kunt openen in BI-toepassingen zoals Fiorified BI-startpunt en OpenDocument.

U moet uw toepassingsserver configureren voor het uitvoeren van eenmalige aanmelding via SAML 2.0.

> **Opmerking**
>
> Stel de volgende vereisten in om de functie voor SAML-verificatie te gebruiken om u aan te melden via het e-mailadres van:
>
> - externe gebruikers.
> Gebruik de opdrachtregelparameter `"-importtpemailduringsync"` om de import van e-mailadressen uit externe systemen in te schakelen:
> 1. Voeg de parameter `"-importtpemailduringsync"` toe aan *CMS- > eigenschappen > Opdrachtregelparameters*.
> 2. Start de CMS opnieuw.
> 3. Werk de externe verificatie bij van de externe gebruiker waarvan u het e-mailadres wilt gebruiken om u aan te melden.
>
> De ondersteunde typen voor externe verificatie voor deze functie zijn SAP, LDAP en WinAD.
> - Enterprise-gebruikers.
> Zie SAP Note 2642247.

9.2.4.2 BI-platform configureren als SAML-serviceprovider

Om BI-platform te kunnen gebruiken als SAML-serviceprovider, moet u het platform configureren voor SAML 2.0-verificatie.

Met ingang van deze release zijn de stappen vereenvoudigd om een toepassingsserver te configureren als een SAML-serviceprovider. Hierbij zijn de volgende stappen verwijderd:

- SAML-JAR-bestanden kopiëren naar de installatiemap voor BI-platform
- Het bestand securitycontext.xml bewerken
- Het bestand web.xml bewerken

Dit betekent dat de SAML-JAR-bestanden, de XML-codes voor elke webtoepassing in het bestand securitycontext.xml en de filters in het bestand web.xml standaard beschikbaar zijn. Daarmee kunt u met het uitvoeren van de onderstaande stappen SAML 2.0-verificatie in- of uitschakelen voor elke webtoepassing via het eigenschappenbestand van elke webtoepassing.

> **Opmerking**
>
> Gebruik SAP Cloud Identity Provider als standaardidentiteitsprovider.

> **Opmerking**
>
> U kunt de Tomcat-. WebSphere- en JBoss-toepassingsserver gebruiken als SAML-serviceprovider.

1. Volg hiervoor de procedure in Vertrouwde verificatie met websessies configureren [pagina 243].
2. Als u SAP Cloud Platform Identity Provider gebruikt, exporteert u alle gebruikers en importeert u deze naar het BI-platform. Zie How to import users in bulk from Central Management Console.

Zie Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service voor informatie over het importeren van SAP Cloud Platform-gebruikers naar CSV.

3. Bewerk het eigenschappenbestand door `logon.webssoauthnetication.framework=None` te wijzigen in `logon.webssoauthnetication.framework=SAML`.

   - Ga voor het Fiorified BI-startpunt naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` en bewerk het bestand `fioriBI.properties`.
   - Ga voor OpenDocument naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` en bewerk het bestand `OpenDocument.properties`.
   - Ga voor CMC naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` en bewerk het bestand `CMCApp.properties`.

   > **Opmerking**
   >
   > Stel naast het toevoegen van `saml.enabled=true` de eigenschap `sso.supported.types = trustedSession` in de `CMC\FioriBI\OpenDocument`-eigenschappenbestanden in.

4. Als u de IDP-metagegevens wilt bijwerken in SP, download u de gegevens eerst van de betreffende IDP-serviceproviders en kopieert u het metagegevensbestand naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF` een wijzigt u de naam in `idp-meta-downloaded.xml`.

   Zie Tenant SAML 2.0 Configuration voor meer informatie over het downloaden van de IDP-metagegevens.

   > **Opmerking**
   >
   > Als het BI-platform wordt geïmplementeerd op een computer waarop geen Windows draait, moet u de scheidingstekens in het bestandspad naar de IDP-metagegevens onder de bean **FilesystemMetadataProvider** wijzigen in het bestand`securityContext.xml` onder `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
   >
   > Bijvoorbeeld: wijzig `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` in `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

   Als u een keystore wilt genereren om SAML 2.0 in te schakelen, raadpleegt u Een keystorebestand voor SAML 2.0 genereren [pagina 244].

5. (Optioneel) U kunt het e-mailadres gebruiken als een attribuut voor SAML-verklaring. Zie het onderwerp E-mailadres gebruiken als attribuut voor SAML-verklaring [pagina 245] voor meer informatie.
6. (Optioneel) Als u lastverdeling of een omgekeerde reverse-proxyserver gebruikt, raapleegt u 2621904 voor meer informatie.
7. Maak het WAR-bestand met het hulpprogramma wdeploy.
   a. Navigeer naar het pad `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Gebruik de juiste implementatieopdracht om het WAR-bestand voor toepassingsspecifieke versies te maken.

   - Voor Windows: `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

- Voor Unix: `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

> **Opmerking**
>
> Vervang <App_Server><Version_Name> door het type toepassingsserver en de bijbehorende versie. Gebruik bijvoorbeeld tomcat8 voor Tomcat-toepassingsserver v8.0. Evenzo kunt u jboss7 gebruiken voor JBoss-toepassingsserver v7.0 en websphere9 voor WebSphere-toepassingsserver v9.0.

8. Als het WAR-bestand is gemaakt, kopieert u dit en implementeert u het bestand op uw toepassingsserver.
9. Genereer de metagegevens van de serviceprovider en upload de gegevens.

> **Opmerking**
>
> U kunt de URL van de eigenschap-entiteitbasis in het bestand securitycontext.xml definiëren om de metagegevens van de serviceprovider te genereren met uw eindpunt-URL. Standaard worden de hostnaam en het poortnummer in de door u opgegeven URL gebruikt wanneer u de metagegevens van de serviceprovider downloadt.

   a. Ga naar `http(s)://host:port/BOE/saml/metadata`.

      Het XML-bestand wordt automatisch gedownload.
   b. Upload het XML-bestand naar de identiteitsprovider. Als u Microsoft Active Directory Federation Services als uw identiteitsprovider gebruikt, raadpleegt u Afhankelijke vertrouwensrelatie maken [pagina 246] voor meer informatie.

> **Opmerking**
>
> U kunt het standaardmetagegevensbestand voor serviceproviders `spring_saml_metadata.xml` uit `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` gebruiken in plaats van dit handmatig te genereren. U moet de XML-code`<replace_withip>` vervangen door het IP-adres of de hostnaam van de machine uit uw netwerk en `<replace_withport>` door het poortnummer van de toepassingsserver. Vervang HTTP door HTTPS als u HTTPS hebt ingeschakeld op de toepassingsserver.

10. Als u SAP Cloud Identity gebruikt en een SAML-toepassing wilt maken in IDP en de SP `metadata.xml` in de IDP wilt uploaden om de SAML-SSO voor BI-platform te configurerenhttps://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/f96e4c5930a94d1ba117e05a3f3c30fc.html, raadpleegt u Configure a Trusted Service Provider.

> **Opmerking**
>
> Genereer de meest recente serviceprovidermetagegevens nadat het keystore-bestand is gewijzigd.

> **→ Tip**
>
> Om te controleren of de SAML-integratie is geslaagd, wordt u doorgestuurd naar de IDP nadat u de voor SAML geconfigureerde toepassing (BI-startpunt, Fiorified BI-startpunt of OpenDocument) hebt gestart.

9.2.4.2.1 Vertrouwde verificatie met websessies configureren

U moet vertrouwde verificatie met websessies configureren als onderdeel van de configuratie van een toepassingsserver als SAML-serviceprovider.

> **Opmerking**
>
> Om veiligheidsredenen mag vertrouwde verificatie alleen worden ingeschakeld met HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

1. Maak het bestand `global.properties` onder de aangepaste map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.
2. Voer de volgende gegevens in als inhoud van het bestand `global.properties`:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

> **Opmerking**
>
> Onderhoud dezelfde waarden voor de parameters `trusted.auth.user.param` en `trusted.auth.shared.secret` zoals bijgewerkt in het bestand *custom.jsp*.

3. Ga naar *CMC* > *Verificatie* > *Enterprise*.
4. Stel een waarde tussen 0 en 365 (in *dagen*) in als de *Geldigheid*.
5. Kies *Nieuw gedeeld geheim*.
6. Kies *Gedeeld geheim downloaden* om het gegenereerde gedeelde geheim te downloaden.

   Het bestand `TrustedPrincipal.conf` wordt gedownload.
7. Kopieer en plak het bestand `TrustedPrincipal.conf` naar de locaties `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` en `\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Ga naar *CMC* > *Verificatie* > *Enterprise* en kies *Bijwerken*.
9. Werk het bestand custom.jsp bij met de sleutelwaarde van het gedeelde geheim voor het klassieke BI-startpunt en het Fiorified BI-startpunt. Zie Het bestand custom.jsp bewerken [pagina 400] voor meer informatie.

> **Opmerking**
>
> Werk het bestand custom.jsp bij als u Microsoft ADFS en Microsoft Azure gebruikt als identiteitsprovider.

9.2.4.2.2 Een keystorebestand voor SAML 2.0 genereren

Genereer uw eigen keystorebestand voor SAML 2.0 om het bestand te gebruiken.

Uitwisselingen via SAML maken gebruik van cryptografie om gegevens te ondertekenen en encrypteren. Een voorbeeld van een zelfondertekend keystorebestand, `sampletestKeystore.jks`, wordt meegeleverd met het product en is geldig tot 18 oktober 2019. `sampletestKeystore.jks` heeft een aliasnaam **Testkey** en wachtwoord **Password1**.

U kunt nu een zelfondertekend keystorebestand genereren met behulp van het Java-hulpprogramma Keytool.

1. Navigeer naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Voer de volgende opdracht uit: `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Opdracht	Beschrijving
-alias	Voer de aliasnaam van het certificaat in
-keypass	Voer het wachtwoord van het certificaat in
-keystore	De naam van het keystore bestand
-validity	Geldigheid van het certificaat
numberofdays	Het aantal dagen dat het zelfondertekende certificaat geldig is.

Beantwoord de volgende vragen nadat de opdracht is uitgevoerd:

- Voer het keystore-wachtwoord in. *****
- Voer het nieuwe wachtwoord opnieuw in: *****
- Wat zijn uw voornaam en achternaam? : **`MY_FIRST_AND_LAST_NAME`**
- Wat is de naam van uw organisatie-eenheid? : **`MY_ORGANIZATIONAL_UNIT`**
- Wat is de naam van uw organisatie? : **`MY_ORGANIZATION`**
- Wat is de naam van uw plaats of locatie? : **`MY_CITY`**
- Wat is de naam van uw staat of provincie? : **`MY_STATE`**
- Wat is de landcode van twee letters voor deze eenheid? : **`COUNTRY_CODE`**

Het keystorebestand wordt gegenereerd in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.

3. Verplaats het keystorebestand naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`
4. Wijzig het bestand `securityContext.xml` dat zich bevindt in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` met de nieuwe aliasnaam, wachtwoord en keystorebestandsnaam.

Zie de onderstaande XML-code:

{·} Voorbeeldcode

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Raadpleeg de onderstaande tabel om de argumenten te begrijpen:

XML-code	Beschrijving
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Hiermee zoekt u naar het keystorebestand
`<constructor-arg type="java.lang.String" value="Password1"/>`	Het wachtwoord voor het keystorebestand
`<entry key="aliasname" value="password"/>`	Aliaswachtwoord
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Alias van het standaardcertificaat

9.2.4.2.3 E-mailadres gebruiken als attribuut voor SAML-verklaring

U kunt e-mailverificatie op SAML inschakelen voor het Fiorified BI-startpunt, OpenDocument en de Central Management Console (CMC).

1. Afhankelijk van de toepassing waarin u werkt, werkt u het relevante eigenschappenbestand bij door deze twee regels toe te voegen:

```
saml.enabled=true
saml.isUseEmailAddress=true
saml.authType=secEnterprise
```

ⓘ Opmerking

`saml.isUseEmailAddress` gebruikt Boolean-waarden en `saml.authType` komt overeen met het verificatietype van de gebruikers-/aliasdetails waarmee moet worden aangemeld. De e-

> mailfunctie kan afzonderlijk worden afgehandeld voor alle bovenstaande toepassingen. Als `saml.isUseEmailAddress` is ingesteld op `false`, wordt er aangemeld op basis van de naamparameter. Indien ingesteld op `true`, wordt er aangemeld op basis van de e-mailparameter. `saml.authType` controleert op potentiële duplicaten en zorgt ervoor dat twee aliassen met hetzelfde verificatietype niet hetzelfde e-mailadres hebben.

- Voor het Fiorified BI-startpunt, `fioriBI.properties` onder `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Voor OpenDocument, `OpenDocument.properties` onder `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Voor de CMC, `CMCApp.properties` onder `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

> **Opmerking**
>
> Zorg er bij CMC voor dat de eigenschap `sso.supported.types = trustedSession` in het bestand `CMCApp.properties` wordt gezet.

2. Configureer de IDP voor e-mailondersteuning. U kunt ook de SAP Cloud Platform Identity Authentication-servicehandleiding raadplegen voor meer informatie als u SAP Cloud Identity Provider gebruikt.
   a. Open de beheerconsole-URL van de tenant voor SAP Cloud Platform Identity Authentication-service.

   > **Opmerking**
   >
   > De URL heeft de volgende notatie: `https://<tenant ID>.accounts.ondemand.com/admin` . De tenant-ID wordt automatisch door het systeem gegenereerd. De eerste voor de tenant aangemaakt beheerder ontvangt een activerings-e-mail met een URL die de tenant-ID bevat.

   b. Selecteer *Toepassingen*.
   c. Selecteer een toepassing.
   d. In het tabblad *Vertrouwen*, in de sectie *SAML 2.0*, klikt u op *Naam-ID attribuut*.
   e. Selecteer *E-mail*.
   f. Klik op *Opslaan*.

9.2.4.2.4 Afhankelijke vertrouwensrelatie maken

U moet een afhankelijke vertrouwensrelatie en een claimregel maken in het Microsoft ADFS Management-hulpprogramma om de metagegevens van de serviceprovider bij te werken.

1. Start *Naamserverbeheer*.
2. Ga naar ▶ *Hulpprogramma's* > *AD FS Management* ▶.
3. Vouw de optie *Trust Relationships* uit.
4. Klik met de rechtermuisknop op *Relying Trust Party* en selecteer *Add Relying Trust Party*.
5. Selecteer in de wizard *Add Relying Trust Party* de optie *Start*.
6. Selecteer *Import data about the relying party from a file* en selecteer vervolgens *Bladeren*.
7. Blader naar het gedownloade metagegevensbestand van de serviceprovider en selecteer het bestand.
8. Klik op *Volgende*.

9. Voer de *Weergavenaam* in en selecteer *Volgende*.
10. Selecteer bij de stap *Configure Multi-factor Authentication Now?* de optie *Volgende*.
11. Selecteer de optie *Permit all users to access this relying party* en selecteer vervolgens *Volgende*.
12. Controleer de gegevens op het scherm *Ready to Add Trust* en selecteer *Volgende*.
13. Selecteer *Voltooien*.
    Het dialoogvenster *Edit Claim Rules* wordt geopend. U kunt claimregels maken met een gebruikersnaam of e-mailadres als attribuut.

U hebt nu een afhankelijke vertrouwensrelatie gemaakt.

9.2.4.2.4.1 Een claimregel met gebruikersnaam als attribuut maken

U kunt een claimregel maken met een gebruikersnaam als attribuut voor SAML-verklaring.

Er moet een afhankelijke vertrouwensrelatie beschikbaar zijn.

1. Selecteer in het dialoogvenster *Edit Claim Rules* de optie *Add Rule*.
2. Kies in de *Add Transform Claim Rule Wizard* de optie *Send LDAP Attributes as Claims* en selecteer *Volgende*.
3. Voer de *Claim rule name* in en selecteer *Active Directory* als *Attribute store*.
4. Selecteer onder *LDAP Attribute* de optie *SAM-Account Name*.
5. Selecteer onder *Outgoing Claim Type* de optie *Name ID*.
6. Selecteer *Voltooien*.

De claimregel wordt gemaakt met een gebruikersnaam als attribuut.

9.2.4.2.4.2 Een claimregel met e-mailadres als attribuut maken

U moet twee claimregels maken om een e-mailadres als attribuut voor SAML-verklaring te gebruiken.

1. Selecteer in het dialoogvenster *Edit Claim Rules* de optie *Add Rule*.
2. Kies in de *Add Transform Claim Rule Wizard* de optie *Send LDAP Attributes as Claims* en selecteer *Volgende*.
3. Voer de *Claim rule name* in en selecteer *Active Directory* als *Attribute store*.
4. Kies onder *LDAP Attribute* de optie *E-Mail-Addresses* en kies vervolgens onder *Outgoing Claim Type* de optie *E-Mail Address*.
5. Kies in het tweede gegeven onder *LDAP Attribute* de optie *Given Name* en voer vervolgens onder *Outgoing Claim Type* de tekst *FirstName* in.
6. Selecteer *Voltooien*.

   U hebt de eerste regel gemaakt. Volg onderstaande stappen om de tweede claimregel te maken.
7. Selecteer in het dialoogvenster *Edit Claim Rules* de optie *Add Rule*.

8. Kies in de *Add Transform Claim Rule Wizard* de optie *Transfer an Incoming Claim* en selecteer *Volgende*.
9. Voer de *Claim rule name* in, kies *E-mail Address* als *Incoming claim type*, *Name ID* als *Outgoing claim type* en *Email* als *Outgoing name format*.
10. Selecteer *Voltooien*.

9.2.4.3 WebSphere-toepassingsserver gebruiken als SAML-serviceprovider

Dit onderwerp bevat instructies voor het configureren van de WebSphere-toepassingsserver voor SAML 2.0-verificatie.

> **Opmerking**
>
> In de onderstaande stappen wordt de SAP Cloud Identity Provider als de standaardidentiteitsprovider gebruikt.

Volg de onderstaande stappen:

1. Kopieer de SAML JAR-bestanden in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\SAMLJARS` naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF\lib`.
2. Volg de onderstaande stappen om betrouwbare verificatie met websessie te configureren:
   1. Voeg het bestand global.properties toe aan de aangepaste map `<WebSphere-installatiemap>\WebSphere\\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF\config\custom`. Hieronder volgt de inhoud voor global.properties:
      ```
      sso.enabled=true
      trusted.auth.user.retrieval=WEB_SESSION
      trusted.auth.user.param=UserName
      ```
   2. Ga naar *CMC* > *Verificatie* > *Enterprise*.
   3. Schakel *Vertrouwde verificatie* in.
   4. Stel de *Geldigheid* in.
   5. Kies *Nieuw gedeeld geheim*.
   6. Kies *Gedeeld geheim downloaden* om het gegenereerde gedeelde geheim te downloaden.
      <Het bestand `TrustedPrincipal.conf` wordt gedownload.
   7. Plak het bestand TrustedPrincipal.conf in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` en `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
   8. Ga naar *CMC* > *Verificatie* > *Enterprise* en kies *Bijwerken*.
   9. Start de WebSphere-toepassingsserver opnieuw.
3. Als u SAP Cloud Platform Identity Provider gebruikt, exporteert u alle gebruikers en importeert u deze naar het BI-platform. Zie Gebruikers tegelijkertijd importeren uit Central Management Console

   Zie Bestaande gebruikers exporteren van een tenant van de identiteitsverificatieservice van SAP Cloud Platform voor informatie over het importeren van SAP Cloud Platform-gebruikers naar CSV.

4. Bewerk het eigenschappenbestand door `saml.enabled=true` toe te voegen. Zie de bestandsnamen en hun locatie hieronder:
   1. Ga voor Fiorified BI-startpunt naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF\config\custom` en bewerk het bestand *fioriBI.properties*.
   2. Ga voor OpenDocument naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF\config\custom` en bewerk het bestand *OpenDocument.properties*.
   3. Ga voor CMC naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF\config\custom` en bewerk het bestand *CMC.properties*.

      > **Opmerking**
      >
      > Voor CMC moet u een andere eigenschap `sso.supported.types = trustedSession` instellen in het bestand *CMCApp.properties*.

   > **Opmerking**
   >
   > Als de toepassing het aangepaste eigenschappenbestand niet bevat, maakt u een nieuw eigenschappenbestand.

5. Als u de IDP-metagegevens wilt bijwerken in SP, downloadt u de IDP-metagegevens van de respectieve IDP-serviceproviders. Kopieer het metagegevensbestand naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF` en wijzig de naam in **idp-meta-downloaded.xml** . Zie Tenantconfiguratie voor SAML 2.0 voor meer informatie over het downloaden van de IDP-metagegevens.

   > **Opmerking**
   >
   > Een nieuw algoritme SHA-256 wordt nu ondersteund voor SAML-integratie.

6. Start de WebSphere-toepassingsserver opnieuw.

   > **Opmerking**
   >
   > Als BOE wordt geïmplementeerd op een niet-Windows-computer, moeten de padscheidingstekens in het bestandspad naar de IDP-metagegevens onder de bean **FilesystemMetadataProvider** worden gewijzigd in `securityContext.xml` onder `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF`.
   >
   > ofwel `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` moet worden gewijzigd in `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

Keystore genereren voor het inschakelen van SAML 2.0 (optioneel)

Deze stap is alleen van toepassing als u uw eigen keystorebestand wilt gebruiken.

Bij gegevensuitwisseling in SAML wordt cryptografie gebruikt voor het ondertekenen en coderen van gegevens. Een voorbeeld van een zelfondertekende keystore `sampletestKeystore.jks` wordt meegeleverd met het product en is geldig tot 18 oktober 2019. `sampletestKeystore.jks` heeft de aliasnaam `Testkey` en het wachtwoord `Password1`. U kunt nu een zelfondertekend keystorebestand genereren met behulp van het Java-hulpprogramma Keytool. Volg de onderstaande stappen om een keystorebestand te genereren.

1. Navigeer naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
2. Voer de volgende opdracht uit: `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

Opdracht	Beschrijving
-alias	Voer de aliasnaam van het certificaat in
-keypass	Voer het wachtwoord van het certificaat in
-keystore	De naam van het keystore bestand
-validity	Geldigheid van het certificaat
numberofdays	Het aantal dagen dat het zelfondertekende certificaat geldig is.

   Nadat de opdracht is uitgevoerd worden de volgende vragen gesteld:
   - Voer het keystore-wachtwoord in. *****
   - Voer het nieuwe wachtwoord opnieuw in: *****
   - Wat zijn uw voornaam en achternaam? : <Voor- en achternaam>
   - Wat is de naam van uw organisatie-eenheid? : <Afdelingsnaam>
   - Wat is de naam van uw organisatie? : <Bedrijfsnaam>
   - Wat is de naam van uw plaats en locatie? : <Plaatsnaam>
   - Wat is de naam van uw staat en provincie? : <Naam staat of provincie>
   - Wat is de tweeletterige landcode voor deze eenheid? : <Landnaam of ISO-code>
3. Stop de WebSphere-toepassingsserver.
   Het keystorebestand wordt gegenereerd in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
4. Verplaats het keystorebestand naar `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF`.
5. Bewerk het bestand `securityContext.xml` in `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>\BOE.ear\BOE.war\WEB-INF` met de nieuwe aliasnaam, het nieuwe wachtwoord en de naam van het keystorebestand. Zie de onderstaande XML-code:

Voorbeeldcode

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Raadpleeg de onderstaande tabel voor informatie over de argumenten:

XML-code	Beschrijving
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	Hiermee zoekt u naar het keystorebestand.
`<constructor-arg type="java.lang.String" value="Password1"/>`	Het wachtwoord voor het keystorebestand.
`<entry key="aliasname" value="password"/>`	Aliaswachtwoord
`<constructor-arg type="java.lang.String" value="Testkey"/>`	Alias van het standaardcertificaat

7. Genereer de metagegevens van de serviceprovider en upload de gegevens.
   1. Ga naar http(s)://host:port/BOE/saml/metadata. Het XML-bestand wordt automatisch gedownload nadat u naar de bovenstaande URL bent genavigeerd.
   2. Upload het XML-bestand naar de identiteitsprovider.

Opmerking

U kunt het standaardmetagegevensbestand voor serviceproviders `spring_saml_metadata.xml` in `<WebSphere-installatiemap>\WebSphere\AppServer\profiles\<Profielnaam>\installedApps\<Knooppuntnaam>` gebruiken in plaats van het bestand handmatig te genereren. U moet de XML-tag `<replace_withip>` vervangen door het IP-adres of de hostnaam van de machine uit uw netwerk en `<replace_withport>` door het poortnummer van de WebSphere-toepassingsserver. Vervang HTTP door HTTPS als u HTTPS hebt ingeschakeld in WebSphere.

8. Als u SAP Cloud Identity gebruikt en een SAML-toepassing wilt maken in IDP en de SP `metadata.xml` in de IDP wilt uploaden voor het configureren van de SAML SSO voor BIPlatform, raadpleegt u Een vertrouwde serviceprovider configureren.
9. Start de WebSphere-toepassingsserver opnieuw.

> **Opmerking**
>
> Nadat het keystorebestand is aangepast, moeten de nieuwste serviceprovidermetagegevens worden gegenereerd.

> **Tip**
>
> De SAML-integratie is geslaagd als u nadat u de voor SAML geconfigureerde toepassing (BI-startpunt, Fiorified BI-startpunt of OpenDocument) hebt gestart, wordt doorgestuurd naar de IDP.

9.2.5 Vertrouwde verificatie instellen tussen SAP NetWeaver Java Application Server en BI-platform

- SAP NetWeaver Java Application Server is voor SAML 2.0-verificatie als serviceprovider geconfigureerd.
- Er moet een gebruiker bestaan in SAP NetWeaver Java Application Server.
- Er worden SAML 2.0-certificaten van de serviceprovider en de identiteitsprovider uitgewisseld om het vertrouwen tussen beide te configureren.
  Dezelfde gebruiker moet als een Enterprise-gebruiker worden geïmporteerd op het BI-platform.

Volg de onderstaande stappen om vertrouwde verificatie in te stellen tussen de SAP NetWeaver Java Application Server en het BI-platform:

> **Opmerking**
>
> - U moet de methode `USER_PRINCIPAL` gebruiken om de gebruiker op te halen wanneer u vertrouwde verificatie inschakelt voor webtoepassingen.
> - Om veiligheidsredenen mag vertrouwde verificatie alleen worden ingeschakeld met HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

1. Genereer een BI-webtoepassing met behulp van WDeploy.
   a. Ga naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Voer de volgende opdracht uit om het bestand `BOE.sca` te genereren: `wdeploy.bat sapappsvr73 -DAPP=BOE predeploy`

      `BOE.sca` wordt gegenereerd in `<INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application`.
2. Schakel vertrouwde verificatie in door het bestand `web.xml` te bewerken.
   a. Extraheer het bestand `BOE.sca` in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application` met een programma als winrar of winzip.
   b. Maak een kopie van het bestand `BOE.sca` voordat u wijzigingen aanbrengt. Navigeer in `BOE.sca` naar *DEPLOYARCHIVES* > *BOE.ear* > *BOE.war* > *WEB-INF*.
   c. Bewerk het bestand `web.xml` door de volgende XML-codes toe te voegen vóór `</web-app>`.

Opmerking

Voeg de rollen (vermeld in de onderstaande XML-code) toe aan SAP NetWeaver Java Application Server en wijs deze toe aan een gebruikersgroep of gebruiker.

- j2ee-admin
- j2ee-guest
- j2ee-special

Voorbeeldcode

```
<security-constraint>
<web-resource-collection>
 <web-resource-name>InfoView</web-resource-name>
<url-pattern>*</url-pattern>
<http-method>DELETE</http-method>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>PUT</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>j2ee-admin</role-name>
<role-name>j2ee-guest</role-name>
<role-name>j2ee-special</role-name>
</auth-constraint>
<user-data-constraint>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
<realm-name>InfoView</realm-name>
</login-config>
<security-role>
<description>Assigned to the SAP J2EE Engine System Administrators</
description>
<role-name>j2ee-admin</role-name>
</security-role>
<security-role>
<description>Assigned to all users</description>
<role-name>j2ee-guest</role-name>
</security-role>
<security-role>
<description>Assigned to a special group of users</description>
<role-name>j2ee-special</role-name>
</security-role>
```

d. Maak een nieuw XML-bestand `web-j2ee-engine.xml` met de onderstaande XML-codes en sla het bestand op in `<INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\WEB-INF`.

Voorbeeldcode

```
<?xml version="1.0" encoding="UTF-8"?>
<web-j2ee-engine xsi:noNamespaceSchemaLocation="web-j2ee-engine.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<security-role-map>
    <role-name>j2ee-admin</role-name>
    <server-role-name>administrators</server-role-name>
</security-role-map>
<security-role-map>
```

```
        <role-name>j2ee-guest</role-name>
        <server-role-name>guests</server-role-name>
</security-role-map>
<security-role-map>
        <role-name>j2ee-special</role-name>
        <server-role-name>all</server-role-name>
</security-role-map>
 <login-module-configuration>
        <security-policy-domain>/irj</security-policy-domain>
 </login-module-configuration>
</web-j2ee-engine>
```

e. Sla het bestand `web-j2ee-engine.xml` op.
f. Versleep het bestand naar de map `WEB-INF` van het `BOE.war`-archief.

Eenmalige aanmelding inschakelen in BIP - USER PRINCIPAL, gedeeld geheim - `Trustedprincipal.conf`

We schakelen eenmalige aanmelding in door de methode USER PRINCIPAL te gebruiken om de NW-gebruikersnaam door te geven en het bestand `Trustedprincipal.conf` om het gedeelde geheim door te geven.

Voer de onderstaande stappen uit om vertrouwde verificatie in te schakelen en een gedeeld geheim te genereren:

1. Ga naar *CMC* > *Verificatie* > *Enterprise*.
2. Schakel *Vertrouwde verificatie* in.
3. Kies *Nieuw gedeeld geheim maken*.
4. Kies *Gedeeld geheim downloaden* en sla het op uw BOE-computer op.
5. Kies *Bijwerken*.
6. Extraheer in `BOE.war/web-inf/config/default/folder` het volgende bestand naar `BOE.war/web-inf/config/custom/folder`:
   - `global.properties`
7. Voeg het volgende toe aan `global.properties`:
   - `sso.enabled=true`
   - `trusted.auth.user.retrieval=USER_PRINCIPAL`
   - `trusted.auth.user.namespace.enabled=true`
   - `trusted.auth.shared.secret=MySecret`

   > **Opmerking**
   >
   > We hebben trusted.auth.user.namespace.enabled=true ingeschakeld.

   Bij de eerste poging moet u de volgende foutmelding ontvangen: Aanmelding geweigerd: gebruiker "secExternal:samltest" niet gevonden (FWB 00007). Er is een automatische bindingsfunctie die `secExternal: samltest` als een alias aan een BOE-gebruiker toewijst. Meld u op de normale manier in via het aanmeldingsscherm van InfoView. Voor de BOE-aanmeldingsgegevens die u gebruikt is een `secExternal: samltest`-alias gemaakt. Als u bijvoorbeeld de gebruikersaccount samltest gebruikt, kunt u zien dat `secExternal: samltest` als alias is toegewezen.
8. Ga naar `<INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\ WEB-INF\Eclipse\plugins\webpath.InfoView\web\custom.jsp`

9. Voeg de onderstaande XML-codes toe aan het bestand `custom.jsp`.
   Codeblok:

   Voorbeeldcode

```
<%@ page language="java" contentType="text/html;charset=utf-8"%>
<%@ page
import="com.businessobjects.bip.core.web.appcontext.RequestInfo"%>
<%
 request.getSession().setAttribute("MySecret","Your generated shared
secret content");
%>
 <html>
<head>
    <title></title>
 </head>
    <body>
   <script     type="text/javascript"     src="noCacheCustomResources/
custom.js"></script>
   <script     type="text/javascript">
   window.location = "logon.faces";
   </script>
   </body>
</html>
```

10. Sla het bestand op.

3. Werk het archiefbestand bij en sla het op.
4. Nadat u de bovenstaande stappen hebt uitgevoerd in het bestand `BOE.sca`, implementeert u het in NetWeaver.
5. Als BOE.sca is geïmplementeerd, kunt u het starten om het te verifiëren (http://<hostnaam>:<poortnummer>/nwa).
6. Omdat BASIC-verificatie wordt gebruikt in `web.xml`, wordt een pop-up in de browser weergegeven voor verificatie.

   U hebt nu vertrouwde verificatie ingesteld tussen de SAP NetWeaver Java Application Server en het BI-platform.

   Opmerking

   Voer de volgende stappen uit als u een pop-up voor verificatie in de browser ziet:

   1. Meld u aan bij de SAP NetWeaver Java Application Server op http://<hostnaam>:<poortnummer>/nwa.
   2. Navigeer naar *Configuratie* > *Beveiliging* > *Verificatie* > *Eenmalige aanmelding*
   3. Zoek de beleidsconfiguratie van de BI-toepassing op.
   4. Schakel over naar de modus *Bewerken*.
   5. Laat op het tabblad *Verificatiestack* het veld *Gebruikte sjabloon* leeg en voeg *SAML2LoginModule* toe aan de stack bovenaan met de markering *SUFFICIENT*.
   6. Sla de wijzigingen op en sluit af.

9.2.6 SAML 2.0-verificatie gebruiken met SAP NetWeaver Java Application Server

Als u gebruikers van SAP NetWeaver Application Server Java toegang wilt verlenen tot het SAP Business Intelligence-platform via eenmalige aanmelding, moet een mechanisme voor toegang tot die toepassingen worden ingesteld. In de volgende stappen wordt beschreven hoe u vertrouwde verificatie kunt instellen tussen NetWeaver Application Server Java en Business Intelligence.

Bereik: het bereik van deze stappen omvat niet het instellen van SAML-verificatie, omdat IDP kan variëren van leverancier tot leverancier. Raadpleeg leverancierspecifieke documenten voor het instellen van SAML-verificatie.

De configuratie is onderverdeeld in het volgende:

1. SAML-verificatie configureren op de SAP NetWeaver Java Application Server.
2. Vertrouwde verificatie instellen voor het BI-platform.

Voor meer informatie over het inschakelen van SAML-verificatie op de SAP NetWeaver Java Application Server, raadpleegt u SAML 2.0 gebruiken.

9.2.7 Vertrouwde verificatie inschakelen

Vertrouwde verificatie van Enterprise wordt gebruikt bij het uitvoeren van eenmalige aanmelding door te vertrouwen op de webtoepassingsserver voor de verificatie van de identiteit van de gebruiker. Deze verificatiemethode omvat het tot stand brengen van een vertrouwensrelatie tussen de CMS (Central Management Server) en de webtoepassingsserver waarop de webtoepassing van BI-platform wordt gehost. Wanneer de vertrouwensrelatie tot stand is gebracht, draagt het systeem de verificatie van de gebruikersidentiteit over aan de webtoepassingsserver. Vertrouwde verificatie kan worden gebruikt ter ondersteuning van verificatiemethoden, zoals SAML, x.509 en andere methoden die geen speciale verificatie-invoegtoepassingen hebben.

Gebruikers melden zich het liefst één keer bij het systeem aan, zodat ze hun wachtwoord niet meerdere keren hoeven in te voeren tijdens een sessie. Vertrouwde verificatie is een Java-oplossing voor eenmalige aanmelding, waarbij u uw verificatieoplossing voor BI-platform integreert met verificatieoplossingen van derden. Bij toepassingen die vertrouwd worden door de Central Management Server, kunnen gebruikers zich met Vertrouwde verificatie aanmelden zonder hun wachtwoord op te geven.

Als u Vertrouwde verificatie wilt inschakelen, moet u een gedeeld geheim op de server configureren via de instellingen voor Enterprise-verificatie en de client configureren via de eigenschappen die zijn opgegeven voor het `BOE.war`-bestand.

> **Opmerking**
>
> - Voordat u Vertrouwde verificatie kunt gebruiken, moet u Enterprise-gebruikers hebben gemaakt of de externe gebruikers hebben toegewezen die zich moeten kunnen aanmelden bij het BI-platform.
> - Om beveiligingsredenen mag vertrouwde verificatie niet worden ingeschakeld zonder HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

Verwante informatie

De server configureren voor Vertrouwde verificatie [pagina 258]
Vertrouwde verificatie voor de webtoepassing configureren [pagina 263]

9.2.7.1 Vertrouwde verificatie voor RESTful-webservices op webserver

Het onderwerp voorziet in instructies om vertrouwde verificatie voor RESTful-webservices op webserver in te schakelen.

> **Opmerking**
>
> Om veiligheidsredenen mag vertrouwde verificatie alleen worden ingeschakeld met HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

Volg de onderstaande stappen om Vertrouwde verificatie in te schakelen:

1. Genereer een gedeelde geheime sleutel. Raadpleeg Een waarde voor een gedeeld geheim genereren [pagina 404] voor meer informatie.
2. Sla de gedeelde geheime sleutel op `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` in Windows op.
3. Open de gedeelde geheime sleutel in een teksteditor.
4. Kopieer de gedeelde geheime sleutel.
5. 5. Kopieer het bestand biprws.properties van `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps` en plak het in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom`.
6. Open het bestand *biprws.properties* in een teksteditor.
7. Plak de gedeelde geheime sleutel in de waarde *Trusted_Auth_Shared_Secret=*.
8. Voeg de *Methode wordt opgehaald* en *Parameter gebruikersnaam* toe. Raadpleeg de onderstaande tabel om Methode wordt opgehaald en Parameter gebruikersnaam toe te voegen.

RESTful-webservice - eigenschappen voor configuratie van vertrouwde verificatie

Eigenschap	Beschrijving	Standaardwaarde
Methode wordt opgehaald	Deze instelling is een menu waarin u instelt welke querymethode wordt gebruikt om aanmeldingstokens voor vertrouwde verificatie op te halen wanneer u de RESTful-webservice API `/logon/trusted` gebruikt. • *HTTP_HEADER* wordt gebruikt voor GET-query's met de aanvraagkop accept=application/xml (of application/json). • *QUERY_STRING* wordt gebruikt om een aanmeldingsnaam toe te voegen aan het eind van een URL-query met de RESTful-webservice API, bijvoorbeeld /logon/trusted/?user=johndoe. • *COOKIE* wordt gebruikt wanneer de aanmeldingsnaam wordt opgehaald uit een browsercookie. Het domein, de naam, de waarde en het pad moeten in de cookie zijn opgeslagen.	**HTTP_HEADER**
Parameter gebruikersnaam	Dit is het label dat wordt gebruikt om de vertrouwde gebruiker te identificeren bij het ophalen van een aanmeldingstoken.	**X-SAP-TRUSTED-USER**

9. Sla het bestand *biprws.properties* op.
10. Start de webserver opnieuw.

9.2.7.2 De server configureren voor Vertrouwde verificatie

Voordat u Vertrouwde verificatie kunt configureren, moet u Enterprise-gebruikers of toegewezen gebruikers van derden hebben gemaakt die zich moeten aanmelden bij het BI-platform.

> **Opmerking**
>
> Om veiligheidsredenen mag vertrouwde verificatie alleen worden ingeschakeld met HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

1. Meld u aan bij de CMC.
2. Ga naar het beheergebied *Verificatie*.
3. Klik op de optie *Enterprise*.
   Het dialoogvenster *Enterprise* wordt weergegeven.
4. Onder *Vertrouwde verificatie*:
   a. Klik op *Vertrouwde verificatie is ingeschakeld*.
   b. Klik op *Nieuw gedeeld geheim*.
      Het bericht `Sleutel van gedeeld geheim is gegenereerd en kan worden gedownload` wordt weergegeven.
   c. Klik op *Gedeeld geheim downloaden*.

      Het gedeelde geheim wordt door de client en de CMS gebruikt om de vertrouwde relatie vast te leggen. Configureer eerst de server en vervolgens de clientcomputer voor Vertrouwde verificatie.

Het dialoogvenster *Bestand downloaden* wordt weergegeven.

d. Klik op *Opslaan* en sla het `TrustedPrincipal.conf`-bestand op in een van de volgende mappen:

> ⚠ Let op
>
> Stel de time-out niet in op **`0`** (nul). Een waarde **`0`** betekent dat de tijdafwijking tussen de twee kloktijden onbeperkt kan zijn, waardoor u de kwetsbaarheid voor replay-aanvallen verhoogt.

e. Voer in het veld *Geldigheidsperiode van gedeeld geheim* het aantal dagen dat het gedeelde geheim geldig moet zijn.

f. Geef het maximale aantal milliseconden op dat de klok op de client en de klok van de CMS van elkaar mogen afwijken voor aanvragen voor Vertrouwde verificatie.

g. Wilt u het geheim via het bestand TrustedPrincipal.conf delen in plaats van via de websessie, kopieer het dan naar een van de volgende mappen:

   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

5. Klik op *Bijwerken* om het gedeelde geheim vast te leggen.

Het BI-platform controleert niet alle wijzigingen in parameters voor Vertrouwde verificatie. U moet handmatig een back-up maken van de gegevens voor Vertrouwde verificatie.

Het gedeelde geheim wordt door de client en de CMS gebruikt om de vertrouwde relatie vast te leggen. Vervolgens moet u de client configureren voor Vertrouwde verificatie.

9.2.8 Vertrouwde verificatie configureren voor de webtoepassing

Als u Vertrouwde verificatie voor de client wilt configureren, moet u globale eigenschappen voor het `BOE.war`-bestand wijzigen, evenals bepaalde eigenschappen voor het BI-startpunt en OpenDocument-toepassingen.

Gebruik een van de volgende methoden om het gedeelde geheim aan de client door te geven:

- Optie `WEB_SESSION`
- Bestand `TrustedPrincipal.conf`

Gebruik een van de volgende methoden om de gebruikersnaam aan de client door te geven:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

De methode die u gebruikt moet worden aangepast in de globale eigenschappen `Trusted.auth.user.retrieval` voor het `BOE.war`-bestand, onafhankelijk van de manier waarop het gedeelde geheim wordt doorgegeven.

> **Opmerking**
>
> Om beveiligingsredenen mag vertrouwde verificatie niet worden ingeschakeld zonder HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

9.2.8.1 Vertrouwde verificatie gebruiken voor eenmalige aanmelding van SAML

SAML (Security Assertion Markup Language) is een XML-standaard voor het doorgeven van identiteitsgegevens. SAML biedt een veilige verbinding waar identiteit en vertrouwelijke gegevens worden gecommuniceerd. Bovendien wordt eenmalige aanmelding geboden waardoor extra aanmeldingen voor vertrouwde gebruikers die het BI-platform willen gebruiken, worden geëlimineerd.

SAML-verificatie inschakelen

Als uw toepassingsserver als een SAML-serviceprovider kan werken, kunt u Vertrouwde verificatie gebruiken voor eenmalige aanmelding van SAML bij het BI-platform.

Hiervoor moet u eerst de webtoepassingsserver voor SAML-verificatie configureren.

U moet ook een van de volgende methoden gebruiken om de gebruikersnaam door te geven aan de client:

- `REMOTE_USER`
- `USER_PRINCIPAL`

Het onderstaande voorbeeld bevat een web.xml-voorbeeldbestand dat geconfigureerd is voor SAML-verificatie:

```
<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>
```

Raadpleeg de documentatie van uw toepassingsserver voor verdere instructies, aangezien deze voor elke toepassingsserver verschillen.

Vertrouwde verificatie gebruiken

Als uw webtoepassingsserver eenmaal is geconfigureerd om als een SAML-serviceprovider te werken, kunt u Vertrouwde verificatie gebruiken voor eenmalige aanmelding van SAML.

Dynamische aliassen worden gebruikt om eenmalige aanmelding in te schakelen. Wanneer gebruikers de aanmeldingspagina voor het eerst openen via SAML, worden ze gevraagd om zich handmatig aan te melden met de bestaande referenties van hun BI-platformaccount. Als de referenties van de gebruiker zijn geverifieerd, maakt het systeem een alias van de SAML-identiteit van de gebruiker voor zijn/haar BI-platformaccount. Latere aanmeldingspogingen voor de gebruiker worden uitgevoerd via eenmalige aanmelding. Het systeem koppelt de identiteitsalias van de gebruiker dynamisch aan een bestaande account.

> ⓘ Opmerking
>
> Gebruikers moeten in het BI-platform worden geïmporteerd of Enterprise-accounts hebben.

> ⓘ Opmerking
>
> Een specifieke eigenschap voor het BOE.war-bestand - `trusted.auth.user.namespace.enabled` - moet hiervoor worden ingeschakeld.

9.2.8.2 Eigenschappen voor Vertrouwde verificatie voor webtoepassingen

In de volgende tabel worden de instellingen voor Vertrouwde verificatie in de standaard `global.properties` voor het bestand `BOE.war` weergegeven. Maak een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om de instellingen te overschrijven.

> ⓘ Opmerking
>
> Om beveiligingsredenen mag vertrouwde verificatie niet worden ingeschakeld zonder HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging

beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

Eigenschap	Standaardwaarde	Beschrijving
`sso.enabled=true`	`sso.enabled=false`	Hiermee schakelt u eenmalige aanmelding bij het BI-platform in of uit. Stel de waarde in op `true` om Vertrouwde verificatie in te schakelen.
`trusted.auth.shared.secret`	Geen	Naam van sessievariabele die wordt gebruikt om het geheim voor Vertrouwde verificatie op te halen. Alleen van toepassing als de websessie wordt gebruikt om het gedeelde geheim door te geven.
`trusted.auth.user.param`	Geen	Hiermee wordt de variabele opgegeven die wordt gebruikt om de gebruikersnaam voor Vertrouwde verificatie op te halen.
`trusted.auth.user.retrieval`	Geen	Hiermee wordt de methode opgegeven die wordt gebruikt om de gebruikersnaam voor Vertrouwde verificatie op te halen: • `REMOTE_USER` • `HTTP_HEADER` • `COOKIE` • `QUERY_STRING` • `WEB_SESSION` • `USER_PRINCIPAL` Laat deze optie leeg om Vertrouwde verificatie uit te schakelen.
`trusted.auth.user.namespace.enabled`	Geen	Hiermee wordt dynamische binding van aliassen aan bestaande gebruikersaccounts in- en uitgeschakeld. Als de eigenschap is ingesteld op `true`, gebruikt Vertrouwde verificatie aliasbinding om gebruikers van het BI-platform te verifiëren. Met aliasbinding werkt uw toepassingsserver als een SAML-serviceprovider; hiermee biedt Vertrouwde verificatie eenmalige aanmelding van SAML bij het systeem. Als deze eigenschap leeg is, gebruikt Vertrouwde verificatie koppeling van namen bij het verifiëren van gebruikers.

9.2.8.3 Vertrouwde verificatie voor de webtoepassing configureren

Als u het gedeelde geheim wilt opslaan in het bestand `TrustedPrincipal.conf`, zorg er dan voor dat het bestand wordt opgeslagen in de toepasselijke platformmap:

Platform	Locatie van TrustedPrincipal.conf
Windows, standaardinstallatie	• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86`

Er zijn diverse manieren om de gebruikersnaamvariabele te vullen die wordt gebruikt om Vertrouwde verificatie te configureren voor de client die webtoepassingen host. U moet uw webtoepassingsserver zodanig configureren of instellen dat uw gebruikersnamen beschikbaar voor u zijn voordat u deze methoden voor het ophalen van de gebruikersnaam gebruikt. Zie http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html voor meer informatie.

Als u Vertrouwde verificatie voor de client wilt configureren, moet u eigenschappen voor het `BOE.war`-bestand oproepen en wijzigen, waaronder algemene en specifieke eigenschappen voor het BI-startpunt en OpenDocument-webtoepassingen.

> **Opmerking**
>
> U moet mogelijk extra stappen uitvoeren, afhankelijk van hoe u de gebruikersnaam of het gedeelde geheim wilt ophalen.

1. Open de aangepaste map voor het `BOE.war`-bestand op de computer die de webtoepassingen host: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Later moet u het gewijzigde bestand `BOE.war` opnieuw implementeren.
2. Maak een nieuw bestand met Kladblok of een ander tekstverwerkingsprogramma.
3. Geef de volgende eigenschappen voor Vertrouwde verficatie op:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Method for user ID retrieval>
   trusted.auth.user.param=<User Variable>
   trusted.auth.shared.secret=<Secret Variable>
   ```

   Selecteer een van de volgende opties voor het ophalen van de gebruikersnaam voor de eigenschap `trusted.auth.user.retrieval`:

Optie	Methode voor het ophalen van de gebruikersnaam
`HTTP_HEADER`	De gebruikersnaam wordt opgehaald uit de inhoud van een HTTP-header. U geeft de HTTP-header op die u wilt gebruiken in de eigenschap `trusted.auth.user.param`.
`QUERY_STRING`	De gebruikersnaam wordt opgehaald uit een parameter van de aanvraag-URL. U geeft op welke queryreeks moet worden gebruikt in de eigenschap `trusted.auth.user.param`.
`COOKIE`	De gebruikersnaam wordt opgehaald uit een opgegeven cookie. U geeft op welke cookie moet worden gebruikt in de eigenschap `trusted.auth.user.param`.
`WEB_SESSION`	De gebruikersnaam wordt opgehaald uit de inhoud van een opgegeven sessievariabele. U geeft de web-sessievariabele op die moet worden gebruikt in de eigenschap `trusted.auth.user.param` in de `global.properties`.
`REMOTE_USER`	De gebruikersnaam wordt opgehaald via een oproep van `HttpServletRequest.getRemoteUser()`.
`USER_PRINCIPAL`	De gebruikersnaam wordt opgehaald via een aanroep van `getUserPrincipal().getName()` op het object `HttpServletRequest` voor de huidige aanvraag in een servlet of JSP.

→ Aanbeveling

Als u SSO op basis van HTTP_HEADER of SSO op basis van QUERY_STRING gebruikt, moet u ervoor zorgen dat eindgebruikers (browsers) geen directe toegang hebben tot BOE voor verificatie. In plaats daarvan beveelt SAP aan dat de eindgebruikers (browsers) alleen via de portal of de aangepaste toepassing toegang hebben tot BOE.

ⓘ Opmerking

Voor sommige webtoepassingsservers moet de omgevingsvariabele `REMOTE_USER` zijn ingesteld op `true` op de server. Raadpleeg de documentatie bij uw webtoepassingsserver om na te gaan of dit is vereist. Controleer of de omgevingsvariabele is ingesteld op `true` als dit voor uw server is vereist.

ⓘ Opmerking

Als u `USER_PRINCIPAL` of `REMOTE_USER` gebruikt om de gebruikersnaam door te geven, moet u `trusted.auth.user.param` leeg laten.

4. Sla het bestand op met de naam `global.properties`.

5. Start de webtoepassingsserver opnieuw.

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde BOE-webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u meer informatie wilt over het gebruik van WDeploy.

9.2.8.3.1 Voorbeeldconfiguraties

9.2.8.3.1.1 Het gedeelde geheim via het bestand TrustedPrincipal.conf doorgeven

Gebruikersgegevens worden opgeslagen en doorgegeven via de websessie. Het gedeelde geheim wordt doorgegeven via het `TrustedPrincipal.conf`-bestand, dat standaard is opgeslagen in de map `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. De gebundelde versie van Tomcat is de webtoepassingsserver.

1. Maak in de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` een nieuw bestand met Kladblok of een ander tekstverwerkingsprogramma.
2. Voer de volgende waarden in om eigenschappen voor Vertrouwde verificatie op te geven:

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
```

3. Sla het bestand op met de naam **`global.properties`**.
4. Zoek het bestand `custom.jsp` in de map `web` in het bestand `com.businessobjects.webpath.InfoView.jar` in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
5. Voeg de volgende aangepaste Java-code toe aan het bestand `custom.jsp` in het bestand `com.businessobjects.webpath.InfoView.jar`:

```
<%
//custom Java code
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> **Opmerking**
>
> In het codefragment hierboven moet de variabele <Gebruikersnaam> een geldige Enterprise-gebruiker in het BI-platform zijn.

6. Start de webtoepassingsserver opnieuw.
7. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren.

   Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

Controleer of u Vertrouwde verificatie hebt geconfigureerd door de volgende URL te gebruiken om BI-startpunt te openen: `http://<[cmsnaam]>:8080/BOE/BI/custom.jsp`, waar `<[cmsnaam]>` de naam is van de computer die de CMS host. U wordt alleen de eerste keer gevraagd uw gebruikersnaam en wachtwoord in te voeren. Bij een geslaagde aanmelding wordt u automatisch naar het BI-startpunt omgeleid.

9.2.8.3.1.2 Het gedeelde geheim doorgeven via de websessievariabele

Zowel de gebruikersgegevens als het gedeelde geheim worden via een websessievariabele opgeslagen en doorgegeven. Open het eerder opgeslagen bestand TrustedPrincipal.conf en noteer de inhoud van het bestand. In deze voorbeeldconfiguratie wordt aangenomen dat het gedeelde geheim het volgende inhoudt:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

De gebundelde versie van Tomcat is de webtoepassingsserver.

1. Open de volgende map:

   `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`

2. Maak een nieuw bestand in een teksteditor.
3. Geef de eigenschappen voor vertrouwde verificatie op door het volgende in te voeren:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```

4. Sla het bestand op onder de volgende naam:

   `global.properties`

5. Open het volgende bestand:

   Klassiek BI-startpunt: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`

   Fiorified BI-startpunt: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.FioriBI\web\custom.jsp`

6. Wijzig de inhoud van het bestand om het volgende op te nemen:

   ```
   <%
   //custom Java code
   request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
   211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
   6a3f1345285b55a0a7");
   request.getSession().setAttribute("MyUser","<Username>");
   %>
   ```

   > **Opmerking**
   >
   > In het codefragment hierboven moet de variabele <Gebruikersnaam> een geldige Enterprise-gebruiker in het BI-platform zijn.

7. Start de webtoepassingsserver opnieuw.
8. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren.

   Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

Controleer of u Vertrouwde verificatie correct hebt geconfigureerd door via de volgende URL de toepassing BI-startpunt te openen: `http://[cmsnaam]:8080/BOE/BI/custom.jsp`, waarbij [cmsnaam] de naam is van de computer die de CMS host. U wordt alleen de eerste keer gevraagd uw gebruikersnaam en wachtwoord in te voeren. Bij een geslaagde aanmelding wordt u automatisch naar het BI-startpunt omgeleid.

9.2.8.3.1.3 De gebruikersnaam doorgeven via gebruikers-principal

In de volgende voorbeeldconfiguratie wordt aangenomen dat een gebruiker met de naam “JohnDoe” is gemaakt in het BI-platform.

Gebruikersgegevens worden opgeslagen en doorgegeven via de gebruikers-principaloptie. Het gedeelde geheim wordt doorgegeven via het `TrustedPrincipal.conf`-bestand, dat standaard is opgeslagen in de map `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. De gebundelde versie van Tomcat is de webtoepassingsserver.

1. Stop de Tomcat-server.
2. Open het `server.xml`-bestand voor Tomcat dat zich standaard bevindt in de map `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
3. Zoek de `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>` en wijzig dit in de volgende waarde:

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. Open het `tomcat-users.xml`-bestand dat zich standaard bevindt in de map `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\`.
5. Zoek de code `<tomcat-users>` en wijzig de volgende waarde:

   ```
   <user name=“JohnDoe” password=“password”
   roles=“onjavauser”/>
   ```

6. Open het bestand `web.xml` in de map `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
7. Voeg de volgende waarden toe vóór de code `</web-app>`:

   ```
   <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>
```

U moet een specifieke pagina invoeren voor de parameter `<url-patroon></url-patroon>`. Deze pagina is normaal gesproken niet de standaard-URL voor BI-startpunt of een andere webtoepassing.

8. Voeg de volgende waarden toe aan het aangepaste `global.properties`-bestand:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

> **Opmerking**
>
> Het instellen van `trusted.auth.user.namespace.enabled=true` is optioneel. U kunt de parameter toevoegen als u een externe gebruikersnaam aan een andere gebruikersnaam van het BI-platform wilt toewijzen.

9. Start de webtoepassingsserver opnieuw.
10. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren.

    Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

De configuraties op de webtoepassingsserver zijn hetzelfde als u de methode Externe gebruiker gebruikt.

Controleer of u Vertrouwde verificatie hebt geconfigureerd door de volgende URL te gebruiken om BI-startpunt te openen: `http://<[cmsnaam]>:8080/BOE/BI`, waar `<[cmsnaam]>` de naam is van de computer die de CMS host. Na enkele ogenblikken wordt een aanmeldingsvenster weergegeven.

9.3 LDAP-verificatie

9.3.1 LDAP-verificatie gebruiken

Deze sectie bevat een algemene beschrijving van LDAP-verificatie in het BI-platform. Vervolgens worden de beheerprogramma's beschreven waarmee u LDAP-accounts voor het platform kunt beheren en configureren.

Wanneer u het BI-platform installeert, wordt automatisch ook de LDAP-verificatiemodule geïnstalleerd, maar deze wordt niet standaard ingeschakeld. Als u LDAP-verificatie wilt gebruiken, moet u eerst nagaan of u de bijbehorende LDAP-map hebt ingesteld. Raadpleeg de LDAP-documentatie voor meer informatie over LDAP.

LDAP (Lightweight Directory Access Protocol) is een algemene, toepassingsonafhankelijke adreslijst waarmee gebruikers gegevens uit een groot aantal toepassingen kunnen delen. U kunt met LDAP, dat is gebaseerd op een open standaard, gegevens in een adreslijst opvragen en bijwerken.

LDAP is gebaseerd op de X.500-standaard, waarbij een DAP (Directory Access Protocol) wordt gebruikt voor de communicatie tussen een adreslijstclient en een adreslijstserver. LDAP kan in plaats van DAP worden gebruikt. Bij LDAP worden minder bronnen gebruikt en worden enkele X.500-bewerkingen en -functies vereenvoudigd of weggelaten.

De items in de adreslijststructuur in LDAP zijn volgens een specifiek schema gerangschikt. Elk item wordt aangegeven met de bijbehorende unieke naam (DN, Distinguished Name) of algemene naam (CN, Common Name). Andere algemene attributen zijn de naam van de bedrijfseenheid (OU, Organizational Unit) en de naam van het bedrijf (O, Organization) Een groep met leden kan zich bijvoorbeeld op de volgende locatie in een

adreslijststructuur bevinden: cn=BI-platformgebruikers, ou=Enterprise-gebruikers A, o=Research. Raadpleeg de LDAP-documentatie voor meer informatie.

Omdat LDAP toepassingsonafhankelijk is, kan elke client met de juiste bevoegdheden toegang tot de adreslijsten krijgen. Met deze beveiligingsinvoegtoepassing kunt u LDAP-verificatie instellen voor aanmeldingen van gebruikers bij het BI-platform. Het geeft gebruikers toegangsrechten tot objecten in het systeem. Zolang u een of meer LDAP-servers uitvoert en LDAP op uw bestaande netwerkcomputersystemen gebruikt, kunt u gebruikmaken van LDAP-verificatie (samen met Enterprise- en Windows Active Directory-verificatie).

De LDAP-beveiligingsinvoegtoepassing van het BI-platform kan desgewenst met uw LDAP-server communiceren via een SSL-verbinding die tot stand is gebracht met serververificatie of door wederzijdse verificatie. De LDAP-server heeft bij serververificatie een beveiligingscertificaat dat door het BI-platform wordt gebruikt om te controleren of de server kan worden vertrouwd, terwijl de LDAP-server verbindingen van anonieme clients toestaat. Bij wederzijdse verificatie hebben zowel de LDAP-server als het BI-platform een beveiligingscertificaat en moet de LDAP-server bovendien het clientcertificaat controleren voordat er een verbinding tot stand kan worden gebracht.

De LDAP-beveiligingsinvoegtoepassing die bij het BI-platform wordt geleverd, kan zo worden geconfigureerd dat er via SSL met uw LDAP-server wordt gecommuniceerd, terwijl er altijd een basisverificatie wordt uitgevoerd wanneer de referenties van gebruikers worden gecontroleerd. Als u LDAP-verificatie implementeert in het BI-platform, moet u op de hoogte zijn van de verschillen tussen deze LDAP-typen. Zie voor meer informatie RFC2251 op het volgende adres: http://www.faqs.org/rfcs/rfc2251.html .

Verwante informatie

LDAP-verificatie configureren [pagina 270]
LDAP-groepen toewijzen [pagina 281]

9.3.1.1 LDAP-beveiligingsinvoegtoepassing

Met de LDAP-beveiligingsinvoegtoepassing kunt u gebruikersaccounts en groepen van de LDAP-adreslijstserver toewijzen in het BI-platform. Bovendien kan het systeem met deze beveiligingsinvoegtoepassing alle aanmeldingen controleren waarvoor LDAP-verificatie is opgegeven. Gebruikers worden geverifieerd op de LDAP-adreslijstserver en hun lidmaatschap van een toegewezen LDAP-groep wordt gecontroleerd, voordat de CMS deze gebruikers een actieve BI-platformsessie toekent. Gebruikerslijsten en groepslidmaatschappen worden dynamisch onderhouden door het systeem. U kunt opgeven dat het platform voor extra beveiliging een SSL-verbinding (Secure Sockets Layer) moet gebruiken voor de communicatie met de LDAP-adreslijstserver.

LDAP-verificatie voor het BI-platform is vergelijkbaar met Windows AD-verificatie omdat u ook bij LDAP-verificatie groepen kunt toewijzen en gebruik kunt maken van verificatie, toegangsrechten en aliassen. Ook kunt u net als bij de NT- of Active Directory-verificatie nieuwe Enterprise-accounts voor bestaande LDAP-gebruikers maken en LDAP-aliassen toewijzen aan bestaande gebruikers, als de gebruikersnamen overeenkomen met de gebruikersnamen in Enterprise. Bovendien kunt u bij de LDAP-verificatie het volgende doen:

- Gebruikers en groepen uit de LDAP-adreslijstservice toewijzen

- LDAP toewijzen voor Active Directory. Er gelden beperkingen bij het configureren van LDAP voor Active Directory.
- Meerdere hostnamen en poorten opgeven
- LDAP configureren met SiteMinder.

Nadat u de LDAP-gebruikers en -groepen hebt toegewezen, ondersteunen alle clienthulpprogramma's van BI-platform de LDAP-verificatie. U kunt ook eigen toepassingen maken die LDAP-verificatie ondersteunen.

Verwante informatie

SSL-instellingen voor LDAP-serververificatie of wederzijdse verificatie configureren [pagina 274]
LDAP toewijzen voor Windows Active Directory [pagina 284]
De LDAP-invoegtoepassing voor SiteMinder configureren [pagina 279]

9.3.2 LDAP-verificatie configureren

Ter vereenvoudiging van het beheer ondersteunt het BI-platform LDAP-verificatie voor gebruikers- en groepsaccounts. Voordat gebruikers zich echter met hun LDAP-gebruikersnaam en -wachtwoord kunnen aanmelden bij het systeem, moet u hun LDAP-account toewijzen aan het BI-platform. Wanneer u een LDAP-account toewijst, kunt u een nieuwe account maken of de account koppelen aan een bestaande BI-platformaccount.

Voordat u LDAP-verificatie instelt en inschakelt, controleert u of de LDAP-map is ingesteld. Raadpleeg de LDAP-documentatie voor meer informatie.

Het configureren van LDAP-verificatie omvat de volgende taken:

- De LDAP-host configureren
- De LDAP-server voorbereiden voor SSL (indien vereist)
- De LDAP-invoegtoepassing voor SiteMinder configureren (indien vereist)

> **Opmerking**
>
> als u LDAP configureert voor Active Directory, kunt u uw gebruikers toewijzen. U kunt dan echter geen eenmalige aanmelding van Active Directory of eenmalige databaseaanmelding configureren. Methoden voor eenmalige aanmelding van LDAP, zoals SiteMinder en vertrouwde verificatie, blijven beschikbaar.

9.3.2.1 De LDAP-host configureren

Het is raadzaam ervoor te zorgen dat uw LDAP-server geïnstalleerd en actief is voordat u de LDAP-host configureert.

1. Selecteer *Verificatie* in de navigatielijst om naar het beheergebied *Verificatie* van de CMC te gaan.
2. Dubbelklik op *LDAP*.

3. Als u LDAP-verificatie voor het eerst instelt, klikt u op *Wizard LDAP configureren starten*.
4. Voer de naam en het poortnummer van uw LDAP-hosts in het vak *LDAP-host toevoegen (hostnaam:poort)* in (bijvoorbeeld mijnserver:123), klik op *Toevoegen* en klik vervolgens op *Volgende*.

> → Tip
>
> Herhaal deze stap om meerdere LDAP-hosts van hetzelfde servertype toe te voegen als u hosts wilt toevoegen die als overnameserver kunnen fungeren. Als u een host wilt verwijderen, selecteert u de hostnaam en klikt u op *Verwijderen*.

5. Selecteer het servertype in de lijst *LDAP-servertype*.

> ⓘ Opmerking
>
> Als u LDAP toewijst aan Active Directory, selecteert u *Microsoft Active Directory Application Server* als servertype.

6. Klik op *Attribuuttoewijzingen weergeven* als u de LDAP-serverattribuuttoewijzingen of de LDAP-standaardzoekattributen wilt weergeven of wijzigen.

   Standaard zijn de toegewezen serverattributen en zoekattributen van elk ondersteund servertype ingesteld.
7. Klik op *Volgende*.
8. Typ in het veld *Onderscheidende basisnaam LDAP* de DN-naam (Distinguished Name), bijvoorbeeld o=EenBasis, voor uw LDAP-server en klik vervolgens op *Volgende*.
9. Typ in het vak *LDAP-serverbeheerreferenties* de DN-naam (Distinguished Name) en het wachtwoord van een gebruikersaccount die leesrechten voor de map heeft.

   Beheerdersreferenties zijn niet vereist.

   Als uw LDAP-server anonieme bindingen toestaat, laat u dit gebied leeg. BI-platformservers en -clients worden via anonieme aanmelding gekoppeld aan de primaire host.
10. Als u verwijzingen op uw LDAP-host hebt geconfigureerd, voert u de verificatiegegevens in het gebied *LDAP-toewijzingsreferenties* in en voert u vervolgens het aantal verwijzingssprongen in het veld *Maximale verwijzings-hops* in.

    U moet het gebied *LDAP-toewijzingsreferenties* configureren als alle volgende criteria van toepassing zijn:
    - De primaire host is geconfigureerd om te verwijzen naar een andere mapserver die query's voor vermeldingen onder een bepaalde basis verwerkt.
    - De host waarnaar wordt verwezen is ingesteld voor het weigeren van anonieme bindingen.
    - Een groep van de host waarnaar wordt verwezen, wordt toegewezen aan het BI-platform.

> ⓘ Opmerking
>
> Hoewel groepen van meerdere hosts kunnen worden toegewezen, kan slechts één set toewijzingsreferenties worden ingesteld. Als u dus meerdere hosts met toewijzingsreferenties hebt, moet u op elke host een gebruikersaccount met dezelfde DN-naam (Distinguished Name) en hetzelfde DN-wachtwoord maken.

> ⓘ Opmerking
>
> Als *Maximaal aantal verwijzings-hops* is ingesteld op nul, worden verwijzingen niet gevolgd.

11. Klik op *Volgende*.
12. Selecteer het type SSL-verificatie (Secure Sockets Layer) dat wordt gebruikt:
    - *Basis (geen SSL)*
    - *Serververificatie*
    - *Wederzijdse verificatie*

    Details en vereisten voor wederzijdse en serververificatie worden in een volgende sectie besproken. Als u LDAP-verificatie wilt instellen met een van beide typen SSL, leest u *SSL-instellingen voor LDAP-serververificatie of wederzijdse verificatie configureren* in dit document voordat u deze procedure voortzet.
13. Klik op *Volgende* en selecteer een verificatiemethode voor eenmalige LDAP-aanmelding:
    - *Basis (geen SSO)*
    - *SiteMinder*
14. Klik op *Volgende* en selecteer hoe aliassen en gebruikers aan BI-platformaccounts worden toegewezen.
    a. Selecteer in het gebied *Opties voor nieuwe alias* hoe nieuwe aliassen worden toegewezen aan Enterprise-accounts:
        - *Elke toegevoegde LDAP-alias toewijzen aan een account met dezelfde naam*
          Gebruik deze optie wanneer u weet dat gebruikers een Enterprise-account met dezelfde naam hebben. De LDAP-aliassen worden dus toegewezen aan bestaande gebruikers (de aliassen worden automatisch gemaakt). Gebruikers die geen bestaande Enterprise-account hebben of die in hun Enterprise- en LDAP-account niet dezelfde naam gebruiken, worden toegevoegd als nieuwe gebruikers.
        - *Een nieuwe account maken voor elke toegevoegde LDAP-alias*
          Gebruik deze optie wanneer u voor elke gebruiker een nieuwe account wilt maken.

    b. Selecteer in het gebied *Bijwerkopties van alias* hoe u updates van aliassen wilt beheren voor de Enterprise-accounts:
        - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
          Gebruik deze optie als u automatisch een nieuwe alias wilt maken voor iedere LDAP-gebruiker die is toegewezen aan het BI-platform. Nieuwe LDAP-accounts worden toegevoegd voor gebruikers zonder BI-platformaccount of voor alle gebruikers als u *Een nieuwe account maken voor elke toegevoegde LDAP-alias* hebt ingeschakeld.
        - *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
          Gebruik deze optie wanneer de LDAP-map die u toewijst, veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van het BI-platform. Het systeem maakt niet automatisch aliassen en Enterprise-accounts voor alle gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers die zich aanmelden bij het BI-platform.

    c. Geef in het gebied *Opties voor nieuwe gebruiker* op hoe nieuwe gebruikers worden gemaakt:
        - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
          Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

          > **Opmerking**
          >
          > Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij

> de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het platform, kan een licentie voor 100 gelijktijdige gebruikers bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

15. Voer deze stap uit als u toewijzingen van gebruikersattribuut instelt of als u van plan bent e-mailadressen van de LDAP-server te importeren. In het gebied *Opties voor attribuutbinding* kunt u de prioriteit voor attribuutbinding voor de LDAP-invoegtoepassing opgeven:
    a. Klik op het vak *Volledige naam, e-mailadres en andere attributen importeren*.
    De volledige namen en beschrijvingen die worden gebruikt in de LDAP-accounts, worden met de gebruikersobjecten geïmporteerd en opgeslagen in het systeem.
    b. Geef een optie op voor *Prioriteit van LDAP-attribuutbinding instellen in verhouding tot andere attribuutbindingen*.

    > ⓘ Opmerking
    >
    > Als u de optie instelt op 1, hebben LDAP-attributen prioriteit in scenario's waarbij LDAP en andere invoegtoepassingen (Windows AD en SAP) zijn ingeschakeld. Is de optie op 3 ingesteld, dan hebben attributen van andere ingeschakelde invoegtoepassingen prioriteit.

16. Klik op *Voltooien*..

Verwante informatie

SSL-instellingen voor LDAP-serververificatie of wederzijdse verificatie configureren [pagina 274]
De LDAP-invoegtoepassing voor SiteMinder configureren [pagina 279]

9.3.2.2 Meerdere LDAP-hosts beheren

Met LDAP en het BI-platform kunt u fouttolerantie aan het systeem toevoegen door meerdere LDAP-hosts toe te voegen. Het systeem gebruikt de eerste host die u toevoegt als de primaire LDAP-host. Volgende hosts worden gebruikt als overnamehosts.

De primaire LDAP-host en alle failover-hosts moeten op exact dezelfde manier worden geconfigureerd, en elke LDAP-host moet verwijzen naar alle andere hosts van waaruit u groepen wilt toewijzen. Raadpleeg de LDAP-documentatie voor meer informatie over LDAP-hosts en -verwijzingen.

Als u meerdere LDAP-hosts wilt toevoegen, voert u alle hosts in wanneer u LDAP configureert met de LDAP-configuratiewizard (zie voor meer informatie.) Als u de LDAP al hebt geconfigureerd, gaat u naar het

beheergebied Verificatie van de Central Management Console en klikt u op het tabblad LDAP. Klik in het gebied Overzicht van LDAP-serverconfiguratie op de naam van de LDAP-host om de pagina te openen waarop u hosts kunt toevoegen of verwijderen.

> **Opmerking**
>
> Zorg ervoor dat u eerst de primaire host toevoegt, gevolgd door de overige overnamehosts.

> **Opmerking**
>
> Als u LDAP-overnamehosts gebruikt, kunt u niet het hoogste SSL-beveiligingsniveau gebruiken (u kunt dus niet de optie 'Servercertificaat accepteren als het afkomstig is van een vertrouwde certificeringsinstantie en als het CN-attribuut van het certificaat overeenkomt met de DNS-hostnaam van de server' selecteren).

Verwante informatie

LDAP-verificatie configureren [pagina 270]

9.3.2.3 SSL-instellingen voor LDAP-serververificatie of wederzijdse verificatie configureren

Deze sectie bevat uitgebreide informatie over wederzijdse of serververificatie op basis van SSL voor LDAP. Voor het instellen van verificatie op basis van SSL moet u enkele voorbereidingen treffen. In deze sectie vindt u ook specifieke informatie over het configureren van SSL met LDAP wederzijdse en serverconfiguratie in de CMC. Er wordt aangenomen dat u de LDAP-host hebt geconfigureerd en dat u een van deze opties voor SSL-verificatie hebt gekozen.

Zie de documentatie van uw LDAP-leverancier voor aanvullende informatie of voor informatie over het configureren van de LDAP-hostserver.

Voor Windows-systemen verloopt de standaard-SSL-communicatie via TLS 1.2. Voor Linux-systemen raadpleegt u SAP Note 2623529.

Verwante informatie

De LDAP-host configureren [pagina 270]

9.3.2.3.1 De LDAP-server of wederzijdse verificatie configureren

Bron	Voer de volgende handeling uit voordat u aan deze taak begint
CA-certificaat	Deze handeling is vereist voor zowel server- als wederzijdse verificatie met SSL. 1. Er is een CA-autoriteit (certificeringsautoriteit) vereist om een CA-certificaat te kunnen genereren. 2. Voeg het certificaat toe aan uw LDAP-server. Raadpleeg de LDAP-documentatie van de leverancier voor meer informatie.
Servercertificaat	Deze handeling is vereist voor zowel server- als wederzijdse verificatie met SSL. 1. Vraag een servercertificaat aan en genereer dit vervolgens 2. Autoriseer het certificaat en voeg het aan de LDAP-server toe.

cert7.db of cert8.db, key3.db	Deze bestanden zijn vereist voor zowel serververificatie als wederzijdse verificatie met SSL.
	1. Download de certutil-toepassing om een `cert7.db`- of `cert8.db`-bestand te genereren (afhankelijk van uw vereisten) vanaf https://developer.mozilla.org/en-US/docs/NSS/tools .
	2. Kopieer het CA-certificaat naar dezelfde map als de certutil-toepassing.
	3. Genereer het `cert7.db`- of `cert8.db`-bestand en de bestanden `key3.db` en `secmod.db` met de volgende opdracht:
	`certutil -N -d .`
	4. Voeg het CA-certificaat toe aan het `cert7.db`- of `cert8.db`-bestand met de volgende opdracht:
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. Bewaar de drie bestanden in een map op de computer waarop het BI-platform wordt gehost.

cacerts	Dit bestand is vereist voor wederzijdse verificatie met SSL voor Java-toepassingen zoals BI-startpunt. 1. Zoek het `keytool`-bestand in uw Java `bin`-map. 2. Gebruik de volgende opdracht om het `cacerts`-bestand te maken: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore`

Bron	Voer de volgende handeling uit voordat u aan deze taak begint
	3. Sla het bestand `cacerts` op in dezelfde map als het `cert7.db`- of `cert8.db`- en het `key3.db`-bestand.

Clientcertificaat	1. Maak afzonderlijke clientaanvragen voor het `cert7.db`- of `cert8.db`- en het `.keystore`-bestand:
	• Als u de LDAP-invoegtoepassing wilt configureren, moet u een aanvraag voor een clientcertificaat genereren met behulp van de certutil-toepassing.
	• Genereer de aanvraag voor het clientcertificaat met de volgende opdracht:
	`certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .`
	`<client_dn>` omvat gegevens zoals "CN=`<clientnaam>`, OU=`<org-eenheid>`, O=`<bedrijfsnaam>`, L=`<stad>`, ST=`<provincie>` en C=`<land>`.
	2. Laat de certificaataanvraag door de CA verifiëren. Gebruik de volgende opdracht om het certificaat op te halen en in te voegen in het `cert7.db`- of `cert8.db`-bestand:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. Java-verificatie via SSL mogelijk maken:
	• Gebruik het hulpprogramma keytool in de Java `bin`-map om een aanvraag voor een clientcertificaat te genereren.
	• Gebruik de volgende opdracht om een sleutelpaar te genereren:
	`keytool -genkey -keystore .keystore`
	4. Nadat u informatie over uw client hebt opgegeven, gebruikt u de volgende opdracht om een aanvraag voor een clientcertificaat te genereren:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. Nadat de aanvraag voor een clientcertificaat is geverifieerd door de CA, moet het CA-certificaat met de volgende opdracht worden ingevoegd in het `.keystore`-bestand:
	`keytool -import -v -alias <CA_alias_name>`

Bron	Voer de volgende handeling uit voordat u aan deze taak begint

	`-file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. Haal de aanvraag voor een clientcertificaat bij de CA op en gebruik de volgende opdracht om het certificaat in het `.keystore`-bestand in te voegen:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. Bewaar het bestand `.keystore` in dezelfde map als het bestand `cert7.db` of `cert8.db` en het bestand `cacerts` op de computer waarop het BI-platform wordt gehost.

1. Kies het SSL-beveiligingsniveau dat moet worden gebruikt.

   Als u de LDAP-configuratiewizard gebruikt om LDAP-verificatie de eerste keer te configureren, selecteert u *Wederzijdse verificatie* in de lijst *Type SSL-verificatie* en klikt u op *Volgende*. Of, als u uw LDAP-verificatie opnieuw configureert, gaat u naar het gebied *Verificatie* van de CMC en dubbelklikt u op *LDAP*. De pagina *Overzicht van LDAP-serverconfiguratie* wordt weergegeven. Klik op de waarde *SSL-type* en selecteer *Wederzijdse verificatie* in de lijst *Type SSL-verificatie*.

   - *Servercertificaat altijd accepteren*
     Hiermee stelt u een laag beveiligingsniveau in. Voordat het BI-platform een SSL-verbinding kan maken met de LDAP-host (om LDAP-gebruikers en -groepen te verifiëren), moet een beveiligingscertificaat van de LDAP-host ontvangen zijn. In het BI-platform wordt het ontvangen certificaat niet gecontroleerd.
   - *Servercertificaat accepteren als dit afkomstig is van een vertrouwde certificeringsinstantie*
     Hiermee stelt u een gemiddeld beveiligingsniveau in. Voordat het BI-platform een SSL-verbinding kan maken met de LDAP-host (om LDAP-gebruikers en -groepen te verifiëren), moet een beveiligingscertificaat van de LDAP-host worden ontvangen en geverifieerd. Om het certificaat te kunnen verifiëren, moet het systeem in de certificaatdatabase de CA kunnen vinden die het certificaat heeft uitgegeven.
   - *Servercertificaat accepteren als dit afkomstig is van een vertrouwde certificeringsinstantie en als het CN-attribuut van het certificaat overeenkomt met de DNS-hostnaam van de server*
     Hiermee stelt u het hoogste beveiligingsniveau in. Voordat het BI-platform een SSL-verbinding kan maken met de LDAP-host (om LDAP-gebruikers en -groepen te verifiëren), moet een beveiligingscertificaat van de LDAP-host worden ontvangen en geverifieerd. Om het certificaat te kunnen verifiëren, moet het BI-platform de CA die het certificaat heeft uitgegeven, in de certificaatdatabase kunnen vinden en moet kunnen worden bevestigd dat de CN-eigenschap in het servercertificaat exact overeenkomt met de LDAP-hostnaam die u hebt ingevoerd in het vak *LDAP-host toevoegen* bij de eerste stap van de wizard. Als u de LDAP-hostnaam bijvoorbeeld hebt ingevoerd als **`ABALONE.rd.crystald.net:389`**, (het gebruik van **`CN =ABALONE:389`** in het certificaat werkt niet.) .
     De hostnaam op het serverbeveiligingscertificaat is de naam van de primaire LDAP-host. Als u deze optie kiest, kunt u geen LDAP-host voor overname gebruiken.

> **Opmerking**
>
> Java-toepassingen negeren de eerste en laatste instelling en accepteren het servercertificaat alleen als dit afkomstig is van een vertrouwde CA.

2. Typ de hostnaam van elke computer in het vak *SSL-host* en klik op *Toevoegen*.

   Vervolgens moet u de hostnaam toevoegen van elke computer in uw BI-platformimplementatie die gebruikmaakt van de SDK van het BI-platform. (Dit geldt ook voor de computer waarop de Central Management Server wordt uitgevoerd en de computer waarop de webtoepassingsserver wordt uitgevoerd.)
3. Geef de SSL-instellingen op voor elke SSL-host die u aan de lijst hebt toegevoegd:
   a. Selecteer *Standaard* in de SSL-lijst.
   b. Schakel de selectievakjes *Standaardwaarde gebruiken* in.
   c. Typ een waarde in de vakken *Pad naar de certificaat- en sleuteldatabasebestanden* en *Wachtwoord voor de sleuteldatabase*.
   d. Als u instellingen voor wederzijdse verificatie opgeeft, typt u een waarde in het vak *Bijnaam voor het clientcertificaat in de certificaatdatabase*.

> **Opmerking**
>
> De standaardinstellingen worden gebruikt (voor elke instelling) voor elke host waarvoor het vak *Standaardwaarde gebruiken* ingeschakeld is, of voor elke computer waarvan u de naam niet expliciet toevoegt aan de lijst met SSL-hosts.

4. Geef de standaardinstellingen op voor elke host die niet in de lijst staat en klik op *Volgende*.

   Als u instellingen voor een andere host wilt opgeven, selecteert u de naam van de host in de lijst aan de linkerkant en voert u in de vakken rechts waarden in.

> **Opmerking**
>
> De standaardinstellingen worden gebruikt voor elke instelling (voor elke host) waarvoor het vak *Standaardwaarde gebruiken* ingeschakeld is, of voor elke computer waarvan u de naam niet expliciet toevoegt aan de lijst met SSL-hosts.

5. Kies *Basis (geen SSO)* of *SiteMinder* als de verificatiemethode voor eenmalige LDAP-aanmelding.
6. Geef op hoe nieuwe LDAP-gebruikers en -aliassen worden gemaakt.
7. Klik op *Voltooien*.

Verwante informatie

De LDAP-invoegtoepassing voor SiteMinder configureren [pagina 279]

9.3.2.4 Uw LDAP-configuratie-instellingen wijzigen

Wanneer u LDAP-verificatie met de LDAP-configuratiewizard hebt geconfigureerd, kunt u de LDAP-verbindingsparameters en lidgroepen wijzigen met de pagina *Overzicht van LDAP-serverconfiguratie*.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *LDAP*.

   Als LDAP-verificatie is geconfigureerd, wordt de pagina *Overzicht van LDAP-serverconfiguratie* weergegeven. Op deze pagina kunt u verbindingsparametergebieden of -velden wijzigen en opties in het gebied *Toegewezen LDAP-groepen* bewerken.
3. Verwijder de toegewezen groepen die niet langer toegankelijk zijn met de nieuwe verbindingsinstellingen, en klik op *Bijwerken*.

   U kunt toegewezen groepen verwijderen door de gebruikersgroep te selecteren en op de knop *Verwijderen* in de sectie *Toegewezen LDAP-groepen* te klikken.
4. Wijzig de verbindingsinstellingen en klik op *Bijwerken*.
5. Wijzig waar nodig uw *Opties voor nieuwe alias*, *Bijwerkopties van alias* en *Opties voor nieuwe gebruiker*, en klik op *Bijwerken*.
6. Wijs de nieuwe LDAP-lidgroepen toe en klik op *Bijwerken*.

9.3.2.5 De LDAP-invoegtoepassing voor SiteMinder configureren

In deze sectie wordt uitgelegd hoe de CMC moet worden geconfigureerd voor gebruik van LDAP met SiteMinder. SiteMinder is een toegangs- en verificatiehulpprogramma van derden dat u kunt gebruiken met de LDAP-beveiligingsinvoegtoepassing om eenmalige aanmelding in te stellen voor het BI-platform.

Als u SiteMinder en LDAP met het BI-platform wilt gebruiken, moet u op twee plaatsen configuratiewijzigingen doorvoeren:

- LDAP-invoegtoepassing via de CMC
- `BOE.war`-bestandseigenschappen

> ⓘ Opmerking
>
> Controleer of de SiteMinder-beheerder ondersteuning voor 4.x-agenten heeft ingeschakeld. Dit is vereist ongeacht de ondersteunde versie van SiteMinder die u gebruikt. Zie de documentatie voor SiteMinder voor meer informatie over SiteMinder en de installatie ervan.

Verwante informatie

De LDAP-host configureren [pagina 270]

9.3.2.5.1 ETPKI-bibliotheken installeren

Installeer de ETPKI-bibliotheken om de informatie te beveiligen die wordt uitgewisseld tussen de CA Single Sign-on Policy Server en BI-platform.

Download en installeer CA Single Sign-On SDK voordat u ETPKI-bibliotheken installeert.

Alleen CA Single Sign-On 12.x wordt ondersteund voor BI-platform. Als u een eerdere versie van CA Single Sign-On (eerder bekend als CA SiteMinder) hebt, moet u de versie bijwerken naar versie 12.x.

1. Ga naar `<CA Single Sign-On_INSTALLATIEMAP>\CA\sdk\etpki-install-64` voor 64-bits en `<CA Single Sign-On_INSTALLATIEMAP>\CA\sdk\etpki-install` vpor 32-bits besturingssystemen.

   > **Opmerking**
   >
   > Als de CA Single Sign-On-configuratie niet is geïnstalleerd op de machine waarop BI-platform is geïnstalleerd, kopieert u de ETPKI-bibliotheken naar dezelfde machine.

2. ETPKI-bibliotheken installeren in een Linux-omgeving:
   a. Meld u aan met hoofdtoegang en voer de opdracht `./setup install caller=sdk veryverbose` uit.
      Er wordt op het einde van de console of installatie een melding weergegeven dat de installatie is uitgevoerd.
   b. Voer de opdrachten `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` en `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` uit om het pad in te stellen als de installatiemap met de gebruiker van BI-platform.
   c. Start de *Server Intelligence Agent* opnieuw.
3. ETPKI-bibliotheken installeren in een Windows-omgeving:
   a. Voer de opdrachtprompt uit met beheerdersrechten vanuit de locatie van de ETPKI-bibliotheek.
   b. Voer de opdracht `setup.exe install caller=sdk veryverbose` uit.
   c. Controleer het bestand *capki_install.log* binnen *%temp%* voor de melding of de installatie is uitgevoerd.
   d. Start de *Server Intelligence Agent* opnieuw.

U hebt de ETPKI-bibliotheken geïnstalleerd.

9.3.2.5.2 LDAP voor eenmalige aanmelding met SiteMinder configureren

1. Open op een van de volgende manieren het scherm *Configureer de SiteMinder-instellingen*:
   - Selecteer SiteMinder in het scherm *Kies een verificatiemethode voor eenmalige LDAP-aanmelding* van de LDAP-configuratiewizard.
   - Selecteer *Type eenmalige aanmelding* in het scherm voor LDAP-verificatie dat beschikbaar is nadat u LDAP hebt geconfigureerd en eenmalige aanmelding instelt.
2. Typ de naam van elke beleidsserver in het vak *Beleidsserverhost* en klik op *Toevoegen*.
3. Geef voor elke beleidsserverhost de nummers van de *Accounting-*, *Verificatie-* en *Autorisatie*poort op.
4. Voer de naam van de *agent* en het *gedeelde geheim* in. Voer het gedeelde geheim opnieuw in in het vakje *Gedeeld geheim bevestigen*.
5. Klik op *Volgende*.
6. Ga verder met het configureren van de LDAP-opties.

9.3.2.5.3 LDAP en SiteMinder in het BOE.war-bestand inschakelen

Naast de SiteMinder-instellingen voor de LDAP-beveiligingsinvoegtoepassing moeten de SiteMinder-instellingen voor de BOE.war-eigenschappen worden opgegeven.

1. Ga naar de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` in uw BI-platforminstallatie.
2. Maak een nieuw bestand in Kladblok of een andere teksteditor.
3. Voer de volgende instructie in:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Sluit het bestand en sla het op met de naam **`global.properties`** zonder bestandsextensie.
5. Maak nog een bestand in dezelfde map.
6. Voer de volgende instructie in:

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

   Bijvoorbeeld:

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. Sluit het bestand en sla het op met de naam `bilaunchpad.properties`.

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde BOE-webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

9.3.3 LDAP-groepen toewijzen

Wanneer u met de LDAP-configuratiewizard de LDAP-host hebt ingesteld, kunt u LDAP-groepen toewijzen aan Enterprise-groepen.

Zodra LDAP-groepen zijn toegewezen, kunt u ze weergeven door op de LDAP-optie in het gebied voor *verificatiebeheer* te klikken. Als LDAP-verificatie is ingesteld. worden in het gebied Toegewezen LDAP-groepen de LDAP-groepen weergegeven die zijn toegewezen aan het BI-platform.

> **Opmerking**
>
> U kunt ook Windows AD-groepen toewijzen voor verificatie in het BI-platform via de LDAP-beveiligingsinvoegtoepassing.

> **Opmerking**
>
> Als u LDAP voor Active Directory hebt geconfigureerd, worden met deze procedure uw Active Directory-groepen toegewezen.

9.3.3.1 LDAP-groepen toewijzen met het BI-platform

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *LDAP*.

   Als LDAP-verificatie is ingesteld, wordt de LDAP-overzichtspagina weergegeven.
3. Geef in het gebied *Toegewezen LDAP-groepen* uw LDAP-groep op (met CN-naam of DN-naam) in het vak *LDAP-groep toevoegen (met cn of dn)*. Klik op *Toevoegen*.

   Herhaal deze stap om meerdere LDAP-groepen toe te voegen. Als u een groep wilt verwijderen, selecteert u de LDAP-groep en klikt u op *Verwijderen*.
4. Selecteer in het gebied *Opties voor nieuwe alias* een optie voor het toewijzen van LDAP-aliassen aan Enterprise-accounts:
   - *Elke toegevoegde LDAP-alias toewijzen aan een account met dezelfde naam*
     Gebruik deze optie wanneer u weet dat gebruikers een bestaande Enterprise-account met dezelfde naam hebben. De LDAP-aliassen worden dus toegewezen aan bestaande gebruikers (de aliassen worden automatisch gemaakt). Gebruikers die geen bestaande Enterprise-account hebben of die in hun Enterprise- en LDAP-account niet dezelfde naam gebruiken, worden als nieuwe LDAP-gebruikers toegevoegd.
   - *Een nieuwe account maken voor elke toegevoegde LDAP-alias*
     Gebruik deze optie wanneer u voor elke gebruiker een nieuwe account wilt maken.
5. Selecteer in het gebied *Bijwerkopties van alias* een optie om te bepalen of LDAP-aliassen automatisch moeten worden gemaakt voor alle nieuwe gebruikers:
   - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
     Gebruik deze optie als u automatisch een nieuwe alias wilt maken voor iedere LDAP-gebruiker die is toegewezen aan het BI-platform. Nieuwe LDAP-accounts worden toegevoegd voor gebruikers zonder BI-platformaccounts of voor alle gebruikers als u de optie *Een nieuwe account maken voor elke toegevoegde LDAP-alias* hebt ingeschakeld en op *Bijwerken* hebt geklikt.
   - *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
     Gebruik deze optie wanneer de LDAP-map die u toewijst, veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van het BI-platform. Het systeem maakt niet automatisch aliassen en Enterprise-accounts voor alle gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers die zich aanmelden bij het BI-platform.
6. Als uw BI-platformlicentie is gebaseerd op gebruikersrollen, selecteert u in het gebied *Opties voor nieuwe gebruikers* een optie om eigenschappen op te geven van de nieuwe Enterprise-accounts die worden gemaakt om aan LDAP-accounts te worden toegewezen:
   - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke

gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

> **Opmerking**
>
> Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het systeem, kan een licentie voor gelijktijdige toegang van 100 gebruikers bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

7. Klik op *Bijwerken*.

9.3.3.2 De toewijzing van LDAP-groepen opheffen met het BI-platform

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *LDAP*.

   Als LDAP-verificatie is ingesteld, wordt de LDAP-overzichtspagina weergegeven.
3. Selecteer in het gebied Toegewezen LDAP-lidgroepen de LDAP-groep die u wilt verwijderen.
4. Klik op *Verwijderen* en vervolgens op *Bijwerken*.

   De gebruikers in deze groep hebben geen toegang meer tot het BI-platform.

   > **Opmerking**
   >
   > De enige uitzondering hierop is wanneer een gebruiker een alias voor een Enterprise-account heeft. Schakel de Enterprise-account van de gebruiker uit of verwijder deze om de toegang te beperken.

Als u LDAP-verificatie voor alle groepen wilt weigeren, heft u de selectie van het vakje LDAP-verificatie is ingeschakeld op en klikt u op *Bijwerken*.

9.3.3.3 LDAP toewijzen voor Windows Active Directory

Houd bij het configureren van LDAP voor Windows AD rekening met de volgende beperkingen:

- als u LDAP configureert voor Active Directory, kunt u uw gebruikers toewijzen. U kunt dan echter geen eenmalige aanmelding van Active Directory of eenmalige databaseaanmelding configureren. Methoden voor eenmalige aanmelding van LDAP, zoals SiteMinder en vertrouwde verificatie, blijven beschikbaar.
- Gebruikers die alleen lid zijn van standaardgroepen van AD, kunnen zich niet aanmelden. Gebruikers moeten ook lid zijn van een andere, expliciet gemaakte Active Directory-groep en bovendien moet deze groep zijn toegewezen. Een voorbeeld van een dergelijke groep is de groep 'domeingebruikers'.
- Als een toegewezen lokale domeingroep een gebruiker uit een ander domein in het forest bevat, kan de gebruiker uit een ander domein in het forest zich niet aanmelden.
- Gebruikers uit een universele groep uit een ander domein dan de DC die is opgegeven als de LDAP-host, kunnen zich niet aanmelden.
- Met de LDAP-invoegtoepassing kunt u geen gebruikers en groepen van AD-forests toewijzen buiten het forest waarin het BI-platform is geïnstalleerd.
- U kunt de groep 'domeingebruikers' niet toewijzen in Active Directory.
- U kunt een lokale computergroep niet toewijzen.
- Als u de globale catalogus-domeincontroller gebruikt, moet u bij het toewijzen van LDAP voor AD ook rekening houden met de volgende zaken:

Situatie	Overwegingen
Meerdere domeinen bij verwijzing naar de globale catalogus-domeincontroller	U kunt toewijzen in: • Universele groepen in een onderliggend domein • Groepen in hetzelfde domein met daarin universele groepen uit een onderliggend domein • Universele groepen in een ander domein U kunt niet toewijzen in: • Globale groepen in een onderliggend domein • Lokale groepen in een onderliggend domein • Groepen in hetzelfde domein met daarin een globale groep uit het onderliggende domein • Globale groepen uit een ander domein In het algemeen geldt dat universele groepen gebruikers uit andere of onderliggende domeinen ondersteunen. Andere groepen worden niet toegewezen als ze gebruikers uit andere of onderliggende domeinen bevatten. Binnen het domein waarnaar u verwijst, kunt u lokale, globale en universele groepen toewijzen.
Toewijzingen in universele groepen	Als u toewijzingen in universele groepen wilt instellen, verwijst u naar de globale catalogus-domeincontroller. Gebruik daarbij poort 3268 in plaats van de standaardpoort 389.

- Als u meerdere domeinen gebruikt maar niet naar de globale catalogus-domeincontroller verwijst, kunt u niet toewijzen in groepen uit andere of onderliggende domeinen. Alleen vanuit het specifieke domein waarnaar u verwijst, kunt u toewijzen in alle soorten groepen.

9.3.3.4 De LDAP-invoegtoepassing gebruiken om eenmalige aanmelding bij de SAP HANA-database te configureren

In deze sectie vinden beheerders informatie over de stappen die ze moeten uitvoeren om eenmalige aanmelding (Single Sign-on) te configureren tussen het BI-platform dat in SUSE Linux 11 wordt uitgevoerd en de SAP HANA-database. Met LDAP-verificatie via Kerberos kunnen AD-gebruikers worden geverifieerd op een BI-platform dat wordt uitgevoerd in Linux, met name in SUSE. Dit scenario ondersteunt tevens eenmalige aanmelding bij SAP HANA als rapportagedatabase.

> **Opmerking**
>
> Zie de handleiding *voor serverinstallaties en -updates van de SAP HANA Database* voor informatie over het configureren van de SAP HANA-database. Zie de *Handleiding voor gegevenstoegang* voor informatie over het configureren van het onderdeel voor gegevenstoegang voor SAP HANA.

Implementatieoverzicht

De volgende onderdelen zijn vereist voor het gebruik van eenmalige aanmelding via Kerberos.

Onderdeel	Vereiste
Domeincontroller	Moet worden gehost op een computer waarop een Active Directory-instelling wordt uitgevoerd om Kerberos-verificatie te kunnen gebruiken.
Central Management Server	Moet zijn geïnstalleerd en worden uitgevoerd op een computer waarop SUSE Linux Enterprise 11 (SUSE) wordt uitgevoerd.
Kerberos V5-client	Moet samen met de vereiste hulpprogramma's en bibliotheken op de SUSE-host zijn geïnstalleerd. **Opmerking** Gebruik de nieuwste versie van de Kerberos V5-client. Voeg de mappen `bin` en `lib` toe aan de omgevingsvariabelen `PATH` en `LD_LIBRARY_PATH`.
LDAP-verificatie-invoegtoepassing	Moet zijn ingeschakeld op de SUSE-host.
Kerberos-configuratiebestand voor aanmelding	Moet zijn gemaakt op de computer waarop de webtoepassingsserver wordt gehost.

Implementatiewerkstroom

De volgende taken moeten worden uitgevoerd om eenmalige aanmelding voor BI-platformgebruikers bij SAP HANA te configureren door middel van Kerberos-verificatie via JDBC.

1. De AD-host configureren.

2. Accounts en keytab-bestanden voor de SUSE-host en het BI-platform maken op de AD-host.
3. Kerberos-bronnen installeren op de SUSE-host.
4. De SUSE-host configureren voor Kerberos-verificatie.
5. Kerberos-verificatieopties configureren in de LDAP-verificatie-invoegtoepassing.
6. Een Kerberos-configuratiebestand voor aanmelding maken voor de webtoepassingshost.

9.3.3.4.1 De domeincontroller configureren

Mogelijk moet u een vertrouwensrelatie tussen de SUSE-host en de domeincontroller configureren. Als de SUSE-host deel uitmaakt van de Windows-domeincontroller, hoeft u geen vertrouwensrelatie te configureren. Als de BI-platformimplementatie en de domeincontroller zich echter in verschillende domeinen bevinden, moet u mogelijk een vertrouwensrelatie tussen de SUSE Linux-computer en de domeincontroller configureren. Hiervoor moet u het volgende doen:

1. Een gebruikersaccount maken voor de SUSE-computer waarop het BI-platform wordt uitgevoerd.
2. Een SPN (Service Principal Name) voor de host maken.

   > **Opmerking**
   >
   > De notatie van de SPN moet voldoen aan de conventies van Windows AD: host/`<hostnaam>`@`<NAAM_DNS_REALM>`. Gebruik voor /`<hostnaam>` een volledig gekwalificeerde domeinnaam die uit kleine letters bestaat. `<NAAM_DNS_REALM>` moet u in hoofdletters opgeven.

3. Voer de keytab-setup-opdracht `ktpass` van Kerberos uit om de SPN aan de gebruikersaccount te koppelen:

   ```
   c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
   Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
   ```

De volgende stappen moeten worden uitgevoerd op de computer waarop de domeincontroller wordt gehost.

1. Maak een gebruikersaccount voor de service die het BI-platform uitvoert.
2. Klik op de pagina *Gebruikersaccounts* met de rechtermuisknop op de nieuwe serviceaccount en kies *Eigenschappen* > *Machtiging*.
3. Selecteer *Deze gebruiker mag delegeren aan alle services (alleen Kerberos)*.
4. Voer de keytab-setup-opdracht `ktpass` van Kerberos uit om een SPN-account voor de nieuwe serviceaccount te maken:

   ```
   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
   ```

   > **Opmerking**
   >
   > De notatie van de SPN moet voldoen aan de conventies van Windows AD: sianame/`<servicenaam>`@`<NAAM_DNS_REALM>`. Geef de `<servicenaam>` in kleine letters op, anders kan deze mogelijk niet door het SUSE-platform worden omgezet. `<NAAM_DNS_REALM>` moet u in hoofdletters opgeven.

Parameter	Beschrijving
`-princ`	Hiermee wordt de hoofdnaam voor Kerberos-verificatie opgegeven.
`-out`	Hiermee wordt de naam opgegeven van het `keytab`-bestand van Kerberos dat moet worden gegenereerd. Deze naam moet overeenkomen met de waarde van `<sianaam>` die is gebruikt in `-princ`.
`-mapuser`	Hiermee wordt de naam opgegeven van de gebruikersaccount waaraan de SPN is toegewezen. De Server Intelligence Agent wordt via deze account uitgevoerd.
`-pass`	Hiermee wordt het wachtwoord opgegeven dat door de serviceaccount wordt gebruikt.
`-ptype`	Hiermee wordt het principal-type opgegeven: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Hiermee wordt het coderingstype opgegeven dat met de serviceaccount moet worden gebruikt: `-crypto RC4-HMAC-NT`

U hebt de vereiste keytab-bestanden voor de vertrouwensrelatie tussen de SUSE-computer en de domeincontroller gegenereerd.

U moet de keytab-bestanden (een of meerdere) naar de SUSE-computer overbrengen en opslaan in de map `/etc`.

9.3.3.4.2 Het SUSE Linux Enterprise 11-systeem configureren

De volgende bronnen zijn vereist voor de configuratie van Kerberos op het SUSE Linux-systeem waarop het BI-platform wordt uitgevoerd:

- Keytab-bestanden die op de domeincontroller zijn gemaakt. Het keytab-bestand dat voor de BI-platformservice is gemaakt is vereist. Het gebruik van het keytab-bestand voor de SUSE-host wordt specifiek aanbevolen als de BI-platformhost en domeincontroller deel uitmaken van verschillende domeinen.
- De nieuwste Kerberos V5-bibliotheek (inclusief de Kerberos-client) moet op de SUSE-host zijn geïnstalleerd. U moet de locatie van de binaire bestanden toevoegen aan de omgevingsvariableen `PATH` en `LD_LIBRARY_PATH`. Om te controleren of de Kerberos-client correct is geïnstalleerd en geconfigureerd, controleert u of de volgende hulpprogramma's en bibliotheken aanwezig zijn op de SUSE-host:
  - `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`

> → Tip
>
> Voer de opdracht `rpm -qa | grep krb` uit om het versienummer van deze bibliotheken te controleren. Zie http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 voor informatie over de nieuwste Kerberos-client, bibliotheken en de configuratie van de Unix-host.

Als alle vereiste bronnen beschikbaar zijn op de SUSE-host, voert u de onderstaande instructies uit om Kerberos-verificatie te configureren.

> ⓘ Opmerking
>
> U kunt deze stappen alleen uitvoeren als u rootrechten hebt.

1. Voer de volgende opdracht uit om de keytab-bestanden samen te voegen:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Wijzig het bestand `/etc/kerb5.conf` zodat het naar de domeincontroller (op het Windows-platform) verwijst als Kerberos Domain Controller (KDC).

   Zie het onderstaande voorbeeld:

```
[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
            }
```

   > ⓘ Opmerking
   >
   > Het bestand `krb5.conf` bevat Kerberos-configuratiegegevens, zoals de locaties van KDC's en servers voor de realms of interest van Kerberos, Kerberos-toepassingen en toewijzingen van hostnamen aan Kerberos-realms. Het bestand `krb5.conf` is normaliter geïnstalleerd in de map `/etc`.

3. Voeg de domeincontroller toe aan `/etc/hosts` zodat de SUSE-host de KDC kan vinden.
4. Voer het programma `kinit` in de map `/usr/local/bin` uit om te controleren of Kerberos correct is geconfigureerd. Controleer of u zich met een AD-gebruikersaccount bij het SUSE-systeem kunt aanmelden.

> → Tip
>
> De KDC moet een Ticket Granting Ticket (TGT) uitgeven die u in de cache kunt weergeven. Gebruik het programma `klist` om de TGT weer te geven.

Voorbeeld

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>
> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

U moet `kinit` ook gebruiken om de SPN's te testen.

9.3.3.4.3 Kerberos-verificatieopties voor LDAP configureren

Voordat u Kerberos-verificatie voor LDAP kunt configureren, moet u de LDAP-verificatie-invoegtoepassing voor het BI-platform inschakelen en configureren om verbinding te maken met de AD-map. Als u LDAP-verificatie wilt gebruiken, moet u eerst nagaan of u de bijbehorende LDAP-map hebt ingesteld.

> ⓘ Opmerking
>
> Bij het uitvoeren van de *LDAP-configuratiewizard* moet u de *Microsoft Active Directory Application Server* en de vereiste configuratiegegevens opgeven.

Wanneer LDAP-verificatie is ingeschakeld en er verbinding is gemaakt met uw Microsoft Active Directory Application Server, verschijnt het gebied *Kerberos-verificatie inschakelen* op de pagina Overzicht van LDAP-serverconfiguratie. In dit gebied kunt u Kerberos-verificatie configureren. Dit is vereist voor eenmalige aanmelding bij de SAP HANA-database vanaf een BI-platform dat op een SUSE-systeem is geïmplementeerd.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *LDAP*.

   De pagina *Overzicht van LDAP-serverconfiguratie* wordt weergegeven. Hier kunt u willekeurige verbindingsparameters of velden wijzigen.
3. Als u Kerberos-verificatie wilt configureren, voert u de volgende stappen uit in het gebied *Kerberos-verificatie inschakelen*:
   a. Klik op *Kerberos-verificatie inschakelen*.
   b. Klik op *Beveiligingscontext in cache (vereist voor SSO naar database)*.

> **Opmerking**
>
> Het inschakelen van de beveiligingscontext in de cache is met name belangrijk voor eenmalige aanmelding bij SAP HANA.

c. Geef de SPN (Service Principal Name) voor de account voor het BI-platform op bij *Naam van service-principal*.

   De notatie voor het opgeven van de SPN is `<sianaam/service>@<NAAM_DNS_REALM>`. Daarbij is

`<sianaam>`	Naam van de Server Intelligence Agent
`<service >`	De naam van de serviceaccount die wordt gebruikt om het BI-platform uit te voeren
NAAM_DNS_REALM	De domeinnaam van de domeincontroller in hoofdletters

> **Tip**
>
> Let er bij het opgeven van de SPN op dat `<sianaam/service>` hoofdlettergevoelig is.

d. Geef het domein van de domeincontroller op bij *Standaard Kerberos-realm*.

e. Geef `userPrincipalName` op bij *Naam van gebruikers-principal*.

   Deze waarde wordt door de LDAP-verificatietoepassing gebruikt om waarden van gebruikers-ID's te verstrekken die Kerberos vereist. De opgegeven waarde moet overeenkomen met de waarde die u hebt opgegeven bij het maken van de keytab-bestanden.

4. Klik op *Bijwerken* om de wijzigingen toe te passen en op te slaan.

U hebt Kerberos-configuratieopties geconfigureerd om te verwijzen naar gebruikersaccounts in de AD-map.

U moet een configuratiebestand voor de Kerberos-aanmelding maken - `bscLogin.conf` - om aanmelding en eenmalige aanmelding via Kerberos te kunnen gebruiken.

Verwante informatie

LDAP-verificatie configureren [pagina 270]

9.3.3.4.4 Een configuratiebestand voor de Kerberos-aanmelding maken

Om aanmelding en eenmalige aanmelding via Kerberos te kunnen gebruiken, moet u een configuratiebestand voor aanmelding toevoegen op de computer waarop de webtoepassingsserver van het BI-platform wordt gehost.

1. Maak een bestand met de naam `bscLogin.conf` en sla het op in de map `/etc`.

> **Opmerking**
>
> U kunt dit bestand opslaan op een andere locatie. Als u dit doet, moet u de locatie echter opgeven in de Java-opties. Het is raadzaam om het bestand `bscLogin.conf` en de keytab-bestanden voor

> Kerberos in dezelfde map op te slaan. Bij een gedistribueerde implementatie moet u een exemplaar van het bestand `bscLogin.conf` toevoegen voor elk systeem waarop een webtoepassingsserver wordt gehost.

2. Voeg de volgende code toe aan het configuratiebestand voor aanmelding `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="<naam van principal>";
};
```

> **Opmerking**
>
> Het volgende gedeelte is met name belangrijk voor eenmalige aanmelding:
>
> ```
> com.businessobjects.security.jgss.accept {
> com.sun.security.auth.module.Krb5LoginModule required
> storeKey=true
> useKeyTab=true
> keyTab="/etc/krb5.keytab"
> principal="<naam van principal>";
> };
> ```

3. Sla het bestand op en sluit het.

9.3.3.5 Problemen met nieuwe LDAP-accounts oplossen

- Als u een nieuwe LDAP-gebruikersaccount maakt en de account geen lid is van een groepsaccount die is toegewezen aan het BI-platform, wijst u de groep toe of voegt u de nieuwe LDAP-gebruikersaccount toe aan een groep die al is toegewezen aan het systeem.
- Als u een nieuwe LDAP-gebruikersaccount maakt en de account lid is van een groepsaccount die is toegewezen aan het BI-platform, vernieuwt u de gebruikerslijst.

Verwante informatie

LDAP-verificatie configureren [pagina 270]
LDAP-groepen toewijzen [pagina 281]

9.4 Windows Active Directory-verificatie

9.4.1 Windows Active Directory-verificatie gebruiken

9.4.1.1 Ondersteuningsvereisten en eerste installatie van Windows AD

In deze sectie wordt u begeleid bij het configureren van Windows AD-verficatie (Active Directory) op het BI-platform. Alle vereiste end-to-end-werkstromen die u moet uitvoeren, worden weergegeven met validatietests en controles.

> **Opmerking**
>
> Zie SAP Knowledge Base KBA 1631734 voor aanvullende informatie over het configureren van Windows AD-verificatie. Deze is beschikbaar op https://service.sap.com/sap/support/notes/1631734.

Ondersteuningsvereisten

Houd rekening met de volgende ondersteuningsvereisten als u AD-verificatie wilt gebruiken voor het BI-platform.

- De CMS moet altijd worden geïnstalleerd op een ondersteund Windows-platform.
- Bepaalde BI-platformtoepassingen mogen alleen bepaalde verificatiemethoden gebruiken. Toepassingen zoals het BI-startpunt en de Central Management Console ondersteunen bijvoorbeeld alleen Kerberos.

Aanbevolen werkstroom voor set-up van AD

Voer de volgende werkstroom uit om handmatige AD-verificatie met het BI-platform in te stellen:

1. Stel de domeincontroller in.
2. Configureer AD-verificatie in de CMC.
3. Configureer de AD-gebruikersaccount op de SIA (Server Intelligence Agent).
4. Uw webtoepassingsserver configureren voor AD-verificatie met Kerberos

> **Opmerking**
>
> Voer deze werkstroom uit, ongeacht of eenmalige aanmelding is vereist. Met de werkstroom die in de volgende secties wordt besproken, kunt u zich in eerste instantie handmatig (met een AD-gebruikersnaam en -wachtwoord) aanmelden bij het BI-platform. Wanneer u handmatige AD-verificatie hebt geconfigureerd, wordt u in een uitgebreide sectie begeleid bij het instellen van SSO voor AD-verificatie.

9.4.2 De domeincontroller voorbereiden

9.4.2.1 Een serviceaccount aanmaken voor AD-verificatie met Kerberos

Als u het BI-platform wilt configureren om met Windows AD (Kerberos)-verificatie te werken, hebt u een serviceaccount nodig. U kunt een nieuwe domeinaccount maken of een bestaande domeinaccount gebruiken. De serviceaccount wordt gebruikt voor het uitvoeren van de BI-platformservers. Nadat u de account hebt ingesteld, moet u een SPN voor de account instellen. Deze SPN wordt gebruikt om AD-gebruikersgroepen te importeren in het BI-platform.

> **Opmerking**
>
> Als u AD met SSO wilt gebruiken, moet u later teruggaan naar de set-up van de serviceaccount om de accountspecifieke rechten te verlenen en de account te configureren voor beperkte machtiging.

9.4.2.1.1 De serviceaccount instellen op een Windows 2008-domein

U moet een nieuwe serviceaccount instellen om Windows AD-verificatie met het Kerberos-protocol te kunnen inschakelen. Deze serviceaccount wordt voornamelijk gebruikt om gebruikers in een opgegeven AD-groep toe te staan zich aan te melden bij het BI-startpunt. De volgende taak wordt uitgevoerd op de computer van de AD-domeincontroller.

1. Maak een nieuwe serviceaccount met een wachtwoord aan op de primaire domeincontroller.
2. Gebruik de opdracht `setspn -s` om de SPN (namen van de service-principal) toe te voegen aan de serviceaccount die u in stap 1 hebt gemaakt. Geef de namen van de service-principals op voor de serviceaccount, evenals de server, een volledig gekwalificeerde domeinserver en IP-adres voor de computer waarop het BI-startpunt is geïmplementeerd.
   Bijvoorbeeld:

   ```
   setspn –s BICMS/service_account_name.domain.com serviceaccountname
   setspn -s HTTP/<servername> <servicename>
   setspn -s HTTP/<servername.domain.com> <servicename>
   setspn -s HTTP/<ip address of server> <servicename>
   ```

   `BICMS` is de naam van de computer waarop de SIA wordt uitgevoerd, `<servernaam>` is de naam van de server waarop BI-startpunt is geïmplementeerd, en `<servernaamdomein>` is de volledig gekwalificeerde domeinnaam.
3. Voer `setspsn -1<servicenaam>` uit om te verifiëren dat de namen van de service-principals aan de serviceaccount zijn toegevoegd.
   De uitvoer voor de opdracht moet alle geregistreerde namen van de service-principal bevatten, zoals u hieronder kunt zien:

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<servername>.@example.com
   ```

```
HTTP/<servername>
<servername>/<servicename>@example.com
```

Hieronder vindt u een voorbeeld van de uitvoer:

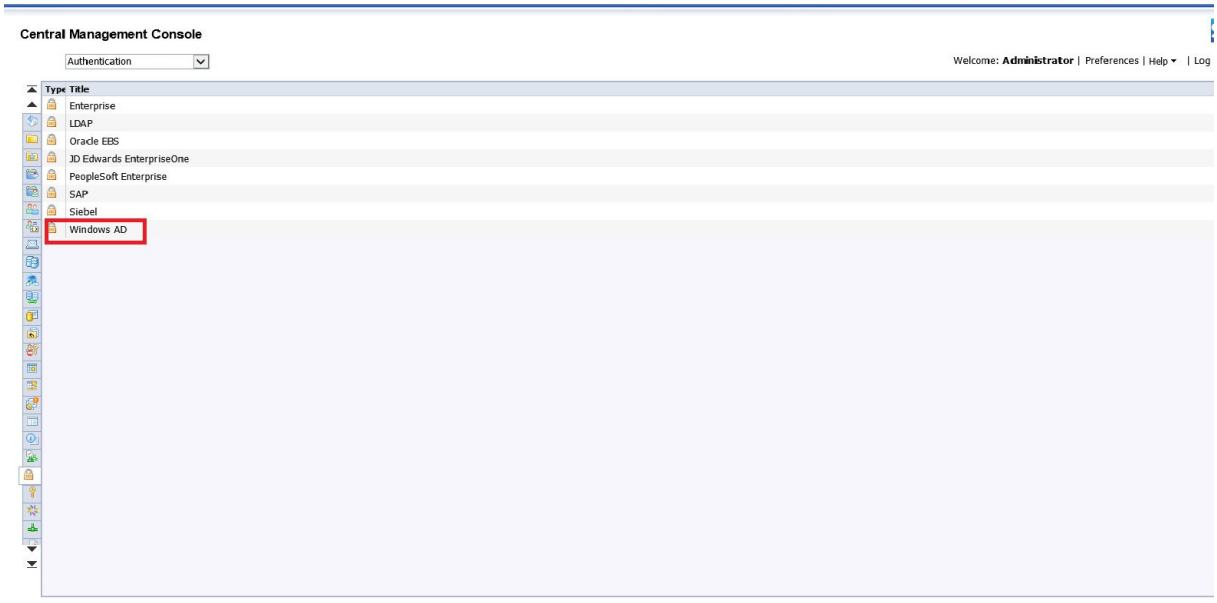
```
C:\Users\Admin>setspn -L bossosvcacct
Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
        BICMS/bossosvcacct@example.com
        HTTP/Tomcat HTTP/Tomcat@example.com
        HTTP/Load_Balancer.@example.com
```

Nadat u de serviceaccount hebt aangemaakt, moet u er rechten aan verlenen en moet u de account toevoegen aan de lokale beheerdersgroep van de server. De naam van de service-principal wordt gebruikt om in de volgende sectie AD-groepen te importeren.

9.4.3 AD-verificatie configureren in de CMC

9.4.3.1 Windows Active Directory-beveiligingsinvoegtoepassing

Met de Windows AD-beveiligingsinvoegtoepassing kunt u gebruikersaccounts en -groepen uit uw gebruikersdatabase van AD 2008 toewijzen aan het BI-platform. Dit maakt het ook mogelijk het systeem te gebruiken om alle aanmeldingsaanvragen waarvoor AD-verificatie is opgegeven, te controleren. Gebruikers worden geverifieerd in de AD-gebruikersdatabase en hun lidmaatschap van een toegewezen AD-groep wordt gecontroleerd voordat de CMS (Central Management Server) deze gebruikers een actieve BI-platformsessie toekent. U kunt de invoegtoepassing gebruiken om updates voor de geïmporteerde AD-groepen te configureren.



Met de Windows AD-beveiligingsinvoegtoepassing kunt u het volgende configureren:

- Windows AD-verificatie met Kerberos
- Windows AD-verificatie met NTLM
- Windows AD-verificatie met SiteMinder voor eenmalige aanmelding

De AD-beveiligingsinvoegtoepassing is compatibel met domeinen van AD 2008 die in de systeemeigen of gemengde modus worden uitgevoerd.

Zodra u de AD-gebruikers en -groepen hebt toegewezen, hebben zij toegang tot de clienthulpprogramma's van BI-platform via de verificatieoptie van *Windows AD*.

- Windows AD-verificatie werkt als de CMS wordt uitgevoerd onder Windows. SSO bij een database werkt alleen als de rapportservers worden uitgevoerd onder Windows. Alle andere servers en services kunnen op alle platforms worden uitgevoerd die door het BI-platform worden ondersteund.

  > ⓘ Opmerking
  >
  > De configuratie is alleen gedaan en getest met SUSE linux Enterprise 11.

- De Windows AD-invoegtoepassing voor het BI-platform ondersteunt domeinen in meerdere forests.

9.4.3.2 Windows AD-gebruikers en -groepen toewijzen

Voordat u AD-gebruikersgroepen in het BI-platform kunt importeren, moet u de volgende voorbereidingen treffen:

- U hebt een serviceaccount gemaakt op de domeincontroller voor het BI-platform. De account wordt gebruikt om BI-platformservers uit te voeren.

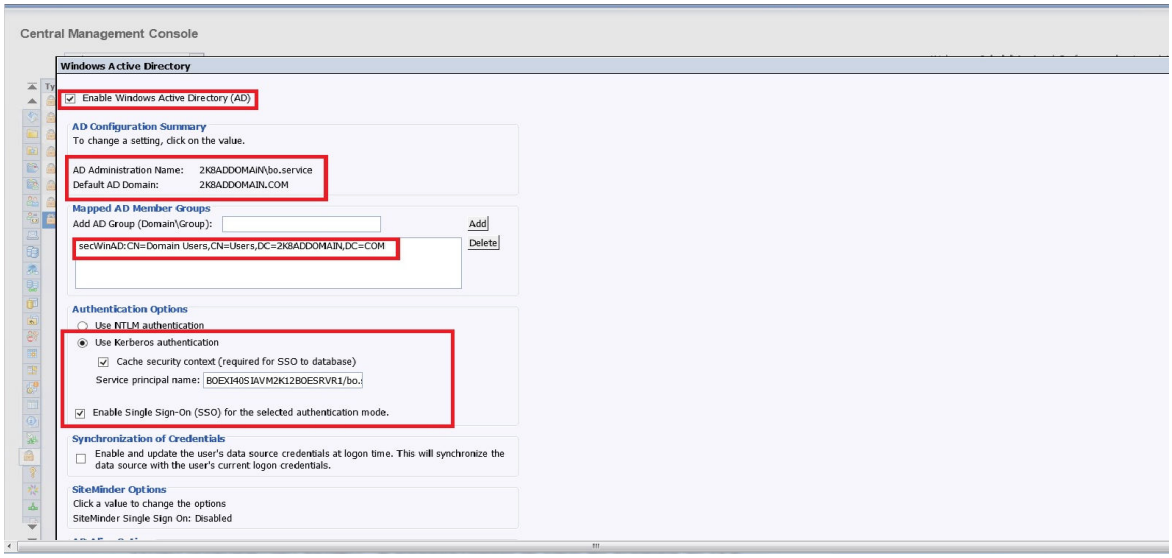
  > ⓘ Opmerking
  >
  > Om AD-verificatie met eenmalige aanmelding (SSO) van Vintela in te schakelen, geeft u een voor dit doel geconfigureerde SPN op. Aan de hand van de onderstaande stappen kunt u handmatige AD-verificatie bij het BI-platform configureren. Wanneer u handmatige AD-verificatie hebt geconfigureerd, raadpleegt u de sectie *Single Sign-On instellen* in dit hoofdstuk voor meer informatie over het toevoegen van SSO aan uw configuratie van AD-verificatie.

- U hebt geverifieerd dat de SPN met de naam van de computer waarop de SIA wordt uitgevoerd, aan de serviceaccount is toegevoegd.

Stap 1 tot en met 11 hieronder zijn verplicht bij het importeren van AD-groepen in het BI-platform.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Windows AD*.
3. Schakel het selectievakje *Windows Active Directory (AD) inschakelen* in.
4. Klik in het gebied *Overzicht van AD-configuratie* op de koppeling naast *AD-beheernaam*.

   > ⓘ Opmerking
   >
   > Voordat de Windows AD-invoegtoepassing is geconfigureerd, worden in plaats van deze koppeling aanhalingstekens weergegeven. Nadat u de configuratie hebt opgeslagen, worden AD-beheernamen aan de koppeling toegevoegd.



5. Voer de naam en het wachtwoord in van een ingeschakelde domeingebruikersaccount.

   Beheerreferenties kunnen de volgende notaties hebben:

   - NT-naam (`DomeinNaam\Gebruikersnaam`)
   - UPN (`gebruiker@DNS_domein_naam`)

   In het BI-platform wordt deze account gebruikt om te zoeken naar informatie uit AD. Er wordt geen inhoud uit AD gewijzigd, toegevoegd of verwijderd. Aangezien de informatie alleen wordt gelezen, zijn alleen de desbetreffende rechten nodig.

   > **Opmerking**
   >
   > AD-verificatie wordt niet voortgezet als de account die is gebruikt voor het lezen van de AD-map ongeldig wordt (bijvoorbeeld als het wachtwoord voor de account is gewijzigd of verlopen, of als de account is uitgeschakeld).

6. Voer het AD-domein in het vakje *Standaard AD-domein* in.

   Het domein moet als VOLLEDIGE DOMEINNAAM in HOOFDLETTERS worden opgegeven, of als naam van onderliggend domein waar de meeste gebruikers zich bij het BI-platform aanmelden. Dit moet overeenkomen met het standaarddomein dat is opgegeven in de Kerberos-configuratiebestanden die zijn gebruikt om de toepassingsserver te configureren. U kunt groepen uit het standaarddomein toewijzen zonder het voorvoegsel van de domeinnaam op te geven. Als u een standaard AD-domeinnaam invoert, hoeven gebruikers vanuit het standaarddomein de AD-domeinnaam niet meer in te voeren wanneer ze zich via AD-verificatie aanmelden bij het BI-platform.

7. Voer onder *Toegewezen AD-ledengroepen* het/de AD-domein/groep in het vak *AD-groep toevoegen (domein/groep)* in een van de volgende notaties in:

   - Security Account Manager-accountnaam (SAM), ook wel NT-naam genoemd (`Domeinnaam\Groepsnaam`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   > **Opmerking**
   >
   > Als u een lokale groep wilt toewijzen, kunt u alleen de NT-naamnotatie gebruiken: `\\<Servernaam>\<Groepsnaam>`. AD biedt geen ondersteuning voor lokale gebruikers. Lokale

gebruikers die tot een toegewezen lokale groep behoren, worden niet aan het BI-platform toegewezen. Deze gebruikers hebben daarom geen toegang tot het systeem.

> → Tip
>
> Gebruikers van andere domeinen die zich handmatig bij BI-startpunt aanmelden, moeten de domeinnaam in hoofdletters na hun gebruikersnaam opgeven. Zo is `CHILD.PARENTDOMAIN.COM` het domein in
>
> ```
> user@CHILD.PARENTDOMAIN.COM
> ```

8. Klik op *Toevoegen*.

   De groep wordt aan de lijst toegevoegd onder *Toegewezen AD-ledengroepen*.

9. Voer in het gebied *Toegewezen AD-ledengroepen* het/de gewenste AD-domein\-groep in het veld *AD-groep zoeken (domein\groep)* in.

   Er wordt dan naar de gewenste groep in de lijst gezocht. U kunt ook *Weergeven* kiezen om de volledige lijst met AD-groepen in een afzonderlijk dialoogvenster weer te geven.

10. Selecteer onder *Verificatieopties Kerberos-verificatie gebruiken*.
11. Voer in het vakje *Naam van serviceprincipal* de SPN in die is toegewezen aan de serviceaccount die u hebt gemaakt om BI-platformservers uit te voeren.

> ⓘ Opmerking
>
> Geef de SPN op voor de serviceaccount waarop de SIA wordt uitgevoerd. Bijvoorbeeld: `BICMS/bossosvcacct.domain.com`.

12. Klik op *Bijwerken*.

> ⚠ Let op
>
> Ga niet verder als gebruikers en/of groepen niet goed zijn toegewezen. Raadpleeg SAP Note 1631734 om problemen met specifieke AD-groepstoewijzingen op te lossen.

> ⓘ Opmerking
>
> Als u AD-groepsaccounts hebt toegewezen en geen AD-verificatieopties of AD-groepsupdates wilt configureren, slaat u stap 12 tot en met 19 over. U kunt deze optionele instellingen configureren nadat u handmatige AD Kerberos-verificatie hebt ingesteld.

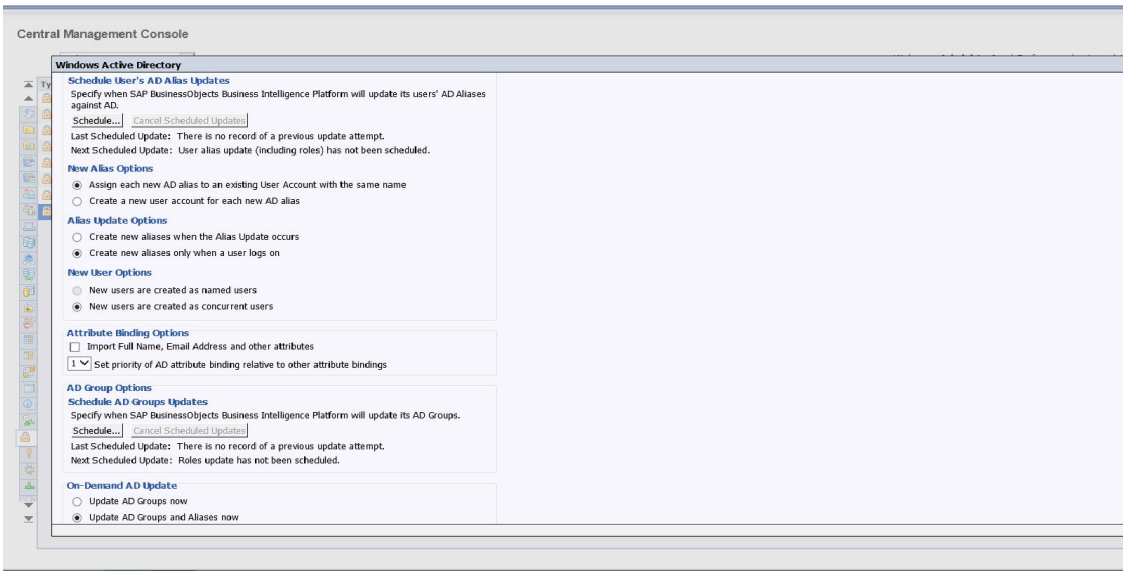
13. Als voor uw configuratie SSO bij een database is vereist, selecteert u *Beveiligingscontext in cache*.

> ⓘ Opmerking
>
> Als dit uw eerste configuratie van AD-verificatie is, wordt aanbevolen dat u eerst handmatige AD-verificatie instelt voordat u de extra configuratie overweegt die voor SSO is vereist.

14. Selecteer *Eenmalige aanmelding inschakelen voor geselecteerde verificatiemodus* als SSO vereist is voor de configuratie van AD-verificatie.
15. Selecteer een optie in het gebied *Synchronisatie van referenties* om de aanmeldingsreferenties voor de gegevensbron van de AD-gebruiker te activeren en bij te werken.

Met deze optie wordt de gegevensbron gesynchroniseerd met de huidige aanmeldingsreferenties van de gebruiker, zodat de gebruiker geplande rapporten kan uitvoeren wanneer de gebruiker niet is aangemeld bij het BI-platform en Kerberos SSO niet beschikbaar is.

16. Geef in het gebied *Opties voor AD-alias* op hoe nieuwe aliassen worden toegevoegd aan en bijgewerkt op het BI-platform.
    a. Selecteer in de lijst *Opties voor nieuwe alias* een optie voor het toewijzen van nieuwe aliassen aan Enterprise-accounts:
        - *Elke nieuwe AD-alias toewijzen aan een bestaande gebruikersaccount met dezelfde naam*
          Selecteer deze optie wanneer u weet dat gebruikers een bestaande Enterprise-account met dezelfde naam hebben. De AD-aliassen worden dus toegewezen aan bestaande gebruikers (de aliassen worden automatisch gemaakt). Gebruikers die geen bestaande Enterprise-account hebben of die niet dezelfde naam gebruiken in de Enterprise- en AD-account, worden toegevoegd als nieuwe gebruikers.
        - *Een nieuwe gebruikersaccount maken voor elke nieuwe AD-alias*
          Selecteer deze optie wanneer u voor elke gebruiker een nieuwe account wilt maken.
    b. Selecteer in het gebied *Bijwerkopties van alias* een optie voor het beheren van aliasupdates voor Enterprise-accounts:
        - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
          Gebruik deze optie als u automatisch een nieuwe alias wilt maken voor iedere AD-gebruiker die is toegewezen aan het BI-platform. Nieuwe AD-accounts worden toegevoegd voor gebruikers zonder BI-platformaccounts, of voor alle gebruikers als u de optie *Een nieuwe gebruikersaccount maken voor elke nieuwe AD-alias* hebt ingeschakeld en op *Bijwerken* hebt geklikt.
        - *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
          Selecteer deze optie wanneer de AD-map die u toewijst, veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van het BI-platform. Het platform maakt niet automatisch aliassen en Enterprise-accounts voor alle gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers die zich aanmelden bij het BI-platform.



    c. Selecteer in het gebied *Opties voor nieuwe gebruiker* een optie voor het maken van nieuwe gebruikers:
        - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
          Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam zijn gekoppeld aan specifieke gebruikers en geven personen toegang

tot het BI-platform op basis van een gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem, ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

> **Opmerking**
>
> Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het systeem, kan een licentie voor gelijktijdige toegang van 100 gebruikers bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

17. Klik op *Planning* als u wilt configureren hoe u updates van AD-aliassen wilt plannen.
    a. Selecteer in het dialoogvenster *Planning* een terugkeerpatroon in de lijst *Object uitvoeren*.
    b. Stel de overige opties en parameters voor de planning naar wens in.
    c. Klik op *Plannen*.
    Wanneer de aliassen worden bijgewerkt, worden de groepsgegevens ook bijgewerkt.
18. In het gebied *Opties voor attribuutbinding* kunt u de prioriteit voor attribuutbinding voor de AD-invoegtoepassing opgeven:
    a. Schakel het selectievakje *Volledige naam, e-mailadres en andere attributen importeren* in.
    De volledige namen en beschrijvingen die worden gebruikt in de AD-accounts, worden met gebruikersobjecten geïmporteerd en opgeslagen in het BI-platform.
    b. Geef een optie op voor *Prioriteit van AD-attribuutbinding instellen in verhouding tot andere attribuutbindingen*.

    Als u de optie instelt op 1, hebben AD-attributen prioriteit in scenario's waarbij AD en andere invoegtoepassingen (LDAP en SAP) zijn ingeschakeld. Is de optie op 3 ingesteld, dan hebben attributen van andere ingeschakelde invoegtoepassingen prioriteit. De bindingen moeten op verschillende waarden worden ingesteld. Als meerdere verificatie-invoegtoepassingen op dezelfde bindingwaarde zijn ingesteld, kan dit onverwachte gevolgen hebben.
19. Configureer updates van AD-groepen in het gebied *Opties voor AD-groepen*:
    a. Klik op *Plannen*.
    Het dialoogvenster *Planning* wordt weergegeven.
    b. Selecteer een terugkeerpatroon in de lijst *Object uitvoeren*.
    c. Stel zo nodig andere planningsopties en -parameters in.
    d. Klik op *Plannen*.

De update wordt gepland en uitgevoerd op basis van de opgegeven planningsgegevens. De volgende geplande update voor de AD-groepsaccounts wordt weergegeven onder de *Opties voor AD-groepen*.

20. Selecteer in het gebied *AD-update op aanvraag* een van de volgende opties:
    - *AD-groepen nu bijwerken*
      Selecteer deze optie als u alle geplande AD-groepen wilt bijwerken wanneer u op *Bijwerken* klikt. De volgende geplande update van AD-groepen wordt weergegeven onder *Opties voor AD-groepen*.
    - *AD-groepen en -aliassen nu bijwerken*
      Selecteer deze optie als u alle geplande AD-groepen en -gebruikersaliassen wilt bijwerken wanneer u op *Bijwerken* klikt. De volgende geplande updates worden weergegeven onder *Opties voor AD-groepen* en *Opties voor AD-alias*.
    - *AD-groepen en -aliassen nu niet bijwerken*
      Er worden geen AD-groepen of -gebruikersaliassen bijgewerkt wanneer u op *Bijwerken* klikt.
21. Klik op *Bijwerken* en klik vervolgens op *OK*.

Als u wilt verifiëren dat u AD-gebruikersaccounts hebt geïmporteerd, gaat u naar *CMC* > *Gebruikers en groepen* > *Groepshiërarchie* en selecteert u de AD-groep die u hebt toegewezen om gebruikers in die groep weer te geven. De huidige en geneste gebruikers in de AD-groep worden weergegeven.

Verwante informatie

Een Kerberos-configuratiebestand maken [pagina 305]

9.4.3.3 Updates voor Windows AD-groepen plannen

Met het BI-platform kunnen beheerders updates plannen voor AD-groepen en gebruikersaliassen. Deze functie is beschikbaar voor AD-verificatie met Kerberos of NTLM. Via de CMC kunt u ook de tijd en datum weergeven waarop de laatste update is uitgevoerd.

> **Opmerking**
>
> U moet configureren hoe updates voor uw AD-groepen en -aliassen worden gepland om AD-verificatie op het BI-platform mogelijk te maken.

Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U kunt het tijdstip waarop het object wordt gestart, en een begin- en einddatum opgeven.
Dagelijks	De update wordt elke dag of om het opgegeven aantal dagen uitgevoerd. U kunt het tijdstip opgeven waarop het object wordt uitgevoerd, plus een begin- en einddatum.
Wekelijks	De update wordt elke week uitgevoerd. Het kan eenmaal of verschillende keren per week worden uitgevoerd. U kunt de dagen en het tijdstip waarop het object wordt uitgevoerd, en een begin- en einddatum opgeven.

Terugkeerpatroon	Beschrijving
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Ne dag van de maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
X dag van de Ne week van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

AD-groepsupdates plannen

In het BI-platform is AD nodig voor gebruikers- en groepsgegevens. Het aantal query's dat naar AD wordt verzonden, wordt beperkt doordat met de AD-invoegtoepassing informatie over groepen, de onderlinge relaties en het gebruikerslidmaatschap in de cache worden geplaatst. De update wordt niet uitgevoerd als er geen specifieke planning is gedefinieerd.

U moet de CMC gebruiken om het terugkeerpatroon voor het vernieuwen van groepsupdates te configureren. U dient dit in te stellen om te laten zien hoe vaak u gegevens van groepslidmaatschappen wijzigt.

Updates voor AD-gebruikersaliassen plannen

Van gebruikersobjecten kan een alias worden gemaakt voor een AD-account zodat gebruikers zich met hun AD-referenties kunnen aanmelden bij BI-platform. Updates van AD-accounts worden door de AD-invoegtoepassing doorgegeven aan het BI-platform. Accounts die in AD worden gemaakt, verwijderd of uitgeschakeld, worden ook gemaakt, verwijderd of uitgeschakeld op het BI-platform.

Als u de updates van de AD-aliassen niet plant, worden deze alleen in de volgende gevallen bijgewerkt:

- Een gebruiker meldt zich aan.
- Een beheerder selecteert de optie *AD-groep en -aliassen nu bijwerken* in het gebied *AD-update op aanvraag* van de CMC.

> **Opmerking**
>
> Er worden geen AD-wachtwoorden opgeslagen in de gebruikersalias.

9.4.4 De BI-platformservice configureren om de SIA uit te voeren

9.4.4.1 De SIA uitvoeren onder de BI-platformserviceaccount

Voor ondersteuning van AD Kerberos-verificatie voor het BI-platform moet u aan de serviceaccount het recht toekennen om als onderdeel van het besturingssysteem te fungeren. Dit moet gebeuren op elke computer waarop de SIA (Server Intelligence Agent) met de CMS (Central Management Server) wordt uitgevoerd.

Als u de serviceaccount inschakelen om de SIA uit te voeren/te starten, moet u specifieke besturingssysteeminstellingen configureren die in deze sectie worden besproken.

> **Opmerking**
>
> Als eenmalige aanmelding voor de database is vereist, moet de SIA de volgende servers bevatten:
>
> - Crystal Reports-verwerkingsserver
> - Report Application Server
> - Web Intelligence-verwerkingsserver

9.4.4.2 De SIA configureren om onder de serviceaccount te worden uitgevoerd

Voordat u de SIA-account configureert om onder de serviceaccount van het BI-platform te worden uitgevoerd, moet u de volgende voorbereidingen treffen:

- Er is een serviceaccount gemaakt op de domeincontroller voor het BI-platform.
- U hebt geverifieerd dat de vereiste serviceprincipal-namen aan de serviceaccount zijn toegevoegd.
- U hebt AD-gebruikersgroepen toegewezen in het BI-platform.

Voer de volgende stappen uit als u een gebruiker specifieke rechten wilt geven:

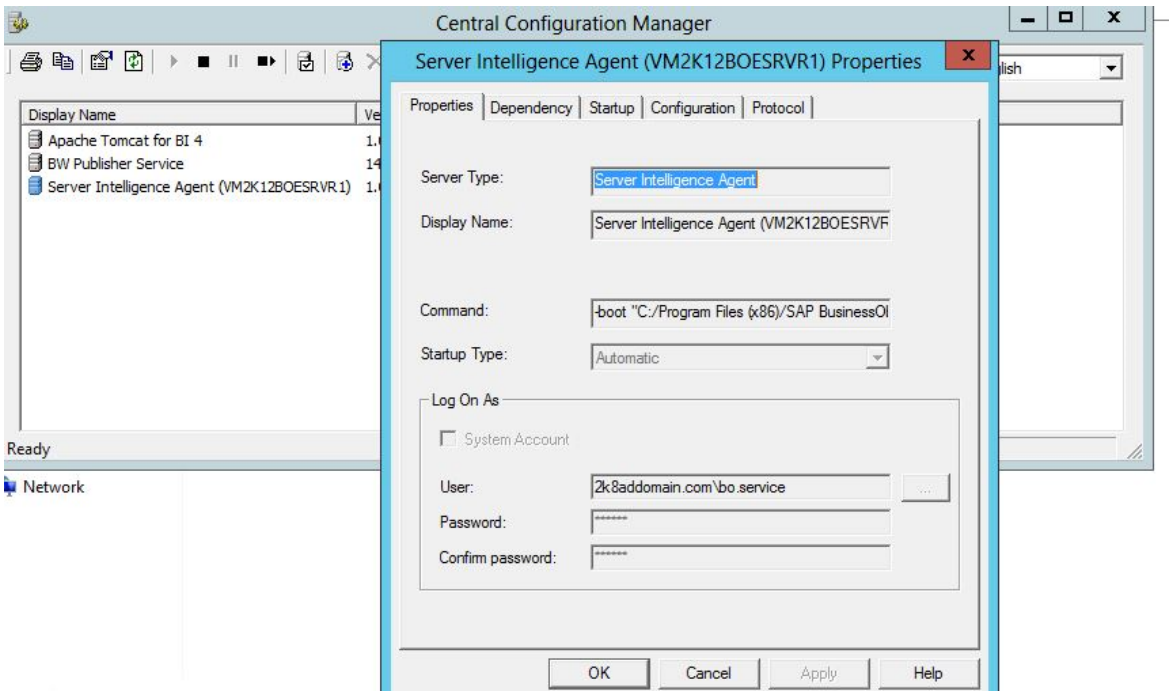
1. Klik op *Start> Configuratiescherm > Systeembeheer > Lokaal beveiligingsbeleid*.
2. Vouw *Lokaal beleid* uit en klik vervolgens op *Toewijzingen van gebruikersrechten*.
3. Dubbelklik op *Fungeren als deel van het besturingssysteem*.
4. Klik op *Toevoegen* en voer de naam in van de serviceaccount die u hebt gemaakt. Klik vervolgens op *OK*.

Voer deze taak voor elke SIA (Server Intelligence Agent) uit die services uitvoert die door de serviceaccount worden gebruikt.

1. Kies *Programma's* > *SAP Business Intelligence* > *SAP BusinessObjects BI-platform 4* > *Central Configuration Manager* om de CCM te starten.
   De startpagina van CCM wordt geopend.
2. Klik in de CCM met de rechtermuisknop op de SIA (Server Intelligence Agent) en kies *Stoppen*.

> **Opmerking**
>
> Wanneer u de SIA stopt, worden alle services die door de SIA worden beheerd ook gestopt.

3. Klik met de rechtermuisknop op de SIA en selecteer *Eigenschappen*.



4. Schakel het selectievakje *Systeemaccount* uit.
5. Typ de servicereferenties (`<DOMEINNAAM>\<servicenaam>`) en klik op *OK*.

   De serviceaccount moet de volgende rechten hebben op de computer waarop de SIA wordt uitgevoerd:

   - De account moet specifiek het recht "Functioneren als deel van het besturingssysteem" hebben.
   - De account moet specifiek het recht "Aanmelding als service" hebben.
   - Volledige beheerrechten voor de map waarin BI-platform is geïnstalleerd.
   - Volledige beheerrechten voor "HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects" in het systeemregister.
6. Herhaal deze stappen voor elke computer waarop een server van het BI-platform wordt uitgevoerd.

> **Opmerking**
>
> het is belangrijk dat de effectieve rechten worden gecontroleerd nadat u *Fungeren als deel van het besturingssysteem* hebt geselecteerd. Normaal gesproken moet u hiervoor de server opnieuw opstarten. Als deze optie nog niet is ingeschakeld wanneer u de server opnieuw hebt opgestart, worden de instellingen voor het lokale beleid vervangen door de instellingen voor het domeinbeleid.

7. Start de SIA opnieuw.
8. Herhaal zo nodig stap 1 tot en met 5 voor elke SIA waarmee een service wordt uitgevoerd die moet worden geconfigureerd.

U moet u nu bij de CCM kunnen aanmelden met AD-referenties.

9.4.4.3 AD-referenties testen op de CCM

Als u deze taak wilt uitvoeren, moet u een AD-gebruikersgroep in het BI-platform hebben toegewezen.

1. Open de CCM en klik op het pictogram *Servers beheren*.
2. Zorg dat de juiste informatie in het veld *Systeem* wordt weergegeven.
3. Selecteer *Windows AD* in de lijst met verificatieopties.
   Er wordt een aanmeldingsvenster weergegeven.
4. Meld u aan met een bestaande AD-account van de AD-groep die u aan het BI-platform hebt toegewezen.

> **Opmerking**
>
> Als u een AD-account gebruikt die zich niet in het standaarddomein bevindt, meldt u zich aan als `domein\gebruikersnaam`.

U moet geen foutberichten ontvangen. U moet zich via de CCM kunnen aanmelden met een toegewezen AD-account voordat u naar de volgende sectie gaat.

> **→ Tip**
>
> Als u een foutbericht ontvangt, gaat u naar *CMC* > *Verificatie* > *Windows AD*. Onder *Verificatieopties* wijzigt u *Kerberos-verificatie gebruiken* naar *NTLM-verificatie gebruiken* en klikt u op *Bijwerken*. Herhaal stap 1-4 hierboven. Als dit werkt, is er een probleem met uw Kerberos-configuratie.

9.4.5 De webtoepassingsserver configureren voor AD-verificatie

9.4.5.1 De toepassingsserver voorbereiden op Windows AD-verificatie (Kerberos)

Het proces waarbij Kerberos wordt geconfigureerd voor een webtoepassingsserver, varieert afhankelijk van de specifieke toepassingsserver. Configuratie van Kerberos bestaat doorgaans echter uit de volgende stappen:

- Het Kerberos-configuratiebestand (`krb5.ini`) maken.
- Het configuratiebestand voor JAAS-aanmelding (`bscLogin.conf`) maken.

> **Opmerking**
>
> Deze stap is niet vereist voor de SAP NetWeaver 7.3 Java-toepassingsserver. U moet de LoginModule echter toevoegen aan uw SAP NetWeaver-server.

- De Java-opties wijzigen voor uw toepassingsserver.
- De eigenschappen van bestand `BOE.war` overschrijven voor Windows AD-verificatie.
- De Java-toepassingsserver opnieuw starten.

Deze sectie bevat de details voor de configuratie van Kerberos voor gebruik met de volgende toepassingsservers:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Kerberos-configuratiebestanden maken

9.4.5.1.1.1 Een Kerberos-configuratiebestand maken

Voordat u verdergaat, moet u de volgende vereiste taken hebben uitgevoerd:

- Er is een serviceaccount gemaakt op de domeincontroller voor het BI-platform.
- U hebt geverifieerd dat de serviceprincipal-namen aan de serviceaccount zijn toegevoegd.
- U hebt AD-gebruikersgroepen toegewezen in het BI-platform.
- U hebt AD-referenties op de CCM getest.

Voer deze stappen uit om het Kerberos-configuratiebestand te maken als u SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere of WebLogic als de webtoepassingsserver voor uw implementatie van het BI-platform gebruikt.

1. Maak het bestand `krb5.ini` als dit nog niet bestaat en sla het op in `C:\Windows` voor Windows.

   > **Opmerking**
   >
   > Als de toepassingsserver is geïnstalleerd onder Unix, moet u de volgende mappen gebruiken:
   >
   > Solaris: `/etc/krb5/krb5.conf`
   >
   > Linux: `/etc/krb5.conf`

   > **Opmerking**
   >
   > U kunt dit bestand opslaan op een andere locatie. Als u dit doet, moet u de locatie echter opgeven in de Java-opties. Ga voor meer informatie over `krb5.ini` naar http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view .

2. Voeg de volgende vereiste informatie toe aan het Kerberos-configuratiebestand:

```
[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 =
}
```

ⓘ Opmerking

De sleutelparameters worden in de onderstaande tabel toegelicht.

`DOMAIN.COM`	De DNS-naam van uw domein dat in hoofdletters in FQDN-notatie moet worden ingevoerd.
`kdc`	De hostnaam van de domeincontroller.
`[capath]`	Definieert de vertrouwensrelatie tussen domeinen die zich in een ander AD-forest bevinden. In het vorige voorbeeld is `DOMAIN2.COM` een domein in een extern forest met een niet-transitieve tweerichtingsvertrouwensrelatie naar `DOMAIN.COM`.
`default_realm`	In een configuratie met meerdere domeinen kan onder `[libdefaults]` de waarde `default_realm` elk brondomein zijn. U kunt het beste het domein gebruiken met het grootste aantal gebruikers dat de verificatie uitvoert met de AD-account. Als tijdens het aanmelden geen UPN-achtervoegsel wordt toegepast, wordt de standaardwaarde `default_realm` gebruikt. Deze waarde moet overeenkomen met de instelling *standaarddomein* in de CMC. Alle domeinen moeten in hoofdletters worden opgegeven, zoals u in het bovenstaande voorbeeld kunt zien.

9.4.5.1.2 Een JAAS-aanmeldingsconfiguratiebestand maken

9.4.5.1.2.1 Een configuratiebestand voor de Tomcat of WebLogic JAAS-aanmelding maken

Het bestand `bscLogin.conf` wordt gebruikt om de invoegtoepassing voor Java-aanmelding te laden en is vereist voor AD Kerberos-verificatie op Java-webtoepassingsservers.

De standaardlocatie voor de bestanden is `C:\Windows`.

1. Maak een bestand met de naam `bscLogin.conf` als dit nog niet bestaat en sla het op de locatie `C:\Windows` op.

> **Opmerking**
>
> U kunt dit bestand opslaan op een andere locatie. Als u dit doet, moet u de locatie echter opgeven in de Java-opties.

2. Voeg de volgende code toe aan het JAAS-configuratiebestand `bscLogin.conf`:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Sla het bestand op en sluit het.

9.4.5.1.2.2 Een configuratiebestand voor de Oracle JAAS-aanmelding maken

1. Zoek het bestand `jazn-data.xml`.

> **Opmerking**
>
> De standaardlocatie voor dit bestand is `C:\OraHome_1\j2ee \home\config`. Als u Oracle Application Server op een andere locatie hebt geïnstalleerd, zoekt u het specifieke bestand voor uw installatie op.

2. Voeg de volgende inhoud toe aan het bestand tussen de codes `<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. Sla het bestand `jazn-data.xml` op en sluit het.

9.4.5.1.2.3 Een configuratiebestand voor de WebSphere JAAS-aanmelding maken

1. Maak een bestand met de naam `bscLogin.conf` als dit nog niet bestaat en sla het op de standaardlocatie `C:\Windows` op.
2. Voeg de volgende code toe aan het configuratiebestand `bscLogin.conf`:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Sla het bestand op en sluit het.

9.4.5.1.2.4 Een LoginModule toevoegen aan SAP NetWeaver AS

Als u Kerberos en SAP NetWeaver AS 7.3 wilt gebruiken, configureert u het systeem alsof u de Tomcat-webtoepassingsserver gebruikt. U hoeft geen `bscLogin.conf`-bestand te maken.

Hierna voegt u een LoginModule toe en werkt u enkele Java-instellingen in SAP NetWeaver AS 7.3 bij.

Teneinde de `com.sun.security.auth.module.Krb5LoginModule` toe te wijzen aan `com.businessobjects.security.jgss.initiate`, moet u handmatig een LoginModule aan SAP NetWeaver AS 7.3 toevoegen.

1. Open SAP NetWeaver Administrator door het volgende adres in een webbrowser in te voeren: `http://<computernaam>:<poort>/nwa`.
2. Klik op *Configuratiebeheer* > *Beveiliging* > *Verificatie* > *Aanmeldingsmodules* > *Bewerken*.
3. Voeg een nieuwe aanmeldingsmodule toe met de volgende informatie:

Weergavenaam	**`Krb5LoginModule`**
Klassenaam	**`com.sun.security.auth.module.Krb5LoginModule`**

4. Klik op *Opslaan*.
   SAP NetWeaver maakt de nieuwe module.
5. Klik op *Onderdelen* > *Bewerken*.
6. Voeg een nieuw beleid toe met de naam **`com.businessobjects.security.jgss.initiate`**.
7. Voeg de aanmeldingsmodule uit stap 3 toe aan de *Aanmeldmodulestack* en stel deze in op *Vereist*.
8. Controleer of er geen andere vermeldingen in *Opties voor geselecteerde aanmeldingsmodule* staan. Zo ja, verwijder ze dan.
9. Klik op *Opslaan*.
10. Meld u af bij SAP NetWeaver Administrator.

9.4.5.1.3 De Java-instellingen van de toepassingsserver wijzigen om configuratiebestanden te laden

9.4.5.1.3.1 Java-opties voor Kerberos op Tomcat wijzigen

1. Selecteer in het menu *Start* achtereenvolgens *Programma's* > *Tomcat* > *Tomcat-configuratie*.
2. Klik op het tabblad *Java*.
3. Voeg de volgende opties toe:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

   Vervang XXXX door de locatie waar u het bestand `bscLogin.conf` hebt opgeslagen.

4. Sluit het Tomcat-configuratiebestand.
5. Start Tomcat opnieuw.

9.4.5.1.3.2 De Java-opties voor SAP NetWeaver AS 7.3 wijzigen

1. Ga naar het hulpprogramma voor Java-configuratie (standaard in `C:\usr\sap\<NetWeaver-ID>\<exemplaar>\j2ee\configtool\`) en dubbelklik op `configtool.bat`.
   Het hulpprogramma voor configuratie wordt geopend.
2. Klik op *Weergave* > *Expertmodus*.
3. Vouw *Clustergegevens* > *Sjabloon* uit.
4. Selecteer het exemplaar dat overeenkomt met uw SAP NetWeaver-toepassingsserver (bijvoorbeeld *Exemplaar* - `<systeem-ID><computernaam>`).
5. Klik op *VM-parameters*.
6. Selecteer *SAP* in de lijst *Leverancier* en vervolgens *GLOBAAL* in de lijst *Platform*.
7. Klik op *Systeem* en voeg de volgende aangepaste parametergegevens toe:

java.security.krb5.conf	`<pad naar het bestand krb5.ini inclusief de bestandsnaam>`
javax.security.auth.useSubjectCredsOnly	false

8. Klik op *Opslaan* en vervolgens op *Configuratie-editor*.
9. Klik op *Configuraties* > *Beveiliging* > *Configuraties* > *com.businessobjects.security.jgss.initiate* > *Beveiliging* > *Verificatie*.
10. Klik op *Bewerkingsmodus*.
11. Klik met de rechtermuisknop op het knooppunt *Verificatie* en selecteer *Subknooppunt maken*.
12. Selecteer *Waarde-invoer* in de bovenste lijst.
13. Typ het volgende:

Naam	create_security_session
Waarde	false

14. Klik op *Maken* en sluit het venster.
15. Klik op *Configuratiehulpmiddel* en op *Opslaan*.

Nadat u de configuratie hebt bijgewerkt, moet u uw SAP NetWeaver-toepassingsserver opnieuw starten.

9.4.5.1.3.3 Java-opties voor Kerberos op WebLogic wijzigen

Als u Kerberos gebruikt met WebLogic, moet u de Java-opties wijzigen om de locatie van het Kerberos-configuratiebestand en de Kerberos-aanmeldingsmodule op te geven.

1. Stop het WebLogic-domein dat uw BI-platformtoepassingen uitvoert.
2. Open het script waarmee het WebLogic-domein met de BI-platformtoepassingen wordt gestart (`startWeblogic.cmd` voor Windows, `startWebLogic.sh` voor Unix).
3. Voeg de volgende gegevens toe aan de sectie Java_Options van het bestand:

   ```
   set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
   -Djava.security.krb5.conf=C:/XXX/krb5.ini
   ```

   Vervang XXXX door de locatie waar u het bestand hebt opgeslagen.
4. Start het WebLogic-domein waarin de BI-platformtoepassingen worden uitgevoerd opnieuw.

9.4.5.1.3.4 Java-opties voor Kerberos op WebSphere wijzigen

1. Meld u aan bij de beheerconsole van WebSphere.

   Voor IBM WebSphere 5.1 typt u `http://servernaam:9090/admin` Voor IBM WebSphere 6.0 typt u `http://servername:9060/ibm/console`
2. Vouw Server uit, klik op *Application Servers* en klik op de naam van de toepassingsserer die u hebt gemaakt voor gebruik met het BI-platform.
3. Ga naar de *JVM*-pagina.

   Als u werkt met WebSphere 5.1, voert u de volgende stappen uit om de *JVM*-pagina weer te geven.
   1. Schuif op de serverpagina omlaag tot u *Process Definition* in de kolom *Additional Properties* ziet.
   2. Klik op *Process Definition*.
   3. Schuif omlaag en klik op *Java Virtual Machine*.

   Als u werkt met WebSphere 6.0, voert u de volgende stappen uit om de *JVM*-pagina weer te geven.
   1. Selecteer *Java and Process Management* op de serverpagina.
   2. Selecteer *Process Definition*.
   3. Selecteer *Java Virtual Machine*.
4. Klik op *Generieke JVM-argumenten* en geef de locatie van het bestand `Krb5.ini` en de locatie van het bestand `bscLogin.conf` op.

   -Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

   -Djava.security.krb5.conf=C:\XXXX\krb5.ini

   Vervang XXXX door de locatie waar u het bestand hebt opgeslagen.
5. Klik op *Apply* en vervolgens op *Save*.
6. Stop de server en start deze opnieuw.

9.4.5.1.4 Verifiëren dat Java een Kerberos-ticket kan ontvangen

Voordat u kunt testen of Java het Kerberos-ticket heeft ontvangen, moet u de volgende voorbereidingen treffen:

- Maak het bestand `bscLogin.conf` voor uw toepassingsserver.
- Maak het bestand `krb5.ini`.

1. Ga naar de opdrachtprompt en navigeer naar de map `jdk\bin` in uw installatie van het BI-platform.

   Deze bevindt zich standaard in:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Voer `kinit <gebruikersnaam>` uit.
3. Druk op `Enter`.
4. Typ het wachtwoord.

```
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
```

   Als het bestand `krb5.ini` goed is geconfigureerd en de Java-aanmeldingsmodule is geladen, moet u het volgende bericht zien:

```
Nieuw ticket is opgeslagen in cachebestand
C:\Users\Administrator\krb5cc_Administrator
```

Ga niet verder met de set-up van AD tot u een Kerberos-ticket hebt ontvangen.

Als u geen ticket kunt ontvangen, hebt u de volgende mogelijkheden:

- Raadpleeg de sectie voor probleemoplossing aan het eind van dit hoofdstuk.
- Voor problemen met de KDC, de Kerberos-configuratiebestanden en gebruikersreferenties die niet beschikbaar zijn in de Kerberos-database, raadpleegt u SAP Knowledge Base-artikelen KBA 1476374 en KBA 1245178.

9.4.5.1.5 BI-startpunt configureren voor handmatige AD-aanmelding

Voordat u uw BI-platformtoepassingen configureert voor handmatige AD-aanmelding, moet u de volgende voorbereidingen treffen:

- U hebt een serviceaccount gemaakt op de domeincontroller voor het BI-platform.
- U hebt geverifieerd dat de HTTP-serviceprincipalnamen aan de serviceaccount zijn toegevoegd.
- U hebt AD-gebruikersgroepen toegewezen in het BI-platform.
- U hebt AD-referenties op de CCM getest.
- U hebt de vereiste configuratiebestanden voor uw webtoepassingsserver gemaakt, geconfigureerd en getest.
- De Java-instellingen van uw toepassingsserver zijn gewijzigd om de configuratiebestanden te laden.

Voer de volgende stappen uit om de Windows AD-verificatieoptie voor BI-startpunt te activeren:

1. Open de aangepaste map voor de BOE-webtoepassing op de computer die de webtoepassingsserver host:

   `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

Breng uw wijzigingen in de map `config\custom` en niet de map `config\default` aan. Uw wijzigingen worden anders overschreven wanneer in de toekomst patches op uw implementatie worden toegepast.

U moet de gewijzigde BOE-webtoepassing later opnieuw implementeren.

2. Maak een nieuw bestand.

> **Opmerking**
>
> Gebruik Kladblok of een ander programma voor tekstverwerking.

3. Sla het bestand op als `BIlaunchpad.properties`.
4. Voer het volgende in:

```
authentication.visible=true
authentication.default=secWinAD
```

5. Sla het bestand op en sluit het.
6. Start de webtoepassingsserver opnieuw op.

U moet u nu handmatig kunnen aanmelden bij BI-startpunt, een van de toepassingen kunnen openen en Windows AD in de lijst met verificatieopties kunnen selecteren.

> **Opmerking**
>
> Zet uw Windows AD-installatie niet voort tot u zich handmatig bij BI-startpunt met een bestaande AD-account kunt aanmelden.

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde BOE-webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om BOE opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.

> **Opmerking**
>
> Als uw implementatie een firewall gebruikt, moet u alle vereiste poorten openen. Als u dit niet doet, kunnen de webtoepassingen geen verbinding maken met de BI-platformservers.

9.4.6 Eenmalige aanmelding instellen

9.4.6.1 SSO bij het BI-platform met AD-verificatie

Opties voor SSO met Windows AD

Er worden drie methoden ondersteund voor het instellen van eenmalige aanmelding voor Windows AD-verificatie met het BI-platform:

- Vintela: deze optie kan alleen met Kerberos worden gebruikt.
- SiteMinder: deze optie kan alleen met Kerberos worden gebruikt.

SSO bij de database

SSO bij de database stelt aangemelde gebruikers in staat om handelingen uit te voeren waarvoor databasetoegang is vereist, met name het weergeven en vernieuwen van rapporten, zonder dat ze hun aanmeldingsreferenties opnieuw moeten opgeven. Hoewel beperkte machtiging optioneel is voor AD-verificatie en Vintela SSO, is het vereist bij implementaties met eenmalige aanmelding bij de systeemdatabase.

End-to-end SSO

In het BI-platform wordt eenmalige end-to-end-aanmelding ondersteund via Windows Active Directory en Kerberos. In dit scenario beschikken gebruikers zowel over eenmalige aanmelding bij het BI-platform bij de front-end als SSO-toegang tot de databases bij de back-end. Gebruikers hoeven in dit geval slechts eenmaal hun aanmeldingsgegevens op te geven, namelijk wanneer ze zich bij het besturingssysteem aanmelden, om toegang te krijgen tot het BI-platform en om acties te kunnen uitvoeren waarvoor databasetoegang nodig is, zoals het weergeven van rapporten.

Configuratie van handmatige versus SSO AD-verificatie

Wanneer u uw implementatie hebt geconfigureerd zodat AD-accounts handmatig bij BI-startpunt kunnen worden aangemeld, moet u teruggaan naar de set-up van AD-verificatie om specifieke SSO-vereisten te activeren. Vereisten zijn afhankelijk van de gekozen SSO-methode.

9.4.6.2 Vintela SSO gebruiken

9.4.6.2.1 Controlelijst voor set-up van Vintela SSO

Als u het BI-platform wilt instellen om met Vintela SSO te werken, moet u de volgende taken uitvoeren:

1. Uw serviceaccount specifiek voor Vintela SSO configureren.
2. Beperkte machtiging configureren (optioneel).
3. De verificatieopties voor Windows AD SSO in de CMC configureren.
4. De algemene eigenschappen en specifieke eigenschappen van BI-startpunt voor Vintela SSO configureren.
5. Als u Tomcat als webtoepassingsserver voor uw implementatie gebruikt, moet u de limiet van de koptekstgrootte verhogen.
6. De internetbrowsers configureren voor Vintela.

9.4.6.2.2 De serviceaccount instellen voor Vintela SSO

Het opdrachtregelprogramma `Ktpass` configureert de serverprincipal-naam voor de host of service in Active Directory en genereert een Kerberos 'Keytab'-bestand dat de sleutel van het gedeelde geheim van de

serviceaccount bevat. Dit programma bevindt zich meestal op domeincontrollers of kan worden gedownload van de Microsoft-ondersteuningssite: http://support.microsoft.com/kb/892777 .

Er is een serviceaccount vereist die specifiek geconfigureerd is om gebruikers in een bepaalde Windows AD-groep toe te staan zich automatisch met hun AD-referenties bij BI-startpunt te verifiëren. U kunt de serviceaccount die voor AD Kerberos-verificatie op de domeincontroller is gemaakt, opnieuw configureren.

Wanneer een client probeert zich aan te melden bij BI-startpunt, wordt een aanvraag gestart bij de Kerberos-server die tickets genereert. De serviceaccount die voor het BI-platform is gemaakt, moet een SPN hebben die overeenkomt met de URL van de toepassingsserver om deze aanvraag te kunnen verwerken. Voer de volgende stappen uit op de computer waarop de domeincontroller wordt gehost.

1. Voer de keytab-setup-opdracht `ktpass` van Kerberos uit om een `keytab`-bestand te maken en op te slaan.

   Geef de `ktpass`-parameters op die in de volgende tabel worden weergegeven:

Parameter	Beschrijving
`-out`	Hiermee wordt de naam opgegeven van het `keytab`-bestand van Kerberos dat moet worden gegenereerd.
`-princ`	Hiermee wordt de naam van de principal in SPN-opmaak opgegeven die voor de serviceaccount wordt gebruikt:`< MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM`, waarbij `<MYSIAMYSERVER>` de naam van de Service Intelligence Agent is zoals opgegeven in de Central Configuration Manager (CCM). **Opmerking** Voor de naam van uw serviceaccount wordt onderscheid gemaakt tussen hoofdletters en kleine letters. De SPN bevat de naam van de hostcomputer waarop het service-exemplaar wordt uitgevoerd. **Tip** De SPN moet uniek zijn in het forest waarin deze is geregistreerd. U controleert dit door het Windows-ondersteuningsprogramma `Ldp.exe` uit te voeren om naar de SPN te zoeken.
`-pass`	Hiermee wordt het wachtwoord opgegeven dat door de serviceaccount wordt gebruikt.
`-ptype`	Hiermee wordt het principal-type opgegeven: `-ptype KRB5_NT_PRINCIPAL`
`-crypto`	Hiermee wordt het coderingstype opgegeven dat met de serviceaccount moet worden gebruikt: `-crypto RC4-HMAC-NT`

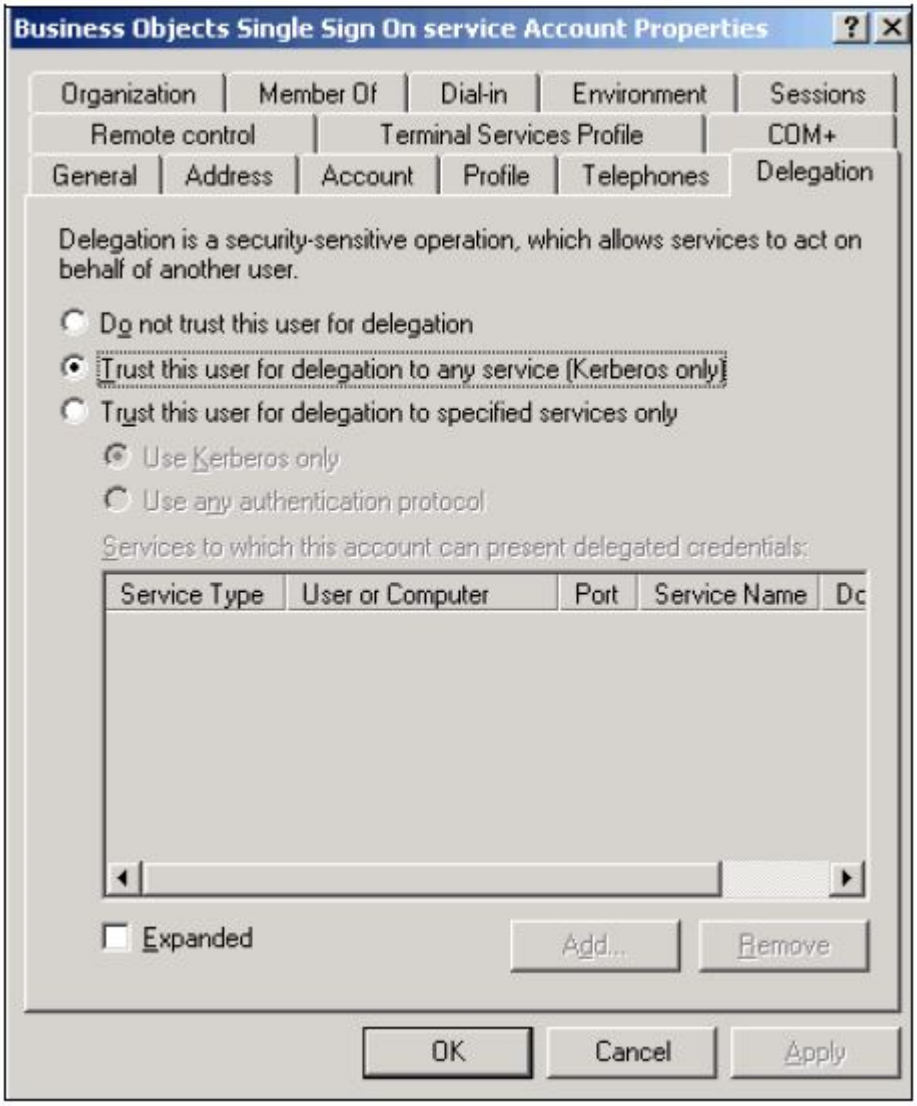
   Bijvoorbeeld:

```
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
```

   De uitvoer van de opdracht `ktpass` moet de doeldomeincontroller bevestigen, en dat een Kerberos `keytab`-bestand met het gedeelde geheim is gemaakt. Met de opdracht wordt ook de naam van de principal aan de (lokale) serviceaccount toegewezen.

2. Klik met de rechtermuisknop op de serviceaccount, selecteer *Eigenschappen* > *Machtiging* .

3. Klik op *Deze gebruiker mag delegeren aan alle services (alleen Kerberos)*.



4. Klik op *OK* om de instellingen op te slaan.

De serviceaccount heeft nu alle vereiste serviceprincipal-namen voor Vintela SSO, en u hebt een keytab-bestand gegenereerd met het gecodeerde wachtwoord voor de serviceaccount.

> **Opmerking**
>
> Voor eenmalige end-to-end-aanmelding of eenmalige aanmelding op databases met behulp van keytab-bestandsscenario's:
>
> In gevallen van fouten die zijn opgelost door KVNO in de keytab te wijzigen, is het waarschijnlijk dat het KVNO-attribuut op de serviceaccount hoger is dan de KVNO die in het creëren van de keytab (tijdens ktpass) wordt gebruikt. Zie http://service.sap.com/sap/support/notes/1853668 voor informatie over hoe u het correcte sleutelversienummer kunt vinden

9.4.6.2.2.1 Beperkte machtiging voor Vintela SSO configureren

Beperkte machtiging is optioneel voor het instellen van Vintela SSO. Het is echter verplicht voor implementaties waarbij SSO bij de systeemdatabase vereist is.

1. Open de Active Directory-module *Gebruikers en computers* op de computer met de AD-domeincontroller.
2. Klik met de rechtermuisknop op de serviceaccount die u in de vorige sectie hebt gemaakt, en klik op *Eigenschappen* > *Machtiging*.
3. Selecteer *Deze gebruiker mag alleen delegeren aan opgegeven services*.
4. Selecteer *Alleen Kerberos gebruiken*.
5. Klik op *Toevoegen* > *Gebruikers of computers*.
6. Voer de naam van de serviceaccount in en klik op *OK*.
   Er wordt een lijst met services weergegeven.
7. Selecteer de volgende services en klik op *OK*.
   - De HTTP-service
   - De service die wordt gebruikt om de SIA (Service Intelligence Agent) uit te voeren op de computer die het BI-platform host.

   De services worden toegevoegd aan de lijst met services die kunnen worden gedelegeerd voor de serviceaccount.

U moet de eigenschappen van de webtoepassing bewerken om rekening te houden met deze wijziging.

9.4.6.2.3 SSO-instellingen configureren in de CMC

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Windows AD*.
3. Zorg dat het selectievakje *Windows Active Directory (AD) inschakelen* is ingeschakeld.
4. Zorg dat onder *Verificatieopties* de optie *Kerberos-verificatie gebruiken* is geselecteerd.
5. Als voor uw configuratie SSO bij de database is vereist, selecteert u *Beveiligingscontext in cache*.
6. Selecteer *Eenmalige aanmelding inschakelen voor geselecteerde verificatiemodus*.
7. Klik op *Bijwerken*.

9.4.6.2.4 eenmalige aanmelding van Vintela inschakelen voor BI-startpunt en OpenDocument

Deze procedure moet worden gebruikt voor BI-startpunt of OpenDocument. Als u SSO bij de webtoepassingen van BI-platform wilt inschakelen, moet u Vintela- en SSO-specifieke eigenschappen opgeven in het bestand `BOE.war`. Voor SSO-installatiedoeleinden is het raadzaam om eerst SSO bij BI-startpunt voor AD-accounts in te schakelen voordat u dit voor andere toepassingen doet.

1. Open de aangepaste map voor de BOE-webtoepassing op de computer die de webtoepassingsserver host: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Breng uw wijzigingen in de map `config\ustom` en niet de map `config\default` aan. Uw wijzigingen worden anders overschreven wanneer in de toekomst patches op uw implementatie worden toegepast.

   U moet de gewijzigde BOE-webtoepassing later opnieuw implementeren.
2. Maak een nieuw bestand in een teksteditor.
3. Typ het volgende:

```
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
```

> **Opmerking**
>
> De parameters `idm.realm` en `idm.princ` vereisen geldige waarden. `Idm.realm` moet dezelfde waarde hebben als de waarde die u hebt ingesteld bij het configureren van de `standaardrealm` in het bestand `krb5.ini`. De waarde moet worden ingevoerd in hoofdletters. De parameter `idm.princ` is de SPN die wordt gebruikt voor de serviceaccount die is gemaakt voor Vintela SSO.

> **Opmerking**
>
> U moet forwardslashes gebruiken om de locatie van het Keytab-bestand op te geven.

   Sla de volgende stap over als u geen beperkte machtiging wilt gebruiken voor Windows AD-verificatie en Vintela SSO.
4. Voeg het volgende toe om beperkte machtiging te gebruiken:

```
idm.allowS4U=true
```

5. Sluit het bestand en sla het op met de naam `global.properties`.

> **Opmerking**
>
> Zorg ervoor dat de bestandsnaam niet wordt opgeslagen met extensies zoals `.txt`.

6. Maak nog een bestand in dezelfde map. Sla het bestand op als `OpenDocument.properties` of `BIlaunchpad.properties` al naar gelang uw vereisten.
7. Voer het volgende in:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

   Bijvoorbeeld:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Sla het bestand op en sluit het.
9. Start de webtoepassingsserver opnieuw op.

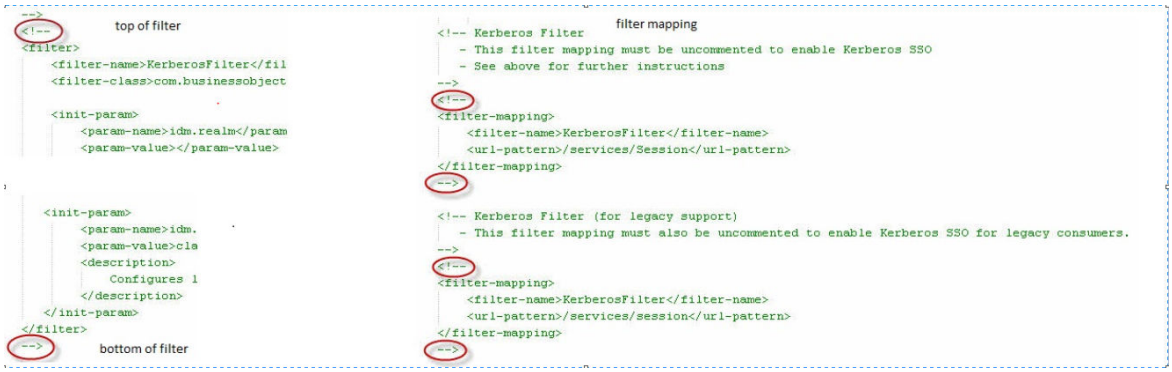
De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde BOE-webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om BOE opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.

> **Opmerking**
>
> Als uw implementatie een firewall gebruikt, moet u alle vereiste poorten openen. Als u dit niet doet, kunnen de webtoepassingen geen verbinding maken met de BI-platformservers.

9.4.6.2.5 Eenmalige aanmelding van Vintela inschakelen voor webservices

Sommige clienthulpprogramma's moeten worden geverifieerd via webservices. Volg deze stappen om eenmalige aanmelding voor webservices te activeren. Zie voor meer informatie SAP Note op: http://service.sap.com/sap/support/notes/1646920

1. Maak een back-up van dit bestand: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml` en open het bestand om het te bewerken.
2. Verwijder het commentaar uit de secties voor het Kerberox-proxyfilter en het Kerberos-filter om eenmalige aanmelding van Kerberos voor Windows Active Directory-verificatie (secWinAD) te activeren.



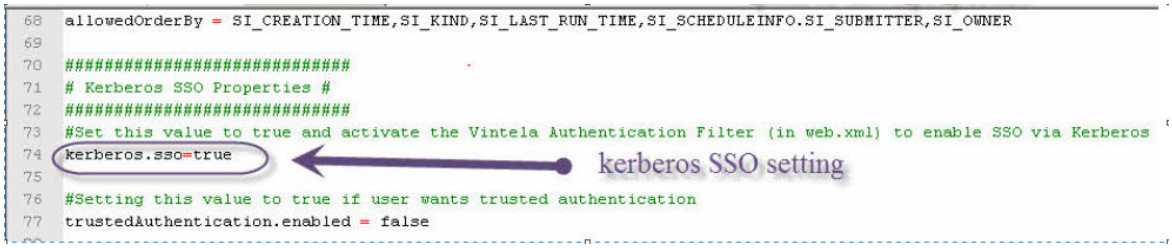
De volgende opties moeten worden opgegeven (de overige opties zijn optioneel):

- `idm.realm` (hetzelfde als de default_realm die is opgegeven in het bestand Krb5.ini).
- `idm.princ` (hetzelfde als opgegeven voor idm.princ in het bestand global.properties dat zich bevindt op `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
- `idm.keytab` (hetzelfde als opgegeven voor idm.keytab in het bestand global.properties dat zich bevindt op `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

> **Opmerking**
>
> Als u het hardcoded wachtwoord gebruikt dat is ingesteld in de Java-opties van Tomcat, moet u de keytab-regels in het bestand `web.xml` niet wijzigen.

3. Als SSL niet wordt gebruikt met de Java-toepassingsserver, stelt u de parameter idm.allowUnsecured in op **`true`**.

   Voor meer informatie over Tomcat SSL raadpleegt u Knowledge Base-artikel-id:1484802.
4. Maak een back-up van dit bestand: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties` en open het bestand om het te bewerken.
5. Stel kerberos.sso in op **`true`** en sla het bestand op.



6. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren.

   Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.
7. Start Tomcat opnieuw.
8. Als u uw instellingen wilt testen, start u Query as a Web Service Designer op de clientcomputer waarop clienthulpprogramma's zijn geïnstalleerd.
9. Voeg een nieuwe beheerde host toe.
10. Voer de naam van de toepassingsserver in.
11. Voer de URL van de webservices in met de volgende notatie: `http://<Webtoepassingsserver>:<poortnummer>/dswsbobje/services/Session`.

    Voorbeeld: `http://BI4:8080/dswsbobje/services/Session`.
12. Voer de CMS-hostnaam in.
13. Wijzig het verificatietype naar *Windows AD*.
14. Selecteer *Windows Active Directory Single Sign On activeren*.
15. Bij de aanmeldingsaanwijzing laat u de velden *Gebruiker* en *Wachtwoord* leeg en klikt u op *OK*.

9.4.6.2.6 Eenmalige aanmelding van Vintela inschakelen voor RESTful-webservices

Sommige clienthulpprogramma's vereisen verificatie via RESTful-webservices. Volg deze stappen om eenmalige aanmelding voor webservices te activeren.

1. Kopieer het bestand `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\biprws.properties` naar `<INSTALLATIEMAP>\SAP`

`BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` en open het om het te bewerken.

2. Als u Kerberos SSO wilt inschakelen voor Windows Active Directory-verificatie (secWinAD), stelt u `sso.enabled` in op `true`. Zie de onderstaande schermafbeelding:

```
# ------------------------------------------------------ SSO Related Default Global Core Web Properties ------------------------------------------------------
# Vintela single sign on properties
sso.enabled=
idm.realm=
idm.princ=
idm.keytab=
idm.allowUnsecured=
idm.allowNTLM=
idm.logger.name=
idm.logger.props=
```

   Geef de volgende verplichte opties op:

   - `idm.realm` (hetzelfde als de default_realm die is opgegeven in het bestand Krb5.ini).
   - `idm.princ` (hetzelfde als opgegeven voor idm.princ in het bestand global.properties dat zich bevindt in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - `idm.keytab` (hetzelfde als opgegeven voor idm.keytab in het bestand global.properties dat zich bevindt in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - De parameter `idm.allowUnsecured` moet worden ingesteld op `true` als SSL niet wordt gebruikt met de Java-toepassingsserver. Voor meer informatie over Tomcat SSL raadpleegt u *Knowledge Base-artikel-id:1484802*.

3. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.
4. Start Tomcat opnieuw.
5. Als u uw instellingen wilt testen op de clientmachine opent u een willekeurige browser en opent u de URL: http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso.
   Het REST-token moet worden weergegeven als reactie op de API.

9.4.6.2.7 De maximale koptekstgrootte voor Tomcat verhogen

In Active Directory wordt een Kerberos-token gemaakt die wordt gebruikt in het verificatieproces. Deze token wordt opgeslagen in de HTTP-header. De Java-toepassingsserver heeft een standaard HTTP-headergrootte. Let erop dat de minimale standaardgrootte 16384 bytes is, zodat fouten worden voorkomen. (Bepaalde implementaties vereisen mogelijk een hogere waarde. Zie de Microsoft-richtlijnen hierover op de ondersteuningswebsite http://support.microsoft.com/kb/327825 voor meer informatie.)

1. Open het bestand `Server.xml` op de server waarop Tomcat is geïnstalleerd.

   In Windows bevindt dit bestand zich in `<Tomcat-installatiemap>/conf`.

   - Als u de versie van Tomcat gebruikt die bij het BI-platform is geïnstalleerd in Windows en de standaardinstallatielocatie niet hebt gewijzigd,
     vervangt u `<TomcatINSTALLATIEMAP>` door `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\`.
   - Als u een andere ondersteunde webtoepassingsserver gebruikt, raadpleegt u de documentatie bij uw webtoepassingsserver om het juiste pad te bepalen.

2. Zoek naar de bijbehorende code `<Connector …>` voor het poortnummer dat u hebt geconfigureerd.

   Als u de standaardpoort 8080 gebruikt, zoekt u de code `<Connector …>` met poort="8080".

   Bijvoorbeeld:

```
<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. Voeg de volgende waarde toe aan de code `<Connector …>`:

   `maxHttpHeaderSize="16384"`

   Bijvoorbeeld:

```
<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. Sla het bestand `Server.xml` op en sluit het.
5. Start Tomcat opnieuw.

> **Opmerking**
>
> Raadpleeg de documentatie bij de Java-toepassingsserver voor andere Java-toepassingsservers.

9.4.6.2.8 Internet-browsers configureren

U moet BI-platformclients configureren voor ondersteuning van Vintela SSO voor AD Kerberos-verificatie. Hiervoor moet de webbrowser op de clientcomputers worden geconfigureerd.

9.4.6.2.8.1 IE-browser configureren op de clientcomputers

1. Open een IE-browser op de clientcomputer.
2. Schakel geïntegreerde Windows-verificatie in.
   a. Klik in het menu *Extra* op *Internet-opties*.
   b. Klik op het tabblad *Geavanceerd*.
   c. Ga naar *Beveiliging*, selecteer *Geïntegreerde Windows-verificatie inschakelen* en klik op *Toepassen*.
3. Voeg de Java-toepassingsserver of de URL toe aan de vertrouwde sites. U kunt de volledige domeinnaam van de website invoeren.
   a. Klik in het menu *Extra* op *Internet-opties*.
   b. Klik op de tab *Beveiliging*.

c. Klik op *Sites* en klik op *Geavanceerd*.
d. Selecteer of voer de site in en klik op *Toevoegen*.
e. Klik op *OK* totdat het dialoogvenster Internetopties wordt gesloten.

4. Sluit het IE-browservenster en open dit opnieuw, zodat de wijzigingen worden doorgevoerd.
5. Herhaal deze stappen op elke clientcomputer met BI-platform.

9.4.6.2.8.2 Firefox configureren op de clientcomputers

1. *network.negotiate-auth.delegation-uris wijzigen*
   a. Open een Firefox-browser op de clientcomputer.
   b. Typ **`about:config`** in het URL-adresveld.
   Er wordt een lijst met eigenschappen weergegeven die u kunt configureren.
   c. Dubbelklik op *network.negotiate-auth.delegation-uris* om de eigenschap te bewerken.
   d. Voer de URL in die u wilt gebruiken voor toegang tot uw BI-startpunt.

   Als de URL voor uw BI-startpunt bijvoorbeeld **`http://<computer.domein.com>:8080/BOE/BI`** is, moet u **`http://<computer.domein.com>`** invoeren.

   > ⓘ Opmerking
   >
   > Als u meerdere URL's wilt toevoegen, scheidt u deze met een komma, bijvoorbeeld: **`http://<computer.domein.com>,<computer2.domein.com>`**.

   e. Klik op *OK*.
2. *network.negotiate-auth.trusted-uris wijzigen*
   a. Open een Firefox-browser op de clientcomputer.
   b. Typ **`about:config`** in het URL-adresveld.
   Er wordt een lijst met eigenschappen weergegeven die u kunt configureren.
   c. Dubbelklik op *network.negotiate-auth.trusted-uris* om de eigenschap te bewerken.
   d. Voer de URL in die u wilt gebruiken voor toegang tot uw BI-startpunt.
   Als de URL voor uw BI-startpunt bijvoorbeeld **`http://<computer.domein.com>:8080/BOE/BI`** is, moet u **`http://<computer.domein.com>`** invoeren.

   > ⓘ Opmerking
   >
   > Als u meerdere URL's wilt toevoegen, scheidt u deze met een komma, bijvoorbeeld: **`http://<computer.domein.com>,<computer2.domein.com>`**.

   e. Klik op *OK*.
3. Sluit het Firefox-browservenster en open dit opnieuw, zodat de wijzigingen worden doorgevoerd.
4. Herhaal deze stappen op elke clientcomputer met BI-platform.

9.4.6.2.9 Vintela SSO testen voor AD Kerberos-verificatie

U moet uw SSO-set-up testen vanaf een clientwerkstation. Zorg dat de client zich op hetzelfde domein bevindt als uw BI-platformimplementatie, en dat u als toegewezen AD-gebruiker bij het werkstation bent aangemeld. Deze gebruikersaccount moet handmatig bij BI-startpunt kunnen worden aangemeld.

Als u SSO wilt testen, opent u een browser en voert u de URL voor BI-startpunt in. Als SSO goed is geconfigureerd, moet u niet om uw aanmeldingsreferenties worden gevraagd.

> → Tip
>
> Het is raadzaam om verschillende AD-gebruikersscenario's in uw implementatie te testen. Als uw omgeving bijvoorbeeld gebruikers van verschillende besturingssystemen heeft, moet u SSO voor gebruikers van elk besturingssysteem testen. U moet SSO ook testen op alle mogelijke browsers die in uw organisatie worden ondersteund. Als uw omgeving gebruikers van meerdere forests of domeinen heeft, moet u SSO testen voor een gebruikersaccount van elk domein of elke forest.

9.4.6.2.10 Kerberos en eenmalige aanmelding bij de database configureren voor toepassingsservers

Eenmalige aanmelding bij de database wordt ondersteund voor implementaties die aan alle volgende vereisten voldoen:

- Het BI-platform wordt geïmplementeerd op een webtoepassingsserver.
- De webtoepassingsserver is geconfigureerd voor Vintela SSO voor AD-verificatie.
- De database waarvoor SSO is vereist, is een ondersteunde versie van SQL Server of Oracle.
- Aan de groepen of gebruikers die toegang tot de database moeten hebben, moeten machtigingen zijn toegewezen in SQL Server of Oracle.

De laatste stap is het wijzigen van het bestand `krb5.ini` voor de ondersteuning van SSO bij de database voor webtoepassingen.

9.4.6.2.10.1 Eenmalige aanmelding bij de database configureren voor Java-toepassingsservers

1. Open het bestand `krb5.ini` dat wordt gebruikt voor de implementatie van het BI-platform.

   De standaardlocatie van dit bestand is de map WIN op de webtoepassingsserver.

   > ⓘ Opmerking
   >
   > Als u het bestand niet kunt vinden in de map WIN, kunt u de locatie van het bestand vinden in het volgende Java-argument:
   >
   > ```
   > -Djava.security.auth.login.config
   > ```

> Deze variabele wordt opgegeven tijdens de configuratie van AD met Kerberos op uw webtoepassingsserver.

2. Ga naar de sectie `[libdefaults]` van het bestand.
3. Voer de volgende tekenreeks in vóór het begin van de sectie `[realms]` van het bestand:

```
forwardable=true
```

4. Sla het bestand op en sluit het.
5. Start de webtoepassingsserver opnieuw op.

Eenmalige aanmelding bij de database wordt ingeschakeld wanneer u het selectievakje *Beveiligingscontext in cache (vereist voor eenmalige aanmelding bij database)* op de Windows AD-verificatiepagina in de CMC inschakelt.

9.4.6.3 SiteMinder gebruiken

9.4.6.3.1 Windows AD met SiteMinder gebruiken

In deze sectie wordt uitgelegd hoe u AD en SiteMinder gebruikt. SiteMinder is een toegangs- en verificatiehulpprogramma van derden dat u kunt gebruiken met de AD-beveiligingsinvoegtoepassing om eenmalige aanmelding in te stellen voor het BI-platform. U kunt SiteMinder gebruiken met Kerberos.

Zorg dat uw SiteMinder-identiteitsbeheerbronnen zijn geïnstalleerd en geconfigureerd voordat u Windows AD-verificatie configureert om met SiteMinder te werken. Zie de documentatie voor SiteMinder voor meer informatie over SiteMinder en de installatie ervan.

U moet twee taken uitvoeren om eenmalige AD-aanmelding met SiteMinder in te schakelen:

- De AD-invoegtoepassing voor eenmalige aanmelding configureren met SiteMinder
- SiteMinder-eigenschappen configureren voor de BOE-webtoepassing

> ⓘ Opmerking
>
> Controleer of de SiteMinder-beheerder ondersteuning voor 4.x-agenten heeft ingeschakeld. Dit is vereist ongeacht de ondersteunde versie van SiteMinder die u gebruikt. Zie de SiteMinder-documentatie voor meer informatie over SiteMinder-configuratie.

9.4.6.3.1.1 SiteMinder-eigenschappen voor BI-startpunt instellen

Naast de SiteMinder-instellingen voor de Windows AD-beveiligingsinvoegtoepassing moeten de SiteMinder-instellingen voor de BOE WAR-eigenschappen worden opgegeven.

1. Zoek de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` in uw BI-platforminstallatie.

2. Gebruik Kladblok of een andere teksteditor om een nieuw bestand te maken in deze map.
3. Voeg de volgende waarden toe aan het nieuwe bestand:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Sla het bestand op met de naam `global.properties`.

> ⓘ Opmerking
>
> Zorg ervoor dat de bestandsnaam niet wordt opgeslagen met een extensie, bijvoorbeeld `.txt`.

5. Maak nog een bestand in dezelfde map.
6. Voeg de volgende waarden toe aan het nieuwe bestand:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

Bijvoorbeeld:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Sla het bestand op met de naam `BIlaunchpad.properties` en sluit het bestand.

De nieuwe eigenschappen worden van kracht nadat BOE.war opnieuw is geïmplementeerd op de computer waarop de webtoepassingsserver wordt uitgevoerd. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.

9.4.6.3.1.2 SiteMinder-instellingen configureren in de CMC

Voordat u de CMC voor SiteMinder configureert, moet u de volgende voorbereidingen treffen:

- U hebt AD-gebruikersgroepen toegewezen in het BI-platform.
- U hebt AD-referenties op de CCM getest.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Windows AD*.
3. Schakel het selectievakje *Windows Active Directory (AD) inschakelen* in.
4. Selecteer bij Verificatieopties de optie *NTLM-verificatie gebruiken* of *Kerberos-verificatie gebruiken*.

   Als u het BI-platform wilt configureren voor Kerberos- en AD-verificatie met Kerberos, hebt u een serviceaccount nodig. U kunt een nieuwe domeinaccount maken of een bestaande domeinaccount gebruiken. De serviceaccount wordt gebruikt om BI-platformservers uit te voeren.

   > → Tip
   >
   > Gebruikers van andere domeinen die zich handmatig bij het BI-startpunt aanmelden, moeten de domeinnaam in hoofdletters na hun gebruikersnaam opgeven. In `gebruiker@ONDERLIGGEND.BOVENLIGGENDDOMEIN.COM` is “ONDERLIGGEND.BOVENLIGGENDDOMEIN.COM” het domein.

5. Ga als volgt te werk als u *Kerberos-verificatie gebruiken* hebt geselecteerd:
   a. Als u eenmalige aanmelding bij een database wilt configureren, selecteert u *Beveiligingscontext in cache*.
   b. Verwijder informatie uit het vakje *Naam van service-principal*.
6. Als u eenmalige aanmelding wilt configureren, schakelt u *Eenmalige aanmelding inschakelen voor geselecteerde verificatiemodus* in.

   U moet ook de algemene eigenschappen van de BOE-webtoepassing en de eigenschappen van BI-startpunt configureren om eenmalige aanmelding in te schakelen.
7. Selecteer een optie in het gebied *Synchronisatie van referenties* en werk de gegevensbronreferenties van de AD-gebruiker bij de aanmelding bij.

   Hiermee wordt de gegevensbron gesynchroniseerd met de huidige aanmeldingsreferenties van de gebruiker.
8. Gebruik het gebied *SiteMinder-opties* om SiteMinder te configureren als uw eenmalige aanmelding voor AD-verificatie met Kerberos:
   a. Klik op *Uitgeschakeld.*

      De pagina *Windows Active Directory* wordt weergegeven.

      Als u de Windows AD-invoegtoepassing niet hebt geconfigureerd, wordt een waarschuwing weergegeven en wordt u gevraagd of u wilt doorgaan. Klik op *OK*.
   b. Klik op *Eenmalige aanmelding van SiteMinder gebruiken*.
   c. Typ de naam van elke beleidsserver in het vak *Beleidsserverhost* en klik op *Toevoegen*.
   d. Voor elke beleidsserverhost voert u een poortnummer in de vakjes *Accounting*, *Verificatie* en *Autorisatie* in.
   e. Voer de naam van de agent in het vakje *Naam van agent* in.
   f. Voer het gedeelde geheim in de vakjes *Gedeeld geheim* in.

      Zorg dat de SiteMinder-beheerder ondersteuning voor 4.x Agents heeft ingeschakeld, ongeacht welke ondersteunde versie van SiteMinder u gebruikt. Zie de documentatie van SiteMinder voor meer informatie over SiteMinder en de installatie hiervan.
   g. Klik op *Bijwerken* om op te slaan en naar de hoofdpagina van AD-verificatie terug te keren.
9. Geef in het gebied *Opties voor AD-alias* op hoe nieuwe aliassen worden toegevoegd aan en bijgewerkt in het BI-platform.
   a. Selecteer in de lijst *Opties voor nieuwe alias* een optie voor het toewijzen van nieuwe aliassen aan Enterprise-accounts:
      - *Elke nieuwe AD-alias toewijzen aan een bestaande gebruikersaccount met dezelfde naam*
        Selecteer deze optie wanneer u weet dat gebruikers een bestaande Enterprise-account met dezelfde naam hebben. De AD-aliassen worden dus toegewezen aan bestaande gebruikers (de aliassen worden automatisch gemaakt). Gebruikers die geen bestaande Enterprise-account hebben of die niet dezelfde naam gebruiken in de Enterprise- en AD-account, worden toegevoegd als nieuwe gebruikers.
      - *Een nieuwe gebruikersaccount maken voor elke nieuwe AD-alias*
        Selecteer deze optie wanneer u voor elke gebruiker een nieuwe account wilt maken.
   b. Selecteer in het gebied *Bijwerkopties van alias* een optie voor het beheren van aliasupdates voor Enterprise-accounts:
      - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
        Gebruik deze optie als u automatisch een nieuwe alias wilt maken voor iedere AD-gebruiker die is toegewezen aan het BI-platform. Nieuwe AD-accounts worden toegevoegd voor gebruikers zonder

BI-platformaccounts, of voor alle gebruikers als u de optie *Een nieuwe gebruikersaccount maken voor elke nieuwe AD-alias* hebt ingeschakeld en op *Bijwerken* hebt geklikt.

- *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
  Selecteer deze optie wanneer de AD-map die u toewijst, veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van het BI-platform. Het platform maakt niet automatisch aliassen en Enterprise-accounts voor alle gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers die zich aanmelden bij het BI-platform.

c. Selecteer een nieuwe optie in het gebied *Opties voor nieuwe gebruiker* een optie voor het maken van nieuwe gebruikers:

- *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van een gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem, ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

  > **Opmerking**
  >
  > Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
  >
  > Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het systeem, kan een licentie voor gelijktijdige toegang van 100 gebruikers bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

10. Klik op *Planning* als u wilt configureren hoe u updates van AD-aliassen wilt plannen.
    a. Selecteer in het dialoogvenster *Planning* een terugkeerpatroon in de lijst *Object uitvoeren*.
    b. Stel de overige opties en parameters voor de planning naar wens in.
    c. Klik op *Planning*.
    Wanneer de aliassen worden bijgewerkt, worden de groepsgegevens ook bijgewerkt.
11. In het gebied *Opties voor attribuutbinding* kunt u de prioriteit voor attribuutbinding voor de AD-invoegtoepassing opgeven:
    a. Schakel het selectievakje *Volledige naam, e-mailadres en andere attributen importeren* in.
    De volledige namen en beschrijvingen die worden gebruikt in de AD-accounts, worden met gebruikersobjecten geïmporteerd en opgeslagen in het BI-platform.
    b. Geef een optie op voor *Prioriteit van AD-attribuutbinding instellen in verhouding tot andere attribuutbindingen*.

    Als u de optie instelt op 1, hebben AD-attributen prioriteit in scenario's waarbij AD en andere invoegtoepassingen (LDAP en SAP) zijn ingeschakeld. Is de optie op 3 ingesteld, dan hebben attributen

van andere ingeschakelde invoegtoepassingen prioriteit. De bindingen moeten op verschillende waarden worden ingesteld. Als meerdere verificatie-invoegtoepassingen op dezelfde bindingwaarde worden ingesteld, kan dit onverwachte gevolgen hebben.

12. Configureer updates van AD-groepen in het gebied *Opties voor AD-groepen*:
    a. Klik op *Planning*.
    Het dialoogvenster *Planning* wordt weergegeven.
    b. Selecteer een terugkeerpatroon in de lijst *Object uitvoeren*.
    c. Stel de overige planningsopties en parameters naar wens in.
    d. Klik op *Planning*.

    De update wordt gepland en uitgevoerd op basis van de opgegeven planningsgegevens. De volgende geplande update voor de AD-groepsaccounts wordt weergegeven onder de *Opties voor AD-groepen*.
13. Selecteer in het gebied *AD-update op aanvraag* een optie om aan te geven of AD-groepen of AD-gebruikers moeten worden bijgewerkt (of geen van beide) wanneer u op *Bijwerken* klikt:
    - *AD-groepen nu bijwerken*
      Selecteer deze optie als u alle geplande AD-groepen wilt bijwerken wanneer u op *Bijwerken* klikt. De volgende geplande update van AD-groepen wordt weergegeven onder *Opties voor AD-groepen*.
    - *AD-groepen en -aliassen nu bijwerken*
      Selecteer deze optie als u alle geplande AD-groepen en -gebruikersaliassen wilt bijwerken wanneer u op *Bijwerken* klikt. De volgende geplande updates worden weergegeven onder *Opties voor AD-groepen* en *Opties voor AD-alias*.
    - *AD-groepen en -aliassen nu niet bijwerken*
      Er worden geen AD-groepen of -gebruikersaliassen bijgewerkt wanneer u op *Bijwerken* klikt.
14. Klik op *Bijwerken* en klik vervolgens op *OK*.

9.4.6.3.1.3 SiteMinder uitschakelen

Als u wilt voorkomen dat SiteMinder wordt geconfigureerd of als u SiteMinder wilt uitschakelen nadat deze in de CMC is geconfigureerd, wijzigt u het webconfiguratiebestand voor BI-startpunt.

9.4.6.3.1.3.1 SiteMinder uitschakelen voor Java-clients

De SiteMinder-instellingen moeten uitgeschakeld worden voor de Windows AD-beveiligingsinvoegtoepassing, evenals voor het BOE WAR-bestand op uw webtoepassingsserver.

1. Ga naar de volgende map in uw installatie van BI-platform:
   `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Open het bestand `global.properties`.
3. Stel `siteminder.enabled` in op False.

```
siteminder.enabled=false
```

4. Sla de wijzigingen op en sluit het bestand.

De wijziging wordt pas van kracht nadat `BOE.war` opnieuw is geïmplementeerd op de computer waarop de webtoepassingsserver wordt uitgevoerd. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.

9.4.7 Problemen met de Windows AD-verificatie oplossen

9.4.7.1 Problemen met uw configuratie oplossen

Deze stappen kunnen u helpen bij het oplossen van problemen met de configuratie van Kerberos:

- De logboekfunctie inschakelen
- De Java SDK Kerberos-configuratie testen

9.4.7.1.1 De logboekfunctie inschakelen

1. Selecteer in het menu *Start* achtereenvolgens *Programma's >Tomcat > Tomcat-configuratie*.
2. Klik op het tabblad *Java*.
3. Voeg de volgende opties toe:

   ```
   -Dcrystal.enterprise.trace.configuration=verbose
   -sun.security.krb5.debug=true
   ```

   Er wordt een logboekbestand gemaakt op de volgende locatie:

   ```
   C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
   ```

9.4.7.1.2 De Kerberos-configuratie testen

Voer de volgende opdracht uit om de Kerberos-configuratie te testen, waarbij `servant` de naam is van de serviceaccount en het domein van de CMS, en `wachtwoord` het wachtwoord van de serviceaccount.

```
<Installatiemap>\SAP BusinessObjects Enterprise XI
4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

Bijvoorbeeld:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

De namen van uw domein en service-principal moeten exact overeenkomen met de namen van het domein en de service-principal in Active Directory. Als het probleem zich blijft voordoen, controleert u of u dezelfde naam hebt opgegeven. Let erop dat de naam hoofdlettergevoelig is.

9.4.7.1.3 Aanmeldingsfout vanwege verschillende UPN- en SAM-namen in AD

De Active Directory-id van een gebruiker is toegewezen aan het BI-platform. Desondanks kan de gebruiker zich niet aanmelden bij CMC of BI-startpunt met Windows Active Directory-verificatie en Kerberos met de volgende notatie: `DOMEIN\ABC123`

Dit probleem kan zich voordoen als de gebruiker in Active Directory is ingesteld met een UPN- en SAM-naam die niet gelijk aan elkaar zijn. De volgende voorbeelden kunnen een probleem veroorzaken:

- De UPN is abc123@bedrijf.com, maar de SAM-naam is DOMEIN\ABC123.
- De UPN is jsmit@bedrijf, maar de SAM-naam is DOMEIN\jansmit.

U kunt dit probleem op twee manieren oplossen:

- Laat gebruikers zich aanmelden met UPN-naam in plaats van de SAM-naam.
- Zorg ervoor dat de SAM-accountnaam en de UPN-naam hetzelfde zijn.

9.4.7.1.4 Fout vóór de verificatie

Een gebruiker die zich eerder wel kon aanmelden, kan zich nu niet meer aanmelden. De volgende fout wordt weergegeven: Accountgegevens worden niet herkend. In de Tomcat-foutlogboeken wordt de volgende fout aangegeven: `Pre-authentication information was invalid (24)`.

Dit kan optreden wanneer de Kerberos-gebruiker geen wijziging heeft aangebracht in UPN in AD. Dit houdt mogelijk in dat de Kerberos-gebruikersdatabase en de AD-gegevens niet zijn gesynchroniseerd.

Stel het wachtwoord van de gebruiker opnieuw in AD in om dit probleem op te lossen. Hierdoor worden de wijzigingen correct doorgevoerd.

> **Opmerking**
>
> dit probleem treedt niet op bij J2SE 5.0.

9.5 SAP-verificatie

9.5.1 SAP-verificatie configureren

In deze sectie wordt uitgelegd hoe u BI-platformverificatie configureert voor uw SAP-omgeving.

Met SAP-verificatie kunnen SAP-gebruikers zich bij het BI-platform aanmelden met hun SAP-gebruikersnaam en -wachtwoord, zonder dit wachtwoord op te slaan in het BI-platform. Met SAP-verificatie kunt u ook gegevens bewaren over gebruikersrollen in SAP en deze rolgegevens gebruiken in het platform voor het toewijzen van rechten om beheertaken uit te voeren of toegang te krijgen tot inhoud.

De SAP-verificatietoepassing openen

U moet informatie over uw SAP-systeem toevoegen aan het BI-platform. U kunt een aparte webtoepassing openen via het hoofdbeheerprogramma van het BI-platform, de CMC (Central Management Console). Klik op *Verificatie* om vanaf de startpagina van de CMC deze toepassing te openen.

SAP-gebruikers verifiëren

Met beveiligingsinvoegtoepassingen kunt u de manier waarop het BI-platform gebruikers verifieert, uitbreiden en aanpassen. De functie SAP-verificatie bevat een SAP-beveiligingsinvoegtoepassing (`secSAPR3.dll`) voor het CMS-onderdeel (Central Management Server) van het BI-platform. Deze SAP-beveiligingsinvoegtoepassing heeft een aantal belangrijke voordelen:

- De functie fungeert als een verificatieprovider die gebruikersreferenties namens de CMS controleert in het SAP-systeem. Wanneer gebruikers zich rechtstreeks bij het BI-platform aanmelden, kunnen ze SAP-verificatie kiezen en hun gewone SAP-gebruikersnaam en -wachtwoord opgeven. Het BI-platform kan tevens Enterprise Portal-aanmeldingstickets valideren voor SAP-systemen.
- De invoegtoepassing vergemakkelijkt het maken van accounts door u de mogelijkheid te geven functies uit SAP toe te wijzen aan gebruikersgroepen in BI-platform, en vergemakkelijkt het accountbeheer doordat u in het BI-platform op consistente wijze rechten kunt toekennen aan gebruikers en groepen.
- Het programma onderhoudt op dynamische wijze de lijsten van SAP-functies. Wanneer u een SAP-functie hebt toegewezen aan BI-platform, kunnen alle gebruikers die tot die functie behoren zich aanmelden bij BI-platform. Wanneer u daarna wijzigingen aanbrengt in het lidmaatschap van de SAP-functie, hoeft u de lijst in het BI-platform niet bij te werken of te vernieuwen.
- Het onderdeel SAP-verificatie bevat een webtoepassing om de invoegtoepassing te configureren. U hebt toegang tot deze toepassing in het gebied *Verificatie* van de CMC (Central Management Console).

9.5.2 Gebruikersaccounts maken voor het BI-platform

Het BI-platformsysteem vereist een SAP-gebruikersaccount met het recht op lijsten met SAP-functielidmaatschap te openen en SAP-gebruikers te verifiëren. U hebt deze accountreferenties nodig om het BI-platform te verbinden met uw SAP-systeem. Raadpleeg de SAP BW-documentatie voor algemene instructies over het maken van SAP-gebruikersaccounts en voor het toewijzen van machtigingen via functies.

Gebruik transactie `SU01` om een nieuwe SAP-gebruikersaccount te maken met de naam `CRYSTAL`. Gebruik transactie `PFCG` om een nieuwe functie te maken met de naam `CRYSTAL_ENTITLEMENT`. (Deze namen worden

aanbevolen maar zijn niet verplicht.) Wijzig de machtiging van de nieuwe rol door waarden in te stellen voor de volgende machtigingsobjecten:

Machtigingsobject	Veld	Waarde
Machtiging voor bestandstoegang (S_DATASET)	Activiteit (ACTVT)	Lezen, Schrijven (33, 34)
	Fysieke bestandsnaam (FILENAME)	* (geeft Alle aan)
	ABAP-programmanaam (PROGRAM)	*
Machtigingscontrole op RFC-toegang (S_RFC)	Activiteit (ACTVT)	16
	Naam van RFC die moet worden beveiligd (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Type RFC-object dat moet worden beveiligd (RFC_TYPE)	Functiegroep (FUGR)
Onderhoud basisgegevens gebruiker: Gebruikersgroepen (S_USER_GRP)	Activiteit (ACTVT)	Maken of genereren, en weergeven (03)
	Gebruikersgroep in onderhoud basisgegevens gebruiker (CLASS)	* **Opmerking** Mogelijk geeft u voor een betere beveiliging liever expliciet een overzicht weer van de gebruikersgroepen waarvan de leden toegang nodig hebben tot het BI-platform.

Voeg ten slotte de `CRYSTAL`-gebruiker aan de rol `CRYSTAL_ENTITLEMENT` toe.

→ Tip

Als gebruikers volgens het systeembeleid hun wachtwoord moeten wijzigen wanneer zij zich voor het eerst bij het systeem aanmelden, meldt u zich nu aan met de `CRYSTAL`-gebruikersaccount en stelt u het bijbehorende wachtwoord opnieuw in.

Opmerking

Mogelijk zijn aanvullende machtigingen voor het S_RFC-object vereist als bepaalde prestatieverbeteringen zijn ingeschakeld in de ABAP-omgeving. Deze fouten worden gemeld op de pagina Rol importeren, waarbij de functie wordt vermeld waarvoor de machtiging is mislukt:

Voorbeeld: Geen RFC-machtiging voor functiemodule RFC_METADATA_GET.

Machtigingsobject	Veld	Waarde
Machtigingscontrole op RFC-toegang (S_RFC)	Activiteit (ACTVT)	16
	Naam van RFC die moet worden beveiligd (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY en RFC_METADATA
	Type RFC-object dat moet worden beveiligd (RFC_TYPE)	Functiegroep (FUGR)

9.5.3 Verbinding maken met SAP-machtigingssystemen

Voordat u rollen kunt importeren of BW-inhoud kunt publiceren naar het BI-platform, moet u informatie opgeven over de SAP-machtigingssystemen waarmee u wilt integreren. Het BI-platform gebruikt deze informatie om een verbinding met het SAP-doelsysteem te maken wanneer rollidmaatschappen worden vastgesteld en SAP-gebruikers worden geverifieerd.

9.5.3.1 Een SAP-machtigingssysteem toevoegen

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP*.

   De instellingen van de machtigingssystemen worden weergegeven.

   > → Tip
   >
   > Als er al een machtigingssysteem in de lijst *Logische systeemnaam* wordt weergegeven, klikt u op *Nieuw*.

3. Typ in het veld *Systeem* de systeem-id (SID) van drie tekens voor het SAP-systeem.
4. Typ in het veld *Client* het clientnummer dat het BI-platform moet gebruiken voor de aanmelding bij uw SAP-systeem.
   Het BI-platform combineert uw Systeem- en Client-gegevens, en voegt een vermelding aan de lijst *Logical System-naam* toe.
5. Controleer of het selectievakje *Uitgeschakeld* leeg is.

   > ⓘ Opmerking
   >
   > Gebruik het selectievakje *Uitgeschakeld* om het BI-platform te laten weten dat een bepaald SAP-systeem tijdelijk niet beschikbaar is.

6. Vul de velden *Berichtenserver* en *Aanmeldingsgroep* in, als u taakverdeling zo hebt ingesteld dat het BI-platform via een berichtenserver moet inloggen.

> **Opmerking**
>
> Voeg de juiste vermeldingen toe aan het bestand `Services` op uw BI-platformcomputer om taakverdeling in te schakelen, vooral als uw implementatie meerdere machines betreft. U moet specifiek de computers opnemen die de CMS, de webtoepassingsserver hosten, evenals alle computers die uw verificatie-accounts en -instellingen beheren.

7. Als u geen taakverdeling hebt ingesteld (of als u liever wilt dat de aanmelding van het BI-platform rechtstreeks bij het SAP-systeem plaatsvindt), vult u de velden *Toepassingsserver* en *Systeemnummer* toepasselijk in.
8. Typ in de velden *Gebruikersnaam*, *Wachtwoord* en *Taal* de gebruikersnaam, het wachtwoord en de taalcode voor de SAP-account die u wilt gebruiken wanneer het BI-platform aangemeld wordt bij SAP.

> **Opmerking**
>
> Deze referenties moeten overeenkomen met de gebruikersaccount die u hebt gemaakt voor het BI-platform.

9. Klik op *Bijwerken*.

Als u meerdere machtigingssystemen toevoegt, klikt u op het tabblad *Opties* om het systeem op te geven dat het BI-platform als standaard gebruikt (dat wil zeggen: het systeem waarmee contact wordt gemaakt om gebruikers te verifiëren die zich proberen aan te melden met SAP-referenties maar geen specifiek SAP-systeem opgeven).

9.5.3.2 Controleren of uw machtigingssysteem correct is toegevoegd

1. Klik op het tabblad *Rol importeren*.
2. Selecteer de naam van het machtigingssysteem in de lijst *Logical System-name*.

   Als het machtigingssysteem correct is toegevoegd, bevat de lijst *Beschikbare rollen* een lijst met functies die u kunt kiezen om te importeren.

> **→ Tip**
>
> Als er geen rollen zichtbaar zijn in de lijst *Logical System-name*, kijk dan of er foutberichten op de pagina staan. De foutberichten geven u mogelijk de informatie die u nodig hebt om het probleem op te lossen.

9.5.3.3 Verbinding met een SAP-machtigingssysteem tijdelijk uitschakelen

In de CMC kunt u tijdelijk een verbinding tussen het BI-platform en een SAP-machtigingssysteem uitschakelen. Dit kan handig zijn om het reactievermogen van BI-platform te behouden in gevallen zoals de geplande inactiviteit van een SAP-machtigingssysteem.

1. Ga in de CMC naar het beheergebied *Verificatie*.
2. Dubbelklik op de koppeling *SAP*.
3. Selecteer in de lijst *Logische systeemnaam* het systeem dat u wilt uitschakelen.
4. Schakel het selectievakje *Uitgeschakeld* in.
5. Klik op *Bijwerken*.

9.5.4 Opties voor SAP-verificatie instellen

SAP-verificatie omvat een aantal opties die u kunt aanpassen wanneer u het BI-platform integreert met uw SAP-systeem. U kunt onder andere de volgende opties wijzigen:

- SAP-verificatie in- of uitschakelen
- Verbindingsinstellingen opgeven
- Geïmporteerde gebruikers koppelen aan BI-platformlicentiemodellen
- Eenmalige aanmelding bij het SAP-systeem configureren

9.5.4.1 Opties voor SAP-verificatie instellen

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP* en klik op het tabblad *Opties*.
3. Evalueer en wijzig de volgende instellingen waar nodig:

Instelling	Beschrijving
SAP-verificatie inschakelen	Schakel dit selectievakje uit om SAP-verificatie uit te schakelen. **Opmerking** Als u SAP-verificatie voor een specifiek SAP-systeem wilt uitschakelen, schakelt u het selectievakje *Uitgeschakeld* voor dat systeem uit op het tabblad *Machtigingssystemen*.
Hoofdinhoudsmap	Geef op vanwaaruit het BI-platform het dupliceren van de BW-mappenstructuur in de CMC en het BI-startpunt moet beginnen. De standaardinstelling is `/SAP/2.0`, maar u kunt desgewenst een andere map opgeven. Als u de waarde wilt wijzigen, moet u dit zowel in de CMC als de Workbench voor contentbeheer doen.
Standaardsysteem	Selecteer een SAP-machtigingssysteem waar het BI-platform contact mee moet opnemen om gebruikers

Instelling	Beschrijving
	te verifiëren die proberen zich aan te melden met SAP-referenties maar zonder een specifiek SAP-systeem op te geven. **Opmerking** Als u een standaardsysteem selecteert, hoeven gebruikers van dat systeem geen systeem-id of client op te geven wanneer zij verbinding maken vanuit clienthulpprogramma's als Live Office of Universe Designer met behulp van SAP-verificatie. Wanneer bijvoorbeeld SYS~100 wordt ingesteld als het standaardsysteem, kan bij keuze voor SAP/verificatie SYS~100/gebruiker1 zich aanmelden als gebruiker1.
Max. aantal mislukte pogingen om het machtigingssysteem te openen	Geef op hoe vaak het BI-platform opnieuw moet proberen contact te maken met een SAP-systeem om aan verificatieaanvragen te voldoen. Met een waarde van –1 kan het platform een onbeperkt aantal keren proberen contact te maken met het machtigingssysteem. Met een waarde van 0 kan het BI-platform slechts één keer proberen om contact te maken met het machtigingssysteem. **Opmerking** Gebruik deze instelling samen met *Machtigingssysteem uitgeschakeld houden [seconden]* om te configureren hoe het BI-platform omgaat met SAP-machtigingssystemen die tijdelijk niet beschikbaar zijn. Het systeem gebruikt deze twee opties om te bepalen wanneer de communicatie moet worden gestopt met een SAP-systeem dat niet beschikbaar is, en wanneer deze hervat moet worden.
Machtigingssysteem uitgeschakeld houden [seconden]	Voer in hoeveel seconden het BI-platform moet wachten voordat pogingen om gebruikers met het SAP-systeem te verifiëren, hervat worden. Als u bijvoorbeeld 3 opgeeft voor *Max. mislukte toegangspogingen tot machtigingssysteem*, staat het BI-platform maximaal drie mislukte pogingen toe om gebruikers te verifiëren met een bepaald SAP-systeem. Bij een vierde mislukte poging voorkomt het systeem gedurende de opgegeven periode dat geprobeerd wordt om gebruikers bij dat systeem te verifiëren.
Max. gelijktijdige verbindingen per systeem	Geef op hoeveel verbindingen u gelijktijdig geopend wilt houden op uw SAP-systeem.

Instelling	Beschrijving
	Als u bijvoorbeeld 2 invoert, houdt het BI-platform twee verbindingen met SAP geopend.
Aantal toepassingen per verbinding	Geef op hoeveel bewerkingen per verbinding bij het SAP-systeem zijn toegestaan. Als *Max. gelijktijdige verbindingen per systeem* bijvoorbeeld is ingesteld op 2 en *Aantal toepassingen per verbinding* op 3, wordt een verbinding met drie aanmeldingen door het BI-platform gesloten en opnieuw gestart.
Gelijktijdige gebruikers en *Benoemde gebruikers*	Geef op of nieuwe gebruikersaccounts gebruikerslicenties voor gelijktijdig gebruik of gebruikerslicenties op naam gebruiken. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een klein aantal licenties voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het systeem, kan een licentie voor gelijktijdige toegang van 100 gebruikers bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen. Gebruikerslicenties op naam horen bij gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. **Opmerking** Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden. Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

Instelling	Beschrijving
	Opmerking De optie die u selecteert, heeft geen invloed op het aantal of het type gebruikerslicenties dat u op het BI-platform hebt geïnstalleerd. U moet de juiste licenties beschikbaar hebben in uw systeem.
Volledige naam, e-mailadres en andere attributen importeren	Geef een prioriteitsniveau voor de SAP-invoegtoepassing voor verificatie op. De volledige namen en beschrijvingen die worden gebruikt in de SAP-accounts, worden met gebruikersobjecten geïmporteerd en opgeslagen in het BI-platform.
Prioriteit van SAP-attribuutbinding instellen in verhouding tot andere attribuutbindingen	Hiermee wordt een prioriteit opgegeven voor het binden van SAP-gebruikersattributen (volledige naam en e-mailadres). Als u de optie instelt op 1, hebben SAP-attributen prioriteit in scenario's waarbij SAP en andere invoegtoepassingen (Windows AD en LDAP) zijn ingeschakeld. Is de optie op 3 ingesteld, dan hebben attributen van andere ingeschakelde invoegtoepassingen prioriteit. De bindingen moeten op verschillende waarden worden ingesteld. Als meerdere verificatie-invoegtoepassingen op dezelfde bindingwaarde worden ingesteld, kan dit onverwachte gevolgen hebben.

Stel de volgende opties in om de SAP-service voor eenmalige aanmelding te configureren:

Instelling	Beschrijving
Systeem-id	De systeem-id die door het BI-platform aan het SAP-systeem gegeven wordt bij het uitvoeren van de SAP-service voor eenmalige aanmelding.
Bladeren	Klik om het `keystore`-bestand te uploaden dat is gegenereerd om de eenmalige aanmelding van SAP in te schakelen. U kunt ook handmatig het volledige pad naar het bestand invoeren.
Keystore-wachtwoord	Typ het wachtwoord dat vereist is om toegang te krijgen tot het `keystore`-bestand.
Wachtwoord voor privésleutel	Typ het wachtwoord dat vereist is om toegang te krijgen tot het certificaat dat overeenkomt met het `keystore`-bestand. Het certificaat bevindt zich op het SAP-systeem
Alias van privésleutel	Typ de alias die vereist is om toegang te krijgen tot het `keystore`-bestand.

4. Klik op *Bijwerken*.

9.5.4.2 De hoofdmap van inhoudsmap wijzigen

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP*.
3. Klik op *Opties* en typ de naam van de map in het veld *Hoofdmap van inhoudsmap*.

   De mapnaam die u hier typt, is de map vanwaaruit het BI-platform de herhaling van de BW-mappenstructuur moet beginnen.
4. Klik op *Bijwerken*.
5. Vouw in de BW-werkbank voor inhoudbeheer *Enterprise-systeem* uit.
6. Vouw *Beschikbare systemen* uit en dubbelklik op het systeem waarmee het BI-platform verbinding maakt.
7. Klik op het tabblad *Indeling* en typ in de *Inhoudsbasismap* de map die u wilt gebruiken als de SAP-hoofdmap in het BI-platform (bijvoorbeeld `/SAP/2.0./`).

9.5.5 SAP-rollen importeren

U kunt rolleden toestaan zich bij het systeem aan te melden zonder hun gebruikelijke SAP-referenties door SAP-rollen te importeren in het BI-platform. Bovendien wordt eenmalige aanmelding ingeschakeld zodat SAP-gebruikers automatisch bij het BI-platform worden aangemeld wanneer zij rapporten vanuit de SAP GUI of een SAP Enterprise Portal openen.

> **Opmerking**
>
> voor het inschakelen van SSO moet vaak aan een groot aantal vereisten worden voldaan. Dit kan onder andere het gebruik betreffen van een stuurprogramma en een toepassing waarvoor SSO is ingeschakeld en de voorwaarde dat uw server en webserver zich in hetzelfde domein bevinden.

Voor elke rol die u importeert, wordt in het BI-platform een groep gegenereerd. Voor elke groep wordt de volgende naamgevingsconventie gebruikt: **`<SystemID~ClientNumber@NameOfRole>`**. U kunt de nieuwe groepen weergeven in het beheergebied *Gebruikers en groepen* van de CMC. Met deze groepen kunt u ook objectbeveiliging definiëren in het BI-platform.

Neem drie hoofdcategorieën gebruikers in aanmerking bij het configureren van het BI-platform voor publicatie en bij het importeren van rollen in het systeem:

- BI-platformbeheerders
  Enterprise-beheerders configureren het systeem voor het publiceren van inhoud vanuit SAP. Zij importeren de juiste rollen, maken de benodigde mappen en wijzen rechten toe aan deze rollen en mappen in het BI-platform.
- Inhoudpublishers
  Inhoudpublishers zijn de gebruikers met rechten om inhoud naar functies te publiceren. Het doel van deze gebruikerscategorie is normale functieleden te scheiden van gebruikers met rechten om rapporten te publiceren.
- Functieleden
  Functieleden zijn gebruikers die behoren tot functies voor het “bewaren van inhoud”. Dat wil zeggen: deze gebruikers behoren tot functies waarnaar rapporten worden gepubliceerd. De gebruikers hebben de rechten *Weergeven*, *Weergeven op aanvraag* en *Plannen* voor alle rapporten die worden gepubliceerd naar

de functies waarvan zij lid zijn. Normale functieleden kunnen echter geen nieuwe inhoud en ook geen bijgewerkte versies van inhoud publiceren.

U moet alle rollen voor het publiceren van inhoud en voor het bewaren van inhoud naar het BI-platform importeren voordat u voor de eerste keer publiceert.

> **Opmerking**
>
> het wordt ten zeerste aanbevolen de activiteiten van functies gescheiden te houden. Het is bijvoorbeeld mogelijk vanuit een beheerdersfunctie te publiceren, maar het is beter alleen vanuit functies van inhoudpublishers te publiceren. Bovendien zijn functies voor het publiceren van inhoud alleen bedoeld om te bepalen welke gebruikers inhoud kunnen publiceren. Inhoudspublicatiefuncties moeten dus geen inhoud bevatten en inhoudpublishers moeten publiceren naar functies voor het bewaren van inhoud die toegankelijk zijn voor normale functieleden.

9.5.5.1 SAP-rollen importeren

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP*.
3. Selecteer op het tabblad *Opties* de optie *Gelijktijdige gebruikers* of *Benoemde gebruikers*, afhankelijk van uw licentieovereenkomst.

   Deze optie heeft geen invloed op het aantal of het type gebruikerslicenties dat u in BI-platform hebt geïnstalleerd. U moet de juiste licenties beschikbaar hebben in uw systeem.
4. Klik op *Bijwerken*.
5. Selecteer op het tabblad *Rol importeren* het juiste machtigingssysteem in de lijst *Logische systeemnaam*.
6. Selecteer in het gebied *Beschikbare rollen* de rol(len) die u wilt importeren, en klik op *Toevoegen*.
7. Klik op *Bijwerken*.

9.5.5.2 Controleren of functies en gebruikers juist zijn geïmporteerd

Voordat u deze taak begint, moet u een notitie maken van de gebruikersnaam en het wachtwoord van een SAP-gebruiker die tot een van de rollen behoort die u aan het BI-platform hebt toegewezen.

1. Voor Java BI-startpunt gaat u naar **`http://<webserver>:<poortnummer>/BOE/BI`**.

   Vervang `<webserver>` door de naam van de webserver en `<poortnummer>` door het poortnummer voor het BI-platform. Mogelijk moet u de beheerder vragen naar de naam van de webserver, het nummer van de poort of de exacte URL.
2. In de lijst *Verificatietype* selecteert u *SAP*.

   > **Opmerking**
   >
   > De lijst *Verificatietype* is standaard verborgen in BI-startpunt. Als de lijst niet zichtbaar is, vraagt u uw systeembeheerder om de lijst *Verificatietype* in het bestand `BIlaunchpad.properties` in te schakelen en de toepassingsserver opnieuw te starten.

3. Voer het SAP-syssteem en de systeemclient in waarbij u zich wilt aanmelden.
4. Voer de gebruikersnaam en het wachtwoord van een toegewezen gebruiker in.
5. Klik op *Aanmelden*.

   U bent als de geselecteerde gebruiker aangemeld bij BI-startpunt.

9.5.5.3 SAP-rollen en -gebruikers bijwerken

Nadat u SAP-verificatie heb ingeschakeld, is het noodzakelijk om regelmatig updates te plannen en uit te voeren voor toegewezen rollen die in het BI-platform geïmporteerd zijn. Hierdoor worden gegevens van SAP-rollen correct weergegeven in het platform.

Er bestaan twee opties voor het uitvoeren en plannen van updates voor SAP-rollen:

- Alleen rollen bijwerken: met deze optie worden alleen de koppelingen bijgewerkt tussen rollen die momenteel zijn toegewezen en die in het BI-platform zijn geïmporteerd. Het is raadzaam dat u deze optie gebruikt als u verwacht regelmatig updates uit te voeren, en u zich zorgen maakt over het gebruik van systeembronnen. Er worden geen nieuwe gebruikersaccounts gemaakt als u alleen SAP-rollen bijwerkt.
- Rollen en aliassen bijwerken: met deze optie worden niet alleen koppelingen tussen rollen bijgewerkt, maar worden ook nieuwe gebruikersaccounts gemaakt in het BI-platform voor gebruikersaliassen die zijn toegevoegd aan rollen in het SAP-systeem.

> ⓘ Opmerking
>
> Als u niet hebt opgegeven dat gebruikersaliassen automatisch worden gemaakt voor updates wanneer u SAP-verificatie hebt ingeschakeld, worden er geen accounts gemaakt voor nieuwe aliassen.

9.5.5.3.1 Updates voor SAP-rollen plannen

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem de rollen moet bijwerken.

1. Klik op het tabblad *Gebruikersupdate*.
2. Klik op *Plannen* in de sectie *Alleen rollen bijwerken* of het gebied *Rollen en aliassen bijwerken*.

   > → Tip
   >
   > Klik op *Nu bijwerken* om direct een update uit te voeren.

   > → Tip
   >
   > Gebruik de optie *Alleen rollen bijwerken* als u regelmatig wilt bijwerken en u zich zorgen maakt over de systeembronnen. Het systeem doet er langer over om zowel rollen als aliassen bij te werken.

   Nu wordt het dialoogvenster *Terugkeerpatroon* weergegeven.
3. Selecteer een optie in de lijst *Object uitvoeren* en geef alle gevraagde planningsgegevens op in de desbetreffende velden.

Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U geeft de begintijd en de begin- en einddatum op.
Dagelijks	De update wordt elke dag of elke <n> dagen uitgevoerd (waar <n> het aantal opgegeven dagen is). U kunt de begintijd en begin- en einddatum opgeven.
Wekelijks	De update wordt eens per week of meermaals per week uitgevoerd. U kunt opgeven op welke dagen de update wordt uitgevoerd, evenals de begintijd en de begin- en einddatums.
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt de begintijd en begin- en einddatum opgeven.
Ne dag van de maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
}1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
X dag van de Nde week van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

4. Klik op *Planning*.
   De datum van de volgende geplande rolupdate wordt weergegeven op het tabblad *Gebruikersupdate*.

> → Tip
>
> Als u de volgende geplande update wilt annuleren, klikt u op *Geplande updates annuleren* in het gebied *Alleen rollen bijwerken* of *Rollen en aliassen bijwerken*.

9.5.6 SNC configureren (Secure Network Communication)

In deze sectie wordt beschreven hoe u tijdens het instellen van SAP-verificatie een SNC met het BI-platform kunt configureren.

Zie SAP Note 1396213 voor meer informatie.

Voordat u de SAP- en BI-platformsystemen met elkaar vertrouwd maakt, moet u ervoor zorgen dat de SIA zo geconfigureerd is dat deze uitgevoerd kan worden onder een account die niet is ingesteld voor SNC. U moet ook uw SAP-systeem configureren om het BI-platform te vertrouwen.

Verwante informatie

Overzicht van vertrouwen aan de SAP-serverkant [pagina 343]

9.5.6.1 Overzicht van vertrouwen aan de SAP-serverkant

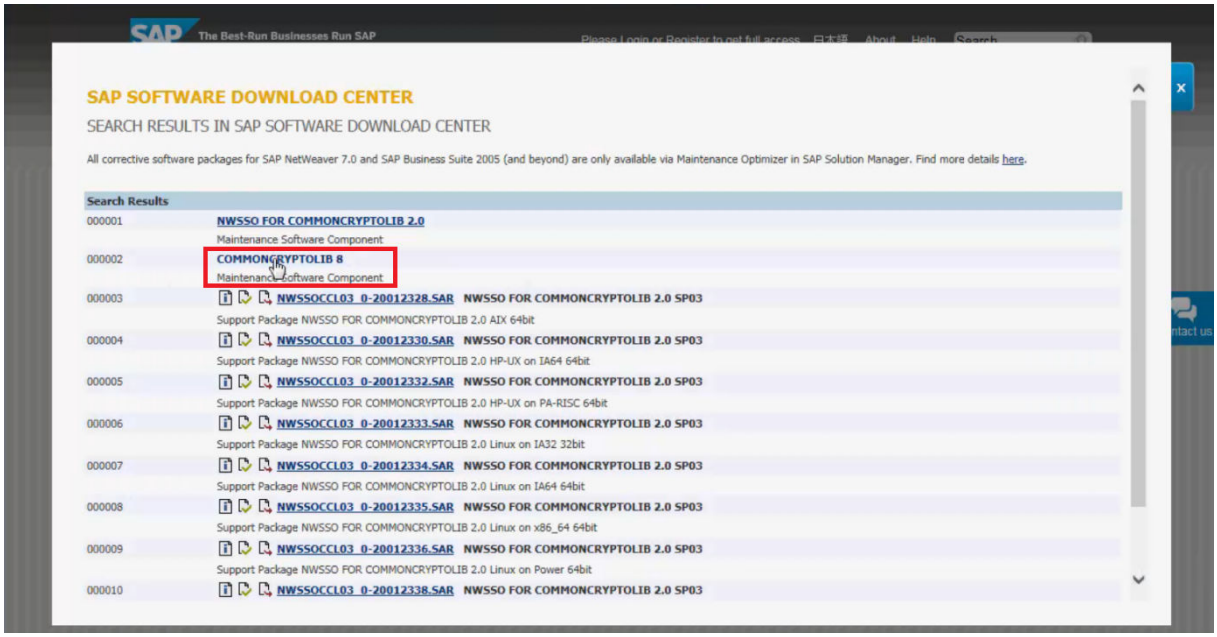
In deze sectie worden procedures beschreven voor het configureren van vertrouwen aan de serverkant tussen SAP-webtoepassingsservers (versie 6.20 en hoger) en SAP BusinessObjects Business Intelligence-platform. U moet vertrouwen aan de serverkant instellen als u gebruikmaakt van rapportburst met meerdere doorlopen (voor publicaties waarbij de rapportquery afhankelijk is van de context van de gebruiker).

Vertrouwen aan de serverkant betekent imitatie zonder wachtwoord. Om een SAP-gebruiker te imiteren zonder een wachtwoord te geven, moet een gebruiker met een veiligere methode als SAP-gebruiker worden geïdentificeerd dan met de gangbare combinatie van gebruikersnaam en wachtwoord. (Een SAP-gebruiker met het verificatieprofiel SAP_ALL kan geen andere SAP-gebruiker imiteren zonder diens wachtwoord te kennen.)

Vertrouwen aan de serverkant activeren met behulp van de SAP-cryptobibliotheek

Teneinde vertrouwen aan de serverzijde in te schakelen voor het BI-platform met behulp van de SAP-cryptobibliotheek, moet u eerst de relevante servers uitvoeren met referenties die worden geverifieerd met een geregistreerde provider van Secure Network Communication (SNC). Deze referenties worden geconfigureerd binnen SAP om toestemming te verkrijgen tot imitatie zonder wachtwoord. Voor het BI-platform moet u de servers die bij rapportbursts zijn betrokken, uitvoeren met deze SNC-referenties, zoals de Adaptive Job Server.

U hebt 32-bits binaire SNC-bestanden nodig voor 32-bits processen, en 64-bits binaire SNC-bestanden voor 64-bits processen. Naast het BI-platform wordt een SAP-cryptobibliotheek geïnstalleerd. Deze cryptografische bibliotheek kan alleen worden gebruikt voor het instellen van het vertrouwen aan de serverkant. De cryptografische bibliotheek is beschikbaar voor Windows en UNIX.



Zie SAP Notes 711093, 597059 en 397175 op de SAP-website voor meer informatie over de cryptografische bibliotheek.

De SAP-server en het BI-platform moeten certificaten krijgen toegewezen die voor elkaar hun wederzijdse identiteit bewijzen. Elke server krijgt een eigen certificaat en een lijst met certificaten van vertrouwde partijen. Teneinde vertrouwen aan de serverkant tussen SAP en het BI-platform te configureren, moet u een serie certificaten met wachtwoordbeveiliging maken. Dit wordt een Personal Security Environment (PSE) genoemd. In deze sectie wordt beschreven hoe u de PSE's installeert en onderhoudt, en op welke wijze u PSE's veilig koppelt aan verwerkingsservers van BI-platform

Verantwoordelijkheden van SAP BusinessObjects BI-platformservers

Specifieke BI-platformservers zijn relevant voor de SAP-integratie met betrekking tot eenmalige aanmelding. Deze servers staan in de volgende tabel, met hun verantwoordelijkheden.

Server	Verantwoordelijk voor
Webtoepassingsserver	Rollijst voor SAP-verificatie
BW Publisher Service	Selectielijst met dynamische parameters en personalisatie van Crystal Reports
CMS	Wachtwoord, ticket, lidmaatschap van rol controleren, en gebruikerslijsten
Page Server	Weergeven op aanvraag van Crystal Reports
Job Server	Crystal Reports plannen
Web Intelligence-verwerkingsserver	Weergave en planning van Web Intelligence-rapporten en zoeklijstaanwijzingen
Multi-Dimensional Analysis-service	Analyse

9.5.6.2 Vertrouwen op SAP-server configureren

Vertrouwen op server geldt uitsluitend voor Crystal Reports-rapporten en Web Intelligence-rapporten die zijn gebaseerd op universes (`.unv`). U moet SNC instellen voor gebruik met het BI-platform. Voor meer informatie of voor assistentie bij het oplossen van problemen raadpleegt u de documentatie die bij uw SAP-server is geleverd.

9.5.6.2.1 SAP configureren voor vertrouwen aan de serverkant

1. U hebt SAP-beheerdersreferenties nodig voor in SAP en voor de computer waarop SAP wordt uitgevoerd, en u hebt beheerdersreferenties nodig voor het BI-platform en de computer(s) waarop dit systeem draait.
2. Zorg op de SAP-computer dat de cryptografische bibliotheek van SAP en het hulpprogramma SAPGENPSE zich bevinden in de map `<STATION>:\usr\sap\<SID>\SYS\exe\run\` (in Windows).
3. Maak een omgeving met de naam **`<SECUDIR>`** die verwijst naar de map waar het 'ticket' is opgeslagen.

   > **Opmerking**
   >
   > Deze variabele moet toegankelijk zijn voor de gebruiker waaronder het proces *disp+work* van SAP wordt uitgevoerd.

4. Ga in de SAP GUI naar de transactie RZ10 en wijzig het exemplaarprofiel in de modus *Extended maintenance* (Uitgebreid onderhoud).

5. Stel in de modus voor bewerking van het profiel de variabelen van het SAP-profiel zodanig in dat ze verwijzen naar de cryptografische bibliotheek en geef het SAP-systeem een Distinguished Name (DN). Deze variabelen moeten de LDAP-naamgevingsconventie volgen:

Code	Betekenis	Beschrijving
CN	Common Name (Algemene naam)	De gewone naam van de bezitter van het certificaat.
OU	Organizational Unit (Organisatorische eenheid)	PG voor productgroep bijvoorbeeld.
O	Organisatie	De naam van de organisatie waarvoor het certificaat is uitgegeven.
C	Country (Land)	Het land waarin de organisatie is gevestigd.

Bijvoorbeeld voor R21: **`p:CN=R21, OU=PG, O=BOBJ, C=NL`**

> ⓘ Opmerking
>
> Het voorvoegsel **`p:`** staat voor de cryptografische bibliotheek van SAP. De prefix is vereist bij verwijzing naar de DN binnen SAP, maar is niet zichtbaar bij de controle van certificaten in STRUST of bij gebruik van SAPGENPSE.

6. Geef de volgende profielwaarden op en vervang waar nodig de gegevens door die van uw SAP-systeem:

Profielvariabele	Waarde
`ssf/name`	**`SAPSECULIB`**
`ssf/ssfapi_lib`	Volledige pad naar cryptografische bibliotheek van SAP
`sec/libsapsecu`	Volledige pad naar cryptografische bibliotheek van SAP
`snc/gssapi_lib`	Volledige pad naar cryptografische bibliotheek van SAP
`snc/identity/as`	De DN van uw SAP-systeem

7. Start uw exemplaar van SAP opnieuw.
8. Wanneer het systeem weer draait, meldt u zich aan en gaat u naar de transactie STRUST, waar nu extra gegevens moeten zijn opgenomen voor SNC en SSL.
9. Klik met de rechtermuisknop op het SNC-knooppunt en klik op *Maken*.
   De identiteit die u in RZ10 hebt opgegeven, moet nu worden weergegeven.
10. Klik op *OK*.
11. Klik op het vergrendelingspictogram als u een wachtwoord wilt toewijzen aan de SNC PSE.

> ⓘ Opmerking
>
> Zorg dat u het wachtwoord niet kwijtraakt. Telkens wanneer u de SNC PSE bekijkt of bewerkt, vraagt STRUST om het wachtwoord.

12. Sla de wijzigingen op.

> ⓘ Opmerking
>
> Als u de wijzigingen niet opslaat, start de toepassingsserver niet opnieuw wanneer u SNC activeert.

13. Keer terug naar transactie RZ10 en geef de rest van de parameters voor het SNC-profiel op:

Profielvariabele	Parameter
`snc/accept_insecure_rfc`	`1`
`snc/accept_insecure_r3int_rfc`	`1`
`snc/accept_insecure_gui`	`1`
`snc/accept_insecure_cpic`	`1`
`snc/permit_insecure_start`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/max`	`3`
`snc/enable`	`1`

Het minimum beveiligingsniveau is ingesteld op alleen verificatie (1) en het maximum is privacy (3). Met de waarde `snc/data_protection/use` wordt aangegeven dat in dit geval alleen verificatie wordt gebruikt, maar ook de volgende waarden zijn mogelijk: (2) voor integriteit, (3) voor privacy en (9) voor maximum. De waarden `snc/accept_insecure_rfc`, `snc/accept_insecure_r3int_rfc`, `snc/accept_insecure_gui` en `snc/accept_insecure_cpic` zijn ingesteld op (1), zodat voorgaande (en potentieel onbeveiligde) communicatiemethoden nog steeds worden toegestaan.

14. Start uw SAP-systeem opnieuw.

U moet het BI-platform nu configureren voor vertrouwen aan de serverzijde.

9.5.6.3 Het BI-platform configureren voor vertrouwen aan de serverzijde

De volgende procedures moeten worden uitgevoerd om het BI-platform te configureren voor vertrouwen aan de serverzijde. Deze stappen zijn bedoeld voor Windows, maar omdat het SAP-hulpprogramma een opdrachtregelprogramma is, zijn de stappen voor UNIX vrijwel gelijk.

1. De omgeving instellen
2. Een PSE (Personal Security Environment) genereren
3. De BI-platformservers configureren
4. PSE-toegang configureren
5. SNC-instellingen voor SAP-verificatie configureren
6. SAP-servergroepen instellen

Verwante informatie

De omgeving installeren [pagina 348]
Een PSE genereren [pagina 349]
BI-platformservers configureren [pagina 350]

Toegang tot de PSE configureren [pagina 350]
SNC-instellingen voor SAP-verificatie configureren [pagina 351]
Servergroepen gebruiken [pagina 352]

9.5.6.3.1 De omgeving installeren

Het BI-platform bevat een standaard cryptografische bibliotheek van SAP. Als u de standaardbibliotheek gebruikt, hoeft u alleen de laatste twee stappen uit te voeren: maak een submap en voeg een omgevingsvariabele toe. Als u een aangepaste kopie van de cryptografische bibliotheek van SAP wilt configureren, voert u alle stappen uit.

U kunt de standaard cryptografische bibliotheek van SAP op de volgende locatie vinden:

- Windows: `<INSTALLATIEMAP>\sap\sapcrypto.dll`
- Unix: `<INSTALLATIEMAP>/sap/libsapcrypto.so`

Zorg voordat u begint voor het volgende:

- De cryptografische bibliotheek van SAP moet uitgevouwen zijn op de host waarop de verwerkingsservers van BI-platform draaien.
- De gewenste SAP-systemen moeten zo zijn geconfigureerd dat de cryptografische bibliotheek van SAP wordt gebruikt als SNC-leverancier.

Voordat u met het onderhoud van een PSE kunt beginnen, moet u de bibliotheek en het hulpprogramma installeren, evenals de omgeving waarin PSE's worden opgeslagen.

1. Kopieer de cryptografische bibliotheek van SAP (met inbegrip van het hulpprogramma voor PSE-onderhoud) naar een map op de computer waarop het BI-platform is geïnstalleerd.

   Bijvoorbeeld: `C:\Programmabestanden\SAP\Crypto`
2. Voeg de map toe aan de omgevingsvariabele `<PATH>`.
3. Voeg voor het hele systeem een omgevingsvariabele `<SNC_LIB>` toe die verwijst naar de cryptografische bibliotheek.

   Bijvoorbeeld: `C:\Programmabestanden\SAP\Crypto\sapcrypto.dll`

   > **Opmerking**
   >
   > De maximumlengte van het pad is 100 tekens.
4. Maak een submap met de naam **`sec`**.

   Bijvoorbeeld: `C:\Programmabestanden\SAP\Crypto\sec`
5. Voeg voor het hele systeem een omgevingsvariabele `<SECUDIR>` toe die verwijst naar de map **`sec`**.

Verwante informatie

Vertrouwen op SAP-server configureren [pagina 345]

9.5.6.3.2 Een PSE genereren

SAP accepteert een BI-platformserver als vertrouwde eenheid als deze beschikt over een PSE en als die PSE is gekoppeld aan SAP. Dit "vertrouwen" tussen SAP en onderdelen van BI-platform wordt ingesteld door de openbare versie van elkaars certificaten te delen. Als eerste moet een PSE voor het BI-platform worden gegenereerd die automatisch zijn eigen certificaat genereert.

1. Open een opdrachtprompt en voer **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`** uit vanuit de map met de cryptografische bibliotheek.
2. Kies een PIN en een DN voor uw BI-platform.

   Bijvoorbeeld: **`CN=MyBOE01, OU=PG, O=BOBJ, C=NL`**.

   U beschikt nu over een standaard PSE met een eigen certificaat.
3. Met de volgende opdracht exporteert u het certificaat in de PSE:

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```
4. Ga in de SAP GUI naar de transactie STRUST en open de systeem-PSE die is gekoppeld aan uw SAP-systeem.

   Mogelijk wordt u nu om het wachtwoord gevraagd dat u al aan deze systeem-PSE hebt toegewezen.
5. Importeer het eerder gemaakte bestand `<MyBOECert.crt>` door linksonder in het STRUST-transactiescherm op "Certificaat importeren" te klikken.

   De certificaten uit SAPGENPSE hebben een Base64-indeling. Zorg ervoor dat u Base64 selecteert bij het importeren van de certificaten.
6. Klik op de knop *Toevoegen aan certificatenlijst* om het certificaat van BI-platform aan de lijst met PSE-certificaten van de SAP-server toe te voegen.
7. Sla de wijzigingen op in STRUST.
8. Klik op *Exporteren* en geef het certificaat een bestandsnaam.

   Bijvoorbeeld: **`MySAPCert.crt`**.

   > ⓘ Opmerking
   >
   > De indeling moet Base64 blijven.
9. Ga naar de transactie SNCO.
10. Voeg een nieuwe vermelding toe, waarbij het volgende geldt:
    - De systeem-id is een willekeurige keuze, maar geeft wel het BusinessObjects BI-platformsysteem weer.
    - De SNC-naam moet de DN zijn (voorafgegaan door **`p:`**) die u hebt opgegeven bij het maken van de PSE van BI-platform in stap 2.
    - De selectievakjes *Vermelding voor RFC geactiveerd* en *Vermelding voor ext. id geactiveerd* zijn beide ingeschakeld:
11. Voer de volgende opdracht uit op de opdrachtprompt om het geëxporteerde certificaat toe te voegen aan de PSE van BI-platform:

    ```
    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
    ```

De cryptografische bibliotheek van SAP is nu geïnstalleerd op de computer met BI-platform. U hebt een PSE gemaakt die door de servers van BI-platform wordt gebruikt om zich te identificeren als SAP-servers. SAP en de PSE van BI-platform hebben certificaten uitgewisseld. SAP staat entiteiten met toegang tot de PSE van BI-platform toe om RFC-aanroepen en imitatie zonder wachtwoord uit te voeren.

Verwante informatie

BI-platformservers configureren [pagina 350]

9.5.6.3.3 BI-platformservers configureren

Nadat u een PSE hebt gegenereerd voor het BI-platform, moet u een serverstructuur configureren die geschikt is voor SAP-verwerking. Met de volgende procedure maakt u een knooppunt voor SAP-verwerkingsservers, zodat u op het knooppuntniveau besturingssysteemreferenties kunt instellen.

> **Opmerking**
>
> In deze versie van het BI-platform worden servers niet meer geconfigureerd in de Central Configuration Manager (CCM). In plaats daarvan moet u nu een nieuwe Server Intelligence Agent (SIA) maken.

1. Maak in de CCM en nieuw knooppunt voor SAP-verwerkingsservers.

   Geef het knooppunt een toepasselijke naam, zoals **SAPProcessor**.
2. Voeg in de CMC de gewenste verwerkingsservers toe aan het nieuwe knooppunt en start vervolgens de nieuwe servers.

9.5.6.3.4 Toegang tot de PSE configureren

Nadat u het knooppunt voor BI-platform en de servers hebt geconfigureerd, moet u de PSE configureren met het hulpprogramma SAPGENPSE.

1. Voer de volgende opdracht uit vanaf de opdrachtprompt:

   ```
   sapgenpse.exe seclogin -p SBOE.pse
   ```

   > **Opmerking**
   >
   > U wordt gevraagd om de PSE PIN. Als u het hulpprogramma onder dezelfde referenties uitvoert als u gebruikt voor de SAP-verwerkingsservers in BI-platform, hoeft u geen gebruikersnaam op te geven.
2. U kunt controleren of de koppeling voor eenmalig aanmelden is ingesteld door de inhoud van de PSE met behulp van de volgende opdracht weer te geven:

   ```
   sapgenpse.exe maintain_pk -l
   ```

   Het resultaat moet er ongeveer zo uitzien:

   ```
   C:\Documents and
   Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My
   Documents\snc\sec\bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ------------------------------------------------------------
              Version:                  0 (X.509v1-1988)
              SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
   ```

```
            IssuerName:                CN=R21Again, OU=PG, O=BOBJ, C=CA
            SerialNumber:              00
            Validity  -  NotBefore:    Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                  NotAfter:
Thu Dec 31 16:00:01 2037 (380101000001Z)
            Public Key Fingerprint:    851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
            SubjectKey:                Algorithm RSA (OID
1.2.840.113549.1.1.1), NULL
C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
```

Als de opdracht **`seclogin`** naar behoren is uitgevoerd, wordt niet meer naar de PSE PIN gevraagd.

> **Opmerking**
>
> Als u problemen ondervindt met de toegang tot PSE, gebruikt u argument `-O` om PSE-toegang op te geven. Wilt u bijvoorbeeld een specifieke gebruiker in een specifiek domein PSE-toegang verlenen, dan typt u deze opdracht in Windows:
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 SNC-instellingen voor SAP-verificatie configureren

Nadat u de toegang tot de PSE hebt geconfigureerd, moet u de instellingen voor de SAP-verificatie configureren in de CMC.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP*.

De instellingen van de machtigingssystemen worden weergegeven.

3. Klik op het tabblad *SNC-instellingen* op de pagina *SAP-verificatie*.
4. Selecteer uw machtigingssysteem in de lijst *Logical System-naam*.
5. Selecteer *Secure Network Communication [SNC] inschakelen* onder *Basisinstellingen*.
6. Selecteer de optie *Standaard gebruiken* om het standaardpad voor de bibliotheek te accepteren, of selecteer de optie *Aangepast pad definiëren* om een andere locatie te kiezen.
7. Selecteer een beschermingsniveau onder *Beveiligingskwaliteit*.

   Selecteer bijvoorbeeld *Verificatie*.

   > ⓘ Opmerking
   >
   > Dit moet niet hoger liggen dan het beveiligingsniveau van het SAP-systeem. Het beveiligingsniveau kan worden aangepast en wordt bepaald door de behoeften van uw organisatie en de mogelijkheden die de SNC-bibliotheek biedt.
   >
   > *Beveiligingskwaliteit* verwijst alleen naar verwerking aan platformzijde. DHTML-viewer van Web Intelligence voldoet bijvoorbeeld aan het opgegeven niveau. Clientcommunicatie met SAP Business Warehouse (BW) moet echter als onbeveiligd worden beschouwd. Communicatie van Web Intelligence Rich Client of het hulpprogramma voor informatieontwerp is bijvoorbeeld nooit gecodeerd.

8. Voer de SNC-naam van het SAP-systeem in bij de *Wederzijdse-verificatie-instellingen*.

   De SNC-naamnotatie is afhankelijk van de SNC-bibliotheek. Aan de hand van de SAP-cryptografiebibliotheek is de aanbeveling voor de DN-naam om de LDAP-naamgevingsconventies te volgen en `p:` als voorvoegsel toe te voegen.
9. Bevestig dat de SNC-naam van de referenties waarmee de BI-platformservers worden uitgevoerd, worden weergegeven in het vakje *SCN-naam van Enterprise-systeem*.

   Als er meerdere SNC-namen zijn geconfigureerd, moet dit veld leeg zijn.
10. Geef de DN's van het SAP-systeem en de PSE van het BI-platform op.

9.5.6.3.6 Servergroepen gebruiken

Tenzij de verwerkingsservers (Crystal Reports of Web Intelligence) uitgevoerd worden met referenties die toegang hebben tot de PSE, moet u een specifieke servergroep maken die alleen deze servers en de vereiste ondersteunende servers bevat. Voor meer informatie en beschrijvingen van de verschillende BI-platformservers raadpleegt u het hoofdstuk “Architectuur”.

U kunt kiezen uit drie opties wanneer u inhoudsverwerkingsservers configureert voor uw SAP-inhoud:

1. Houd één SIA bij, inclusief alle BI-platformservers, die uitgevoerd worden onder referenties met toegang tot de PSE. Dit is de eenvoudigste optie. Er hoeven geen servergroepen gemaakt te worden. Dit is de minst veilige aanpak, omdat een onnodig aantal servers toegang tot de PSE hebben.
2. Maak een tweede SIA met toegang tot de PSE en voeg deze aan de Crystal Reports- of Web Intelligence-verwerkingsservers toe. Verwijder de gedupliceerde servers uit de oorspronkelijke SIA. Er hoeven geen servergroepen gemaakt te worden, maar er zijn minder servers met toegang tot de PSE.
3. Maak een SIA exclusief voor gebruik met SAP en met toegang tot de PSE. Voeg deze aan de Crystal Reports- of Web Intelligence-verwerkingsservers toe. Bij deze optie dient er alleen SAP-inhoud op deze servers uitgevoerd te worden, en belangrijker, SAP-inhoud dient alleen op deze servers uitgevoerd te worden. Aangezien in dit scenario inhoud naar bepaalde servers geleid moet worden, moet u servergroepen voor de SIA maken.

Richtlijnen voor het gebruik van een servergroep

De servergroep moet naar de SIA verwijzen die exclusief voor de verwerking van SAP-inhoud wordt gebruikt. De servergroep moet ook naar de volgende servers verwijzen:

- Adaptive Servers
- Adaptive Job Servers

Alle SAP-inhoud, Web Intelligence-documenten en Crystal Reports-rapporten moeten zo strikt mogelijk aan de servergroep worden gekoppeld, d.w.z. dat ze op servers in de groep moeten worden uitgevoerd. Nadat deze koppeling op objectniveau is ingesteld, moet de servergroepinstelling doorgevoerd worden naar instellingen voor zowel directe planning als publicaties.

Als u wilt voorkomen dat andere (niet-SAP) inhoud op de SAP-specifieke verwerkingsservers wordt verwerkt, moet u een andere servergroep maken met alle servers onder de oorspronkelijke SIA. Het is raadzaam een strikte koppeling tussen deze inhoud en de niet-SAP servergroep in te stellen.

9.5.6.4 Multi-pass publicaties configureren

Problemen oplossen voor publicaties met meerdere fasen

Als u problemen ondervindt met publicaties met meerdere fasen, schakelt u tracering in voor de stuurprogramma's van Crystal Reports (CR) of Multidimensional Data Access (MDA) voor SAP, en controleert u de aanmeldingstekenreeks die voor elke taak of ontvanger wordt gebruikt. Deze aanmeldingstekenreeks moet er ongeveer zo uitzien:

```
 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
```

De tekenreeks moet het gewenste **`EXTIDTYPE=UN`** (als gebruikersnaam) hebben en **`EXTIDDATA`** moet de SAP-gebruikersnaam van de ontvanger zijn. In dit voorbeeld is de aanmeldingspoging geslaagd.

9.5.6.5 Werkstroom voor integratie met Secure Network Communication

Het BI-platform ondersteunt omgevingen waarin SNC (Secure Network Communication) wordt geïmplementeerd voor verificatie en gegevenscodering tussen SAP-onderdelen. Als u de SAP Cryptographic Library hebt geïmplementeerd (of een ander extern beveiligingsproduct waarin de SNC-interface wordt gebruikt), moet u enkele aanvullende waarden instellen om het BI-platform effectief in uw beveiligde omgeving te integreren.

Voer de volgende taken uit als u het platform wilt configureren voor het gebruik van beveiligde netwerkcommunicatie:

1. Configureer de BI-platformservers zodanig dat deze worden gestart en uitgevoerd onder een geschikte gebruikersaccount.
2. Configureer het SAP-systeem zodanig dat uw BI-platformsysteem wordt vertrouwd.
3. Configureer de SNC-instellingen in de SNC-koppeling in de Central Management Console.
4. Importeer SAP-rollen en -gebruikers in het BI-platform.

Verwante informatie

SAP-rollen importeren [pagina 339]

9.5.6.6 SNC-instellingen in de Central Management Console configureren

Voordat u SNC-instellingen kunt configureren, moet u een nieuw machtigingssysteem toevoegen aan het BI-platform, zorgen dat het SNC-bibliotheekbestand in een bekende map staat en een `<RFC_LIB>`-omgevingsvariabele maken om naar het bestand te wijzen.

1. Klik op het tabblad *SNC-instellingen* op de pagina *SAP-verificatie*.
2. Selecteer uw machtigingssysteem in de lijst *Logical System-naam*.
3. Selecteer *Secure Network Communication [SNC] inschakelen* onder *Basisinstellingen*.
4. Als u SAP-verificatie configureert voor de consumptie van `.unx`-universes of OLAP BICS-verbindingen en u STS wilt gebruiken, schakelt u het selectievakje *Onveilige inkomende RFC-verbindingen voorkomen* in.
5. Selecteer de optie *Standaard gebruiken* om het standaardpad voor de bibliotheek te accepteren, of selecteer de optie *Aangepast pad definiëren* om een andere locatie te kiezen.

   De webtoepassingsserver en de CMS moeten zich op hetzelfde type besturingssysteem bevinden met hetzelfde pad naar de cryptobibliotheek.
6. Selecteer een beschermingsniveau onder *Beveiligingskwaliteit*.

   Selecteer bijvoorbeeld *Verificatie*.

   > **Opmerking**
   >
   > Het beveiligingsniveau kan worden aangepast en wordt bepaald door de behoeften van uw organisatie en de mogelijkheden die de SNC-bibliotheek biedt.

7. Voer de SNC-naam van het SAP-systeem in bij de *Wederzijdse-verificatie-instellingen*.

   De SNC-naamnotatie is afhankelijk van de SNC-bibliotheek. Aan de hand van de SAP-cryptografiebibliotheek is de aanbeveling voor de DN-naam om de LDAP-naamgevingsconventies te volgen en `p:` als voorvoegsel toe te voegen.
8. Bevestig dat de SNC-naam van de referenties waarmee BI-platformservers worden uitgevoerd, worden weergegeven in het vakje *SCN-naam van Enterprise-systeem*.
9. Klik op *Bijwerken*.

Verwante informatie

Verbinding maken met SAP-machtigingssystemen [pagina 333]

9.5.6.7 De machtigingsgebruiker aan een SNC-naam koppelen

1. Meld u aan bij het SAP BW-systeem en voer de transactie `SU01` uit.

   Het scherm User Maintenance: Initial Screen (gebruikersonderhoud: beginscherm) wordt weergegeven.
2. Typ in het veld *User* (gebruiker) de naam van de SAP-account die als machtigingsgebruiker is toegewezen en klik op de werkbalk op *Change* (wijzigen).

   Het scherm Maintain User (gebruiker onderhouden) wordt weergegeven.
3. Klik op het tabblad SNC.
4. Typ in het veld *SNC name* (SNC-naam) de `SNC USER ACCOUNT` die u hierboven bij stap 2 hebt opgegeven.
5. Klik op *Opslaan*.

9.5.6.8 Een systeem-id toevoegen aan de SNC Access Control List

1. Meld u aan bij het SAP BW-systeem en voer de transactie `SNC0` uit.

   Het scherm Weergave wijzigen 'SNC: Access Control List (ACL) voor systemen' wordt weergegeven.
2. Klik op *Nieuwe vermeldingen* op de werkbalk.

   Het scherm Nieuwe vermeldingen: Details van toegevoegde vermeldingen wordt weergegeven.
3. Typ de naam van de BI-platformcomputer in het veld *Systeem-id*.
4. Typ `p:<SNC-GEBRUIKERSNAAM>` in het veld *SNC-gebruikersnaam*, waarbij `SNC-GEBRUIKERSNAAM` staat voor de account die is gebruikt voor het configureren van de BI-platformservers.

> **Opmerking**
>
> Als uw SNC-provider 'gssapi32.dll' is, moet u hoofdletters gebruiken om de SNC-GEBRUIKERSNAAM op te geven. Geef bij de gebruikersaccount ook de domeinnaam op. Bijvoorbeeld: domein\gebruikersnaam.

5. Schakel *Vermelding voor RFC geactiveerd* en *Vermelding voor ext. id geactiveerd* in.
6. Schakel alle overige opties uit en klik op *Opslaan*.

9.5.7 Eenmalige aanmelding bij het SAP-systeem instellen

In een geïntegreerde omgeving wisselen verschillende client- en back-endservices van het BI-platform gegevens uit met SAP NetWeaver ABAP back-endsystemen. Het is handig om eenmalige aanmelding van het BI-platform bij deze back-endsystemen (meestal BW) in te stellen. Wanneer een ABAP-systeem als extern verificatiesysteem is geconfigureerd, worden eigen SAP-tokens gebruikt om een mechanisme te creëren dat eenmalige aanmelding ondersteunt voor alle BI-platformclients en -services die verbinding maken met SAP NetWeaver ABAP-systemen.

Zie voor meer informatie note 1670073.

Voor eenmalige aanmelding bij het SAP-systeem moet u een `keystore`-bestand en een overeenkomstig certificaat maken. Gebruik het opdrachtregelprogramma van de `keytool` om het bestand en het certificaat te genereren. Het keytool-programma is standaard geïnstalleerd in de `sdk/bin`-map voor elk platform.

Dit certificaat moet met behulp van de CMC aan uw SAP ABAP BW-systeem en het BI-platform worden toegevoegd.

> **Opmerking**
>
> De invoegtoepassing voor SAP-verificatie moet geconfigureerd zijn voordat u eenmalige aanmelding bij de database voor SAP BW kunt instellen.

9.5.7.1 Het keystore-bestand genereren

Dit onderwerp bevat instructies voor het gebruik van Java Keytool voor het genereren van keystorebestanden. In de onderstaande lijst worden de standaardlocaties van de Java Keytool vermeld:

Platform	Standaardlocatie
Windows	`<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\ win64_x64\sapjvm\bin`
Linux	`sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool`

1. Ga naar de standaardlocatie van Java Keytool en start de opdrachtprompt.
2. Voer de Java Keytool uit voor het genereren van de keystore.
   a. Ga naar <INSTALLATIEMAP>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.

b. Voer de volgende opdracht uit:

- Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
- Linux: `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

> → Tip
>
> Voer het hulpprogramma met de parameter -? uit om de standaardwaarden te overschrijven. Het volgende bericht wordt weergegeven:

> {·} Voorbeeldcode
>
> ```
> Usage: keytool -genkey <options>
>  -keystore <filename(keystore.p12)>
>  -alias <key entry alias(mywin)>
>  -storepass <keystore password (admin1)>
>  -dname <certificate subject DN(CN=palmtree)>
>  -validity <number of days (365)>
>  -cert <filename (cert.der)>
>  (No certificate is generated when importing a keystore)
>  -importkeystore <filename>
> ```

U kunt de parameters gebruiken voor het overschrijven van de standaardwaarden.

> ⓘ Opmerking
>
> U moet Java Keytool gebruiken ter vervanging van hulpprogramma moet gebruiken PKCS12 om de keystore te genereren. Raadpleeg 2524775 voor meer informatie.

9.5.7.2 Het certificaat voor de publieke sleutel exporteren

U moet een certificaat voor het keystore-bestand maken en exporteren.

1. Open een opdrachtprompt en navigeer naar de map waarin het keytool-programma zich bevindt.
2. Als u een sleutelcertificaat voor het keystore-bestand wilt exporteren, gebruikt u de volgende opdracht.

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

Vervang <keystore> door de naam van het keystore-bestand.
Vervang <bestandsnaam> door de bestandsnaam van het certificaat.
Vervang <alias> door de alias die gebruikt is om het keystore-bestand te maken.

3. Voer het wachtwoord in dat u voor het keystore-bestand hebt opgegeven, wanneer u hierom wordt gevraagd.

U hebt nu een keystore-bestand en een certificaat in de map waarin het keytool-programma zich bevindt

9.5.7.3 Het certificaatbestand in het ABAP SAP-doelsysteem importeren

U hebt een keystore-bestand en een gekoppeld certificaat voor uw BI-platformimplementatie nodig om de volgende taak uit te voeren.

> ⓘ Opmerking
>
> Deze handeling kan alleen worden uitgevoerd op een ABAP SAP-systeem.

1. Maak verbinding met uw SAP ABAP BW-systeem via de SAP GUI.

   > ⓘ Opmerking
   >
   > Zorg ervoor dat u verbinding maakt als gebruiker met beheerdersrechten.

2. Voer STRUSTSSO2 uit in de SAP GUI.
   Het systeem is voorbereid op de import van het certificaatbestand.
3. Ga naar het tabblad *Certificate*.
4. Controleer of het selectievakje *Use Binary option* is ingeschakeld.
5. Klik op de knop voor het bestandspad om naar de locatie te verwijzen waar het certificaatbestand zich bevindt.
6. Klik op het groene vinkje.
   Het certificaatbestand wordt geüpload.
7. Klik op *Add to Certificate List*.
   Het certificaat wordt weergegeven in de lijst Certificaat.
8. Klik op *Add to ACL* en geef een systeem-id en client op.

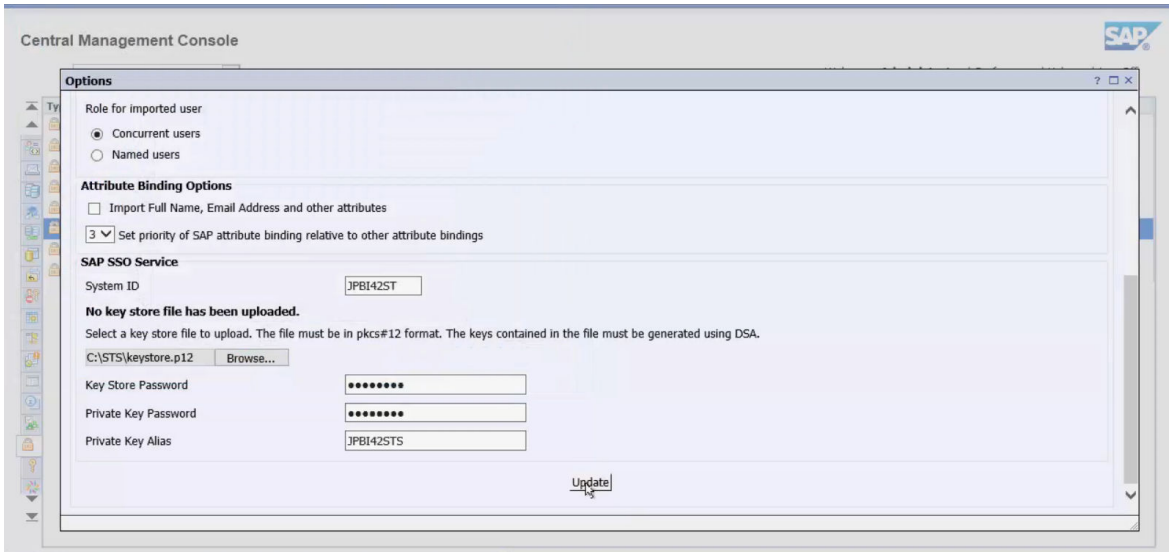
   De systeem-id moet overeenkomen met de id die gebruikt is om het BI-platformsysteem voor SAP BW te identificeren.

   Het certificaat wordt toegevoegd aan de toegangscontrolelijst. De client moet worden opgegeven als “000”.
9. Sla uw wijzigingen op en sluit af.
   De wijzigingen worden opgeslagen in het SAP-systeem.

9.5.7.4 Eenmalige aanmelding bij de SAP-database configureren in de CMC

Voor de volgende procedure moet u de SAP-beveiligingsinvoegtoepassing oproepen via een beheerdersaccount.

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op de koppeling *SAP* en klik vervolgens op het tabblad *Opties*.



Als er geen certificaat is geïmporteerd, moet het volgende bericht in de sectie *SAP SSO-service* worden weergegeven:

```
Er is geen keystore-bestand geüpload.
```

3. Geef de systeem-id voor uw BI-platformsysteem op in het desbetreffende veld.

   Deze moet identiek zijn aan de waarde die gebruikt is bij het importeren van het certificaat in het SAP ABAP-doelsysteem.

4. Klik op de knop *Bladeren* om naar het keystore-bestand te verwijzen.
5. Geef de volgende vereiste gegevens op:

Veld	Vereiste informatie
Keystore-wachtwoord	Typ het wachtwoord dat vereist is om toegang te krijgen tot het keystore-bestand. Dit wachtwoord is opgegeven toen het keystore-bestand werd gemaakt.
Wachtwoord voor privésleutel	Typ het wachtwoord dat vereist is om toegang te krijgen tot het certificaat dat overeenkomt met het keystore-bestand. Dit wachtwoord is opgegeven toen het certificaat voor het keystore-bestand werd gemaakt.
Alias van privésleutel	Typ de alias die vereist is om toegang te krijgen tot het keystore-bestand. Deze alias is opgegeven toen het keystore-bestand werd gemaakt.

6. Klik op *Bijwerken* om de instellingen door te voeren.
   Zodra de instellingen zijn doorgevoerd, wordt het volgende bericht onder het veld Systeem-id weergegeven:

   ```
   Een keystore-bestand is geüpload.
   ```

9.5.7.5 De service voor beveiligingstokens aan de Adaptive Processing Server toevoegen

In een geclusterde omgeving worden de services voor beveiligingstokens apart toegevoegd aan elke Adaptive Processing Server.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op *Kernservices*.
   De lijst met servers wordt onder *Kernservices* weergegeven.
3. Klik met de rechtermuisknop op de Adaptive Processing Server en selecteer *Server stoppen*.

   Ga niet verder voordat de server de status Gestopt heeft.
4. Klik met de rechtermuisknop op de Adaptive Processing Server en selecteer *Services selecteren*.
   Het dialoogvenster *Services selecteren* verschijnt.
5. Gebruik de knop *Toevoegen* om de service voor beveiligingstokens van de lijst *Beschikbare services* naar de lijst *Services* te verplaatsen.
6. Klik op *OK*.
7. Start de Adaptive Processing Server opnieuw.

9.5.8 SSO configureren voor SAP Crystal Reports en SAP NetWeaver

BI-platform wordt standaard zo geconfigureerd dat SAP Crystal Reports-gebruikers toegang hebben tot SAP-gegevens met eenmalige aanmelding.

9.5.8.1 SSO deactiveren voor SAP NetWeaver en SAP Crystal Reports

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Selecteer een van de volgende stuurprogramma's:

Stuurprogramma	Weergavenaam
ODS-stuurprogramma (Operation Data Store)	*crdb_ods*
Open SQL-stuurprogramma	*crdb_opensql*
InfoSet-stuurprogramma	*crdb_infoset*
BW MDX-querystuurprogramma	*crdb_bwmdx*

5. Klik op *Verwijderen*.
6. Klik op *Opslaan en sluiten*.
7. Start SAP Crystal Reports opnieuw op.

9.5.8.2 SSO opnieuw activeren voor SAP NetWeaver en SAP Crystal Reports

Volg de onderstaande stappen om SSO opnieuw te activeren voor SAP NetWeaver (ABAP) en SAP Crystal Reports.

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Typ onder *SSO-context gebruiken voor aanmelding bij database*:

`crdb_ods`	Het ODS-stuurprogramma activeren
`crdb_opensql`	Het Open SQL-stuurprogramma activeren
`crdb_bwmdx`	Het SAP BW MDX-querystuurprogramma activeren
`crdb_infoset`	Het InfoSet-stuurprogramma activeren

5. Klik op *Toevoegen*.
6. Klik op *Opslaan en sluiten*.
7. Start SAP Crystal Reports opnieuw op.

9.6 PeopleSoft-verificatie

9.6.1 Overzicht

Als u uw PeopleSoft Enterprise-gegevens met BI-platform wilt gebruiken, moet u het programma informatie verschaffen over uw implementatie. Met deze informatie kunnen gebruikers door BI-platform worden geverifieerd, zodat ze hun PeopleSoft-referenties kunnen gebruiken om zich aan te melden bij het programma.

9.6.2 PeopleSoft Enterprise-verificatie inschakelen

U kunt BI-platform gebruik laten maken van PeopleSoft Enterprise-informatie door BI-platform informatie te geven over verificatie in uw PeopleSoft Enterprise-systeem.

9.6.2.1 PeopleSoft Enterprise-verificatie inschakelen in het BI-platform

1. Meld u als beheerder aan bij de Central Management Console.

2. Klik in het gebied Beheren op *Verificatie*.
3. Dubbelklik op *PeopleSoft Enterprise*.
   De pagina *PeopleSoft Enterprise* wordt weergegeven. Deze heeft vier tabbladen: *Opties*, *Domeinen*, *Rollen* en *Gebruikersupdate*.
4. Op het tabblad *Opties* selecteert u het vakje *PeopleSoft Enterprise-verificatie inschakelen*.
5. Maak de gewenste wijzigingen onder *Nieuwe alias*, *Bijwerkopties* en *Opties voor nieuwe gebruiker* volgens uw BI-platformimplementatie.

   Klik op *Bijwerken* om de wijzigingen op te slaan voordat u naar het tabblad *Domeinen* gaat.
6. Klik op het tabblad *Domeinen*.
7. In het gebied *PeopleSoft Enterprise-systeemgebruiker* typt u een databasegebruikersnaam en -wachtwoord waarmee BI-platform zich bij uw PeopleSoft Enterprise-database moet aanmelden.
8. In het gebied *PeopleSoft Enterprise-domeinen* voert u de domeinnaam en het QAS-adres in voor verbinding met uw PeopleSoft Enterprise-omgeving en klikt u op *Toevoegen*.

   > ⓘ Opmerking
   >
   > Als u over meerdere PeopleSoft-domeinen beschikt, herhaalt u deze stap voor alle overige domeinen waartoe u toegang hebt. Het eerste domein dat u invoert, wordt het standaarddomein.
9. Klik op *Bijwerken* om de wijzigingen op te slaan.

9.6.3 PeopleSoft-rollen toewijzen aan het BI-platform

BI-platform maakt automatisch een groep voor elke PeopleSoft-rol die u toewijst. Daarnaast maakt het programma aliassen voor de leden van de toegewezen PeopleSoft-rollen.

U kunt een gebruikersaccount maken voor elke gemaakte alias.

Als u echter meerdere systemen uitvoert en de gebruikers accounts hebben in meer dan een systeem, kunt u iedere gebruiker toewijzen aan een alias met dezelfde naam voordat u de accounts maakt in BI-platform.

Op deze manier hoeft u minder accounts voor dezelfde gebruiker te maken in BI-platform.

Als u bijvoorbeeld PeopleSoft HR 8.3 en PeopleSoft Financials 8.4 uitvoert en 30 van uw gebruikers toegang tot beide systemen hebben, hoeft u slechts 30 accounts voor die gebruikers te maken. Als u niet iedere gebruiker toewijst aan een alias met dezelfde naam, worden er 60 accounts voor 30 gebruikers gemaakt in het BI-platform.

Als u echter meerdere systemen uitvoert waarbij gebruikersnamen elkaar overlappen, moet u een nieuwe lidaccount maken voor elke gemaakte alias.

Als u bijvoorbeeld PeopleSoft HR 8.3 met een gebruikersaccount voor Russell Aquino (gebruikersnaam 'raquino') en PeopleSoft Financials 8.4 met een gebruikersaccount voor Raoul Aquino (gebruikersnaam 'raquino') uitvoert, moet u een afzonderlijke account maken voor de alias van iedere gebruiker. Anders worden de twee gebruikers toegevoegd aan dezelfde BI-platformaccount. Beide gebruikers kunnen zich met hun eigen PeopleSoft-referenties bij het BI-platform aanmelden en gegevens uit beide PeopleSoft-systemen opvragen.

9.6.3.1 Een PeopleSoft-rol toewijzen aan het BI-platform

Als de JVM (Java Virtual Machine) van BI-platform geen certificaat voor de PeopleSoft-server heeft, moet u de volgende extra stappen uitvoeren voordat u de hoofdstappen uitvoert:

1. Haal het CER-bestand op van de PeopleSoft-server.
2. Kopieer het CER-bestand naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Voer de volgende opdracht uit via de beveiligingsmap: `"<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`.
4. Start de webtoepassingsserver opnieuw.

Hoofdstappen:

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik op *Verificatie*.
3. Dubbelklik op *PeopleSoft Enterprise*.
4. Selecteer op het tabblad *Rollen* in het gebied PeopleSoft Enterprise-domeinen het domein met de rol die u wilt toewijzen aan BI-platform.
5. Gebruik een van de volgende opties om de rollen te selecteren die u wilt toewijzen:
   - Geef in het tekstvak Rollen zoeken in het gebied *PeopleSoft Enterprise-rollen* de rol op die u wilt zoeken en aan BI-platform wilt toewijzen. Klik vervolgens op >.
   - Selecteer in de lijst *Beschikbare rollen* de rol die u aan het *BI-platform* wilt toewijzen, en klik op >

   > **Opmerking**
   >
   > Als u een bepaalde gebruiker of rol zoekt, kunt u het jokerteken % gebruiken. Typ bijvoorbeeld *A%* om alle rollen weer te geven die beginnen met de letter A. De zoekfunctie is hoofdlettergevoelig.

   > **Opmerking**
   >
   > Als u een rol uit een ander domein wilt toewijzen, selecteert u het nieuwe domein in de lijst met beschikbare domeinen.

6. Ga naar het tabblad *Gebruikersupdate* en klik op de knop *Bijwerken* of plan de updates.
7. Ga op het tabblad *Opties* naar het gebied *Opties voor nieuwe gebruiker* en selecteer een van de volgende opties:
   - *Elke toegevoegde alias toewijzen aan een account met dezelfde naam*
     Selecteer deze optie als u meerdere PeopleSoft Enterprise-systemen hebt met gebruikers die accounts hebben in meer dan één systeem (waarbij gebruikers niet dezelfde gebruikersnaam voor verschillende systemen hebben).
   - *Een nieuwe account maken voor elke toegevoegde alias*
     Selecteer deze optie als u slechts één PeopleSoft Enterprise-systeem hebt, als de meerderheid van de gebruikers een account heeft in slechts één systeem of als de gebruikersnamen voor verschillende gebruikers elkaar overlappen in twee of meer systemen.
8. Selecteer in het gebied *Bijwerkopties van alias* een van de volgende opties:
   - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
     Selecteer deze optie als u een nieuwe alias wilt maken voor iedere gebruiker die is toegewezen aan BI-platform. Als u de optie Een nieuwe account maken voor elke toegevoegde alias hebt ingeschakeld,

worden er nieuwe accounts toegevoegd voor gebruikers zonder BI-platformaccount of voor alle gebruikers.

- *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
  Selecteer deze optie als de rol die u wilt toewijzen veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van BI-platform. Het platform maakt niet automatisch aliassen en accounts voor de gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers wanneer ze zich voor het eerst bij BI-platform aanmelden. Dit is de standaardoptie.

9. Geef in het gedeelte *Opties voor nieuwe gebruiker* op hoe nieuwe gebruikers worden gemaakt.

   Selecteer een van de volgende opties:

   - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

     > **Opmerking**
     >
     > Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
     >
     > Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

   - *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot BI-platform, kan een licentie voor gelijktijdige toegang bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

   De rollen die u hebt geselecteerd, verschijnen nu als groepen in BI-platform.

9.6.3.2 Overweging bij opnieuw toewijzen

Als u gebruikers toevoegt aan een rol die al is toegewezen aan BI-platform, moet u de rol opnieuw toewijzen om de gebruikers toe te voegen aan BI-platform. Wanneer u de rol opnieuw toewijst, is de optie om gebruikers toe te wijzen als gebruikers op naam of gelijktijdige gebruikers alleen van invloed op de nieuwe gebruikers die u toevoegt aan de rol.

U wijst een rol bijvoorbeeld in eerste instantie toe aan BI-platform met de optie *Nieuwe gebruikers worden gemaakt als gebruikers op naam*. Later voegt u gebruikers aan dezelfde rol toe en wijst u de rol opnieuw toe met de optie Nieuwe gebruikers worden gemaakt als *gelijktijdige* gebruikers.

In dit geval worden alleen de nieuwe gebruikers in de rol toegewezen aan BI-platform als gelijktijdige gebruikers. De gebruikers die al zijn toegewezen, blijven gebruikers op naam. Hetzelfde geldt wanneer u gebruikers eerst

toewijst als gelijktijdige gebruikers en vervolgens de instellingen wijzigt om nieuwe gebruikers opnieuw toe te wijzen als gebruikers op naam.

9.6.3.3 De toewijzing van een rol ongedaan maken

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik op *Verificatie*.
3. Klik op *PeopleSoft Enterprise*.
4. Klik op *Rollen*.
5. Selecteer de rol die u wilt verwijderen en klik op <.
6. Klik op *Bijwerken*.

   De leden van de rol hebben geen toegang meer tot BI-platform, tenzij ze andere accounts of aliassen hebben.

   > ⓘ Opmerking
   >
   > U kunt ook afzonderlijke accounts verwijderen of gebruikers uit rollen verwijderen voordat u ze toewijst aan BI-platform, om te voorkomen dat bepaalde gebruikers zich aanmelden.

9.6.4 Gebruikersupdates plannen

U kunt regelmatige gebruikersupdates plannen om ervoor te zorgen dat wijzigingen van uw gebruikersgegevens voor uw ERP-systeem worden weergegeven in uw BI-platformgebruikersgegevens. Deze updates synchroniseren automatisch uw ERP- en BI-platformgebruikers volgens de toewijzingsinstellingen die u hebt geconfigureerd in de CMC (Central Management Console).

Er bestaan twee opties voor het uitvoeren en plannen van updates voor geïmporteerde rollen:

- Alleen rollen bijwerken: met deze optie worden alleen de koppelingen bijgewerkt tussen de rollen die momenteel zijn toegewezen en die in het BI-platform zijn geïmporteerd. Gebruik deze optie als u verwacht regelmatig updates uit te voeren, en u zich zorgen maakt over gebruik van systeembronnen. Er worden geen nieuwe gebruikersaccounts gemaakt als u alleen rollen bijwerkt.
- Rollen en aliassen bijwerken: met deze optie worden niet alleen koppelingen tussen rollen bijgewerkt, maar worden ook nieuwe gebruikersaccounts gemaakt in het BI-platform voor nieuwe gebruikersaliassen die zijn toegevoegd aan het ERP-systeem.

> ⓘ Opmerking
>
> Als u niet hebt opgegeven dat gebruikersaliassen automatisch worden gemaakt voor updates wanneer u verificatie hebt ingeschakeld, worden er geen accounts gemaakt voor nieuwe aliassen.

9.6.4.1 Gebruikersupdates plannen

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem deze rollen moet bijwerken.

1. Klik op het tabblad *Gebruikersupdate*.
2. Klik op *Plannen* in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

   > → Tip
   >
   > Klik op *Nu bijwerken* als u meteen een update wilt uitvoeren.

   > → Tip
   >
   > Gebruik de optie *Alleen rollen bijwerken* als u regelmatig wilt bijwerken en u zich zorgen maakt over systeembronnen. Het systeem doet er langer over om zowel rollen als aliassen bij te werken.

   Nu wordt het dialoogvenster *Terugkeerpatroon* weergegeven.
3. Selecteer een optie in de lijst *Object uitvoeren* en geef alle gevraagde planningsgegevens op.

   Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U kunt het tijdstip waarop het object wordt gestart, en een begin- en einddatum opgeven.
Dagelijks	De update wordt elke dag of om het opgegeven aantal dagen uitgevoerd. U kunt het tijdstip opgeven waarop het object wordt uitgevoerd, plus een begin- en einddatum.
Wekelijks	De update wordt elke week uitgevoerd. Het kan eenmaal of verschillende keren per week worden uitgevoerd. U kunt de dagen en het tijdstip waarop het object wordt uitgevoerd, en een begin- en einddatum opgeven.
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
Dag N van elke maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Op de Ne X van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.

Terugkeerpatroon	Beschrijving
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

4. Klik op *Plannen* nadat u de planningsgegevens heb ingevoerd.
   De datum van de volgende geplande rolupdate wordt weergegeven op het tabblad *Gebruikersupdate*.

> ⓘ Opmerking
>
> U kunt altijd de volgende geplande update annuleren door op *Geplande updates annuleren* te klikken in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

9.6.5 De PeopleSoft Security Bridge gebruiken

Met de Security Bridge-functie van het BI-platform kunt u PeopleSoft EPM-beveiligingsinstellingen importeren in het BI-platform.

Security Bridge werkt in twee modi:

- **Configuratiemodus**
  In de configuratiemodus biedt Security Bridge een interface waarmee u een antwoordbestand kunt maken. Met dit antwoordbestand wordt het gedrag van Security Bridge tijdens de uitvoeringsmodus geregeld.
- **Uitvoeringsmodus**
  Op basis van de parameters die u definieert in het antwoordbestand, importeert Security Bridge de beveiligingsinstellingen van dimensietabellen in PeopleSoft EPM naar universes in het BI-platform.

9.6.5.1 Beveiligingsinstellingen importeren

Als u beveiligingsinstellingen wilt importeren, moet u de volgende taken uitvoeren om:

- De objecten te definiëren die Security Bridge moet beheren.
- Een antwoordbestand te maken.
- De toepassing Security Bridge uit te voeren.

Zie Beveiligingsinstellingen beheren [pagina 371] voor meer informatie over het beheren van de beveiliging nadat u de instellingen hebt geïmporteerd.

9.6.5.1.1 Beheerde objecten definiëren

Voordat u Security Bridge uitvoert, is het belangrijk om de objecten vast te leggen die door de toepassing worden beheerd. Security Bridge beheert een of meer PeopleSoft-rollen, een BI-platformgroep en een of meer universes.

- Beheerde PeopleSoft-rollen

Dit zijn rollen in uw PeopleSoft-systeem. Leden van deze rollen werken met PeopleSoft-gegevens via PeopleSoft EPM. U moet de rollen kiezen die de leden bevatten voor wie u toegangsrechten tot de beheerde universes in het BI-platform wilt aanbieden/bijwerken.
De toegangsrechten die worden gedefinieerd voor de leden van deze rollen zijn gebaseerd op hun rechten in PeopleSoft EPM; Security Bridge importeert deze beveiligingsinstellingen in het BI-platform.

- Beheerde BI-platformgroep
  Wanneer u Security Bridge uitvoert, maakt het programma een gebruiker aan in het BI-platform voor elk lid van een beheerde PeopleSoft-rol.
  De groep waarin de gebruikers worden gemaakt, is de beheerde BI-platformgroep. Leden van deze groep zijn gebruikers van wie de toegangsrechten tot de beheerde universes worden bijgehouden door de Security Bridge. Omdat de gebruikers worden gemaakt in één groep, kunt u Security Bridge zodanig configureren dat de beveiligingsinstellingen niet worden bijgewerkt voor bepaalde gebruikers, door eenvoudigweg gebruikers te verwijderen uit de beheerde BI-platformgroep.
  Voordat u Security Bridge uitvoert, moet u een groep kiezen in het BI-platform die de locatie moet worden waarin de gebruikers worden aangemaakt. Als u een groep opgeeft die niet bestaat, wordt de groep door Security Bridge gemaakt in het BI-platform.
- Beheerde universes
  Beheerde universes zijn de universes waarin Security Bridge beveiligingsinstellingen vanuit PeopleSoft EPM importeert. Uit de universes die worden opgeslagen in uw BI-platformsysteem, moet u kiezen welke moeten worden beheerd door Security Bridge. Leden van beheerde PeopleSoft-rollen die ook lid zijn van de beheerde BI-platformgroep, kunnen geen gegevens opvragen via deze universes waartoe zij geen toegang hebben vanuit PeopleSoft EPM.

9.6.5.1.2 Een antwoordbestand maken

1. Ga naar de map die u hebt opgegeven tijdens het installeren van de beveiligingsbrug en voer het bestand `crpsepmsecuritybridge.bat` (in Windows) en `crpsempsecuritybridge.sh` (in UNIX) uit.

   > **Opmerking**
   >
   > In Windows is deze locatie standaard `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

   Het dialoogvenster Beveiligingsbrug voor PeopleSoft EPM wordt weergegeven.
2. Selecteer *Nieuw* om een antwoordbestand te maken of selecteer *Openen* en klik op *Bladeren* om een antwoordbestand op te geven dat u wilt wijzigen. Selecteer de gewenste taal voor het bestand.
3. Klik op *Volgende*.
4. Geef de locaties van de *PeopleSoft EPM SDK* en *BI-platform SDK* op.

   > **Opmerking**
   >
   > De PeopleSoft EPM SDK bevindt zich gewoonlijk op de PeopleSoft-server in `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

   > **Opmerking**
   >
   > De BI-platform SDK bevindt zich gewoonlijk op `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.

5. Klik op *Volgende*.

   In het dialoogvenster wordt informatie over de verbinding en het stuurprogramma opgevraagd voor de PeopleSoft-database.

6. Selecteer in de lijst Database het gewenste type database en verstrek de informatie voor de volgende velden:

Veld	Beschrijving
Database	De naam van de PeopleSoft-database.
Host	De naam van de server die fungeert als host voor de database.
Poortnummer	Het poortnummer voor toegang tot de server.
Klasselocatie	De locatie van de klassebestanden voor het databasestuurprogramma.
Gebruikersnaam	Uw gebruikersnaam
Wachtwoord	Uw wachtwoord.

7. Klik op *Volgende*.

   In het dialoogvenster wordt een lijst weergegeven van alle klassen die Security Bridge gebruikt bij het uitvoeren. U kunt desgewenst klassen toevoegen aan of verwijderen uit de lijst.

8. Klik op *Volgende*.

   Het dialoogvenster vraagt u om verbindingsinformatie voor het BI-platform.

9. Verstrek de desbetreffende informatie voor de volgende velden:

Veld	Beschrijving
Server	De naam van de server waar de CMS (Central Management Server) zich bevindt.
Gebruikersnaam	Uw gebruikersnaam
Wachtwoord	Uw wachtwoord.
Verificatie	Uw type verificatie.

10. Klik op *Volgende*.
11. Kies een BI-platformgroep en klik op *Volgende*.

    > **Opmerking**
    >
    > De groep die u opgeeft in dit veld is de locatie waar Security Bridge gebruikers maakt voor de leden van de beheerde PeopleSoft-rollen.

    > **Opmerking**
    >
    > Als u een groep opgeeft die nog niet bestaat, wordt deze door Security Bridge gemaakt.

    In het dialoogvenster wordt een lijst van rollen weergegeven uit uw PeopleSoft-systeem.

12. Selecteer de optie *Geïmporteerd* voor de rollen die u de beveiligingsbrug wilt laten beheren en klik op *Volgende*.

> **Opmerking**
>
> De Security Bridge maakt een gebruiker aan in de beheerde groep in het BI-platform (die u in de vorige stap hebt opgegeven) voor elk lid van de rol(len) die u selecteert.

Het dialoogvenster geeft een lijst met universes weer in het BI-platform.

13. Selecteer de universe(s) waarin u Security Bridge beveiligingsinstellingen wilt laten importeren en klik op *Volgende*.
14. Geef een bestandsnaam op voor het Security Bridge-logbestand en een locatie waar het logbestand moet worden opgeslagen. U kunt aan de hand van het logbestand bepalen of Security Bridge al dan niet met succes de beveiligingsinstellingen uit PeopleSoft EPM heeft geïmporteerd.
15. Klik op *Volgende*.

    Het dialoogvenster geeft een voorbeeld weer van het antwoordbestand dat Security Bridge zal gebruiken tijdens de uitvoeringsmodus.
16. Klik op *Opslaan* en kies een locatie waar u het antwoordbestand wilt opslaan.
17. Klik op *Volgende*.

    U hebt met succes het antwoordbestand voor Security Bridge gemaakt.
18. Klik op *Afsluiten*.

> **Opmerking**
>
> Het antwoordbestand is een Java-eigenschappenbestand dat u ook handmatig kunt maken en/of wijzigen. Zie de sectie “PeopleSoft-antwoordbestand” voor meer informatie.

9.6.5.2 De beveiligingsinstellingen toepassen

Voer het batchbestand `crpsepmsecuritybridge.bat` (in Windows) of `crpsempsecuritybridge.sh` (in Unix) uit en gebruik het antwoordbestand dat u als argument hebt gemaakt als u de beveiligingsinstellingen wilt toepassen. Typ bijvoorbeeld**`crpsepmsecuritybridge.bat myresponsefile.properties`** in Windows of**`crpsempsecuritybridge.sh myresponsefile.properties`** in Unix.

De toepassing Security Bridge wordt uitgevoerd. Hiermee worden gebruikers aangemaakt in het BI-platform voor de leden van de PeopleSoft-rollen die u hebt opgegeven in het antwoordbestand, en worden de beveiligingsinstellingen uit PeopleSoft EPM naar de desbetreffende universes geïmporteerd.

9.6.5.2.1 Toewijzingsoverwegingen

In de uitvoermodus maakt Security Bridge een gebruiker aan in het BI-platform voor elk lid van een beheerde PeopleSoft-rol.

De gebruikers worden gemaakt met uitsluitend Enterprise-verificatiealiassen en het BI-platform wijst aan deze gebruikers willekeurig wachtwoorden toe. Als gevolg hiervan kunnen gebruikers zich pas bij het BI-platform aanmelden wanneer de systeembeheerder handmatig nieuwe wachtwoorden heeft toegewezen of de rol(len)

aan het BI-platform heeft toegewezen via de PeopleSoft-beveiligingsinvoegtoepassing om gebruikers in staat te stellen zich aan te melden met hun PeopleSoft-referenties.

9.6.5.3 Beveiligingsinstellingen beheren

U kunt de beveiligingsinstellingen beheren die u hebt toegepast door de objecten te wijzigen die worden beheerd door Security Bridge.

9.6.5.3.1 Beheerde gebruikers

Security Bridge beheert gebruikers op basis van de volgende criteria:

- Of de gebruiker al dan niet lid is van een beheerde PeopleSoft-rol.
- Of de gebruiker lid is van de beheerde BI-platformgroep.

Als u een gebruiker in staat wilt stellen PeopleSoft-gegevens op te vragen via universes in het BI-platform, moet u ervoor zorgen dat de gebruiker lid is van *zowel* een beheerde PeopleSoft-rol als de beheerde groep in het BI-platform.

- Voor leden van beheerde PeopleSoft-rollen die geen accounts hebben in het BI-platform, maakt Security Bridge accounts aan en wijst hier willekeurige wachtwoorden aan toe. De systeembeheerder moet bepalen of handmatig al dan niet nieuwe wachtwoorden worden toegewezen of om de rollen toe te wijzen aan het BI-platform via de PeopleSoft-beveiligingsinvoegtoepassing om gebruikers in staat te stellen zich aan te melden bij het BI-platform.
- Voor leden van beheerde PeopleSoft-rollen die ook lid zijn van de beheerde BI-platformgroep, werkt Security Bridge de beveiligingsinstellingen bij die worden toegepast op de gebruikers, zodat zij de desbetreffende gegevens kunnen opvragen uit de beheerde universes.

Als een lid van een beheerde PeopleSoft-rol een bestaande account heeft in BI-platform, maar *geen* lid is van de beheerde BI-platformgroep, werkt Security Bridge de beveiligingsinstellingen die op de gebruiker van toepassing zijn *niet* bij. Deze situatie doet zich gewoonlijk alleen voor wanneer de systeembeheerder handmatig gebruikersaccounts verwijdert die zijn gemaakt door Security Bridge vanuit de beheerde BI-platformgroep.

> **Opmerking**
>
> Dit is een effectieve methode voor het beheren van de beveiliging: door gebruikers te verwijderen uit de beheerde BI-platformgroep kunt u hun beveiligingsinstellingen configureren op een afwijkende manier van de beveiligingsinstellingen die zij hebben in PeopleSoft.

Omgekeerd, als een lid van de beheerde BI-platformgroep *geen* lid van een beheerde PeopleSoft-rol is, geeft Security Bridge hun *geen* toegang tot de beheerde universes. Deze situatie doet zich gewoonlijk alleen voor wanneer PeopleSoft-systeembeheerders gebruikers verwijderen die eerder door Security Bridge zijn toegewezen aan het BI-platform vanuit de beheerde PeopleSoft-rol(len).

> **Opmerking**
>
> Dit is een andere methode voor het beheren van de beveiliging: door gebruikers te verwijderen uit beheerde PeopleSoft-rollen kunt u ervoor zorgen dat de gebruikers geen toegang tot gegevens hebben vanuit PeopleSoft.

9.6.5.3.2 Beheerde universes

Security Bridge beheert universes via beperkingensets, waarmee de gegevens die beheerde gebruikers kunnen opvragen vanuit beheerde universes worden beperkt.

Beperkingensets zijn groepen beperkingen (bijvoorbeeld beperkingen ten aanzien van query-besturing, genereren van SQL, enzovoort). Door Security Bridge worden beperkingen ten aanzien van rijtoegang en objecttoegang toegepast/bijgewerkt voor de beheerde universes:

- Rijtoegangsbeperkingen worden toegepast op dimensietabellen die zijn gedefinieerd in PeopleSoft EPM. Deze beperkingen zijn gebruikersspecifiek en kunnen worden geconfigureerd op een van de volgende instellingen:
  - De gebruiker kan alle gegevens opvragen.
  - De gebruiker kan geen gegevens opvragen.
  - De gebruiker kan gegevens opvragen op basis van de toegangsrechten op rijniveau in PeopleSoft, die worden uitgedrukt via de Security Join Tables (SJT) die zijn gedefinieerd in PeopleSoft EPM.
- Objecttoegangsbeperkingen worden toegepast om objecten te meten op basis van de velden die worden opgevraagd door de meetwaardeobjecten.
  Als een meetwaardeobject velden opvraagt die zijn gedefinieerd als gegevens in PeopleSoft, dan kan het opvragen van het meetwaardeobject worden toegestaan/geweigerd afhankelijk van of de gebruiker al dan niet de gegevens waarnaar wordt verwezen in PeopleSoft kan opvragen. Als een gebruiker geen van de gegevens kan opvragen, wordt het opvragen van het meetwaardeobject geweigerd. Als de gebruiker alle gegevens kan opvragen, wordt het opvragen van het meetwaardeobject toegestaan.

Als systeembeheerder kunt u ook de gegevens die gebruikers kunnen opvragen vanuit uw PeopleSoft-systeem beperken door het aantal universes dat wordt beheerd door Security Bridge te beperken.

9.6.5.4 PeopleSoft-antwoordbestand

De functie Security Bridge van het BI-platform werkt op basis van de instellingen die u opgeeft in een antwoordbestand.

U genereert gewoonlijk een antwoordbestand met de interface die wordt aangeboden door Security Bridge in de configuratiemodus. Maar omdat het bestand een Java-eigenschappenbestand is, kunt u het ook handmatig maken of wijzigen.

Deze bijlage bevat informatie over de parameters die u in het antwoordbestand moet opnemen als u dit handmatige wilt genereren.

> **Opmerking**
>
> Wanneer u het bestand maakt, moet u letten op de ontsnappingsvereiste van het Java-eigenschappenbestand (voor ':' is bijvoorbeeld de ontsnapping '\:').

9.6.5.4.1 Antwoordbestandparameters

In de volgende tabel worden de parameters beschreven die deel uitmaken van het antwoordbestand:

Parameter	Beschrijving
klassenpad	Het klassepad voor het laden van de benodigde .jar-bestanden. Meerdere klassepaden moeten zowel in Windows als in UNIX van elkaar worden gescheiden door een ';'. De klassepaden die nodig zijn, zijn voor de `com.peoplesoft.epm.pf.jar` en de .jar-bestanden van het JDBC-stuurprogramma.
db.driver.name	De naam van het JDBC-stuurprogramma dat wordt gebruikt om verbinding te maken met de PeopleSoft-database (bijvoorbeeld `com.microsoft.jdbc.sqlserver.SQLServerDriver`).
db.connect.str	De JDBC-verbindingstekenreeks die wordt gebruikt om een verbinding te maken met de PeopleSoft-database (bijvoorbeeld `jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO`)
db.user.name	De gebruikersnaam voor aanmelding bij de PeopleSoft-database.
db.password	Het wachtwoord voor aanmelding bij de PeopleSoft-database.
db.password.encrypted	De waarde voor deze parameter bepaalt of de wachtwoordparameter in het antwoordbestand al dan niet wordt gecodeerd. De waarde kan worden ingesteld op True of False. (Als er geen waarde wordt opgegeven, wordt deze standaard False.)
enterprise.cms.name	De CMS waarin de universes zich bevinden.
enterprise.user.name	De gebruikersnaam voor aanmelding bij de CMS.
enterprise.password	Het wachtwoord voor aanmelding bij de CMS.

Parameter	Beschrijving
enterprise.password.encrypted	De waarde voor deze parameter bepaalt of de wachtwoordparameter in het antwoordbestand al dan niet wordt gecodeerd. De waarde kan worden ingesteld op True of False. (Als er geen waarde wordt opgegeven, wordt deze standaard False.)
enterprise.authMethod	Het verificatiemethode voor aanmelding bij de CMS.
enterprise.role	De beheerde BI-platformgroep. Zie Beheerde objecten definiëren [pagina 367] voor meer informatie.
enterprise.license	Controleert het licentietype wanneer u gebruikers uit PeopleSoft importeert. "0" stelt de gebruikerslicentie op naam in, "1" stelt de licentie voor gelijktijdige toegang in.
peoplesoft.role.n	De lijst van beheerde PeopleSoft-rollen. Zie Beheerde objecten definiëren [pagina 367] voor meer informatie. **<n>** is een geheel getal, en elk item bezit een eigenschap met het voorvoegsel peoplesoft.role. **Opmerking** **<n>** is op 1 gebaseerd. U kunt '*' gebruiken om alle beschikbare PeopleSoft-rollen aan te geven, gegeven dat n is 1 en het de enige eigenschap is die peoplesoft.role als prefix heeft in het antwoordbestand.
mapped.universe.n	De lijst van universes die u door Security Bridge wilt laten bijwerken. Zie Beheerde objecten definiëren [pagina 367] voor meer informatie. **<n>** is een geheel getal, en elk item bezit een eigenschap met het voorvoegsel mapped.universe. **Opmerking** **<n>** is op 1 gebaseerd. U kunt '*' gebruiken om alle beschikbare universes aan te geven, gegeven dat n is 1 en het de enige eigenschap is die mapped.universe als prefix heeft in het antwoordbestand.
log4j.appender.file.File	Het logbestand dat wordt geschreven door Security Bridge.

Parameter	Beschrijving
log4j.*	Standaard log4j-eigenschappen die nodig zijn om log4j naar behoren te laten functioneren: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.Pattern-Layout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	Het klassepad naar de .jar-bestanden van PeopleSoft EPM API. Deze parameter is optioneel.
enterprise.classpath	Het klassepad naar de JAR-bestanden van BI-platform SDK. Deze parameter is optioneel.
db.driver.type	Het type PeopleSoft-database. Deze parameter kan een van de volgende waarden hebben: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Aangepast Aangepast kan worden gebruikt om andere databases op te geven dan de herkende typen of versies. Deze parameter is optioneel.

Parameter	Beschrijving
sql.db.class.location sql.db.host sql.db.port sql.db.database	De locatie van de .jar-bestanden van het JDB-stuurprogramma van SQL Server, de hostcomputer voor SQL Server, de poort voor SQL Server en de databasenaam van SQL Server. Deze parameters kunnen alleen worden gebruikt als db.driver.type de waarde Microsoft SQL Server 2000 heeft. Deze parameters zijn optioneel.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	De locatie van de .jar-bestanden van het JDBC-stuurprogramma voor Oracle, de hostcomputer voor de Oracle-database, de poort voor de Oracle-database en de SID van de Oracle-database. Deze parameters kunnen alleen worden gebruikt als db.driver.type de waarde Oracle Database 10.1 heeft. Deze parameters zijn optioneel.
db2.db.class.location db2.db.host db2.db.port db2.db.sid	De locatie van de .jar-bestanden van het JDBC-stuurprogramma voor DB2, de hostcomputer voor de DB2-database, de poort voor de DB2-database en de SID van de DB2-database. Deze parameters kunnen alleen worden gebruikt als db.driver.type de waarde DB2 UDB 8.2 Fixpack 7 heeft Deze parameters zijn optioneel.
custom.db.class.location custom.db.drivername custom.db.connectStr	De locatie, naam en verbindingstekenreeks van het aangepaste JDBC-stuurprogramma. Deze parameters kunnen alleen worden gebruikt als db.driver.type de waarde Custom heeft. Deze parameters zijn optioneel.

9.7 JD Edwards-verificatie

9.7.1 Overzicht

Als u uw JD Edwards-gegevens met BI-platform wilt gebruiken, moet u het systeem van informatie voorzien over uw JD Edwards-implementatie. Met deze informatie kunnen gebruikers worden geverifieerd door BI-platform, zodat ze hun JD Edwards EnterpriseOne-referenties kunnen gebruiken om zich bij het BI-platform aan te melden.

9.7.2 JD Edwards EnterpriseOne-verificatie inschakelen

Het BI-platform moet weten hoe verificatie voor uw JD Edwards EnterpriseOne-systeem verloopt om JD Edwards EnterpriseOne-gegevens te kunnen gebruiken.

9.7.2.1 JD Edwards-verificatie inschakelen in het BI-platform

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied Beheren op *Verificatie*.
3. Dubbelklik op *JD Edwards EnterpriseOne*.
   De pagina *JD Edwards EnterpriseOne* verschijnt.
4. Schakel op het tabblad *Opties* het selectievakje *JD Edwards EnterpriseOne-verificatie inschakelen* in.
5. Maak de gewenste wijzigingen onder *Nieuwe alias*, *Bijwerkopties* en *Opties voor nieuwe gebruiker* volgens uw BI-platformimplementatie. Klik op *Bijwerken* om de wijzigingen op te slaan voordat u naar het tabblad *Systemen* gaat.
6. Klik op het tabblad *Servers*.
7. Kopieer `jdeutil.jar`, `kernel.jar` en `log4j.jar` van de JD Edwards-installatie naar deze locaties (op Windows): `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` and `<INSTALLDIR>\Tomcat\lib\`.
8. Start Tomcat en de Server Intelligence Agent opnieuw.
9. In het gebied *JD Edwards EnterpriseOne-systeemgebruiker* typt u een databasegebruikersnaam en -wachtwoord waarmee BI-platform zich bij uw JD Edwards EnterpriseOne-database kan aanmelden.
10. In het gebied *JD Edwards EnterpriseOne-domein* voert u de naam, host en poort in voor verbinding met uw JD Edwards EnterpriseOne-omgeving.
11. Voer een naam voor de omgeving in en klik op *OK*.
12. Klik op *Bijwerken* om de wijzigingen op te slaan.

9.7.3 JD Edwards EnterpriseOne-rollen toewijzen aan het BI-platform

BI-platform maakt automatisch een groep voor elke JD Edwards EnterpriseOne-rol die u toewijst. Daarnaast maakt het systeem aliassen voor de leden van de toegewezen JD Edwards EnterpriseOne-rollen.

U kunt een gebruikersaccount maken voor elke gemaakte alias.

Als u echter meerdere systemen uitvoert en de gebruikers accounts hebben in meer dan een systeem, kunt u iedere gebruiker toewijzen aan een alias met dezelfde naam voordat u de accounts maakt in BI-platform.

Op deze manier hoeft u minder accounts voor dezelfde gebruiker te maken in BI-platform.

Als u bijvoorbeeld een JD Edwards EnterpriseOne-testomgeving uitvoert en 30 van uw gebruikers toegang hebben tot beide systemen, worden er slechts 30 accounts gemaakt voor die gebruikers. Als u niet iedere

gebruiker toewijst aan een alias met dezelfde naam, worden er 60 accounts voor 30 gebruikers gemaakt in het BI-platform.

Als u echter meerdere systemen uitvoert waarbij gebruikersnamen elkaar overlappen, moet u een nieuwe lidaccount maken voor elke gemaakte alias.

Als u bijvoorbeeld uw testomgeving met een gebruikersaccount voor Russell Aquino (gebruikersnaam 'raquino') uitvoert en de productieomgeving met een gebruikersaccount voor Raoul Aquino (gebruikersnaam 'raquino'), moet u een afzonderlijke account voor de alias van iedere gebruiker maken. Doet u dit niet, dan worden de twee gebruikers aan dezelfde BI-platformaccount toegevoegd, en kunnen ze zich niet bij BI-platform aanmelden met hun eigen JD Edwards EnterpriseOne-referenties.

9.7.3.1 Een JD Edwards EnterpriseOne-rol toewijzen

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied *Beheren* op *Verificatie*.
3. Dubbelklik op *JD Edwards EnterpriseOne*.
4. Selecteer in het gebied *Opties voor nieuwe alias* een van de volgende opties:
   - *Elke toegevoegde alias toewijzen aan een account met dezelfde naam*
     Selecteer deze optie als u meerdere JD Edwards EnterpriseOne-systemen hebt met gebruikers die accounts hebben op meerdere systemen (waarbij geen twee gebruikers dezelfde gebruikersnaam voor verschillende systemen hebben).
   - *Een nieuwe account maken voor elke toegevoegde alias*
     Selecteer deze optie als u slechts één JD Edwards EnterpriseOne-systeem hebt, als de meerderheid van de gebruikers accounts heeft op slechts een van uw systemen, of als de gebruikersnamen voor verschillende gebruikers elkaar overlappen op twee of meer systemen.
5. Selecteer in het gebied *Bijwerkopties* een van de volgende opties:
   - *Er worden nieuwe aliassen toegevoegd en nieuwe gebruikers gemaakt*.
     Selecteer deze optie als u een nieuwe alias wilt maken voor iedere gebruiker die is toegewezen aan BI-platform. Als u de optie Een nieuwe account maken voor elke toegevoegde alias hebt ingeschakeld, worden er nieuwe accounts toegevoegd voor gebruikers zonder BI-platformaccount of voor alle gebruikers.
   - *Er worden geen nieuwe aliassen toegevoegd en geen nieuwe gebruikers gemaakt*.
     Selecteer deze optie als de rol die u wilt toewijzen veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van BI-platform. Het systeem maakt niet automatisch aliassen en accounts voor de gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers wanneer ze zich voor het eerst bij BI-platform aanmelden. Dit is de standaardoptie.
6. Geef in het gedeelte *Opties voor nieuwe gebruiker* op hoe nieuwe gebruikers worden gemaakt.

   Selecteer een van de volgende opties:
   - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

> **Opmerking**
>
> Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot BI-platform, kan een licentie voor gelijktijdige toegang bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

De rollen die u hebt geselecteerd, verschijnen nu als groepen in BI-platform.

7. Klik op het tabblad *Rollen*.
8. Selecteer onder *Domeinlijst* de JD Edwards-server met de rollen die u wilt toewijzen.
9. Selecteer onder *Beschikbare rollen* de rollen die u aan het BI-platform wilt toewijzen en klik op <.
10. Klik op *Bijwerken*.
    De rollen worden aan BI-platform toegewezen.

9.7.3.2 Overweging bij opnieuw toewijzen

Als u gebruikers toevoegt aan een rol die al is toegewezen aan BI-platform, moet u de rol opnieuw toewijzen om de gebruikers toe te voegen aan BI-platform. Wanneer u de rol opnieuw toewijst, is de optie om gebruikers toe te wijzen als gebruikers op naam of gelijktijdige gebruikers alleen van invloed op de nieuwe gebruikers die u toevoegt aan de rol.

U wijst een rol bijvoorbeeld in eerste instantie toe aan BI-platform met de optie *Nieuwe gebruikers worden gemaakt als gebruikers op naam*. Later voegt u gebruikers aan dezelfde rol toe en wijst u de rol opnieuw toe met de optie Nieuwe gebruikers worden gemaakt als *gelijktijdige* gebruikers.

In dit geval worden alleen de nieuwe gebruikers in de rol toegewezen aan BI-platform als gelijktijdige gebruikers. De gebruikers die al zijn toegewezen, blijven gebruikers op naam. Hetzelfde geldt wanneer u gebruikers eerst toewijst als gelijktijdige gebruikers en vervolgens de instellingen wijzigt om nieuwe gebruikers opnieuw toe te wijzen als gebruikers op naam.

9.7.3.3 De toewijzing van een rol ongedaan maken

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied *Beheren* op *Verificatie*.
3. Klik op het tabblad voor *JD Edwards EnterpriseOne*.

4. Selecteer in het gebied *Rollen* de rol die u wilt verwijderen en klik op <.
5. Klik op *Bijwerken*.

   De leden van de rol hebben geen toegang meer tot BI-platform, tenzij ze andere accounts of aliassen hebben.

   > ⓘ Opmerking
   >
   > U kunt ook afzonderlijke accounts verwijderen of gebruikers uit rollen verwijderen voordat u ze toewijst aan BI-platform, om te voorkomen dat bepaalde gebruikers zich aanmelden.

9.7.4 Gebruikersupdates plannen

U kunt regelmatige gebruikersupdates plannen om ervoor te zorgen dat wijzigingen van uw gebruikersgegevens voor uw ERP-systeem worden weergegeven in uw BI-platformgebruikersgegevens. Deze updates synchroniseren automatisch uw ERP- en BI-platformgebruikers volgens de toewijzingsinstellingen die u hebt geconfigureerd in de CMC (Central Management Console).

Er bestaan twee opties voor het uitvoeren en plannen van updates voor geïmporteerde rollen:

- Alleen rollen bijwerken: met deze optie worden alleen de koppelingen bijgewerkt tussen de rollen die momenteel zijn toegewezen en die in het BI-platform zijn geïmporteerd. Gebruik deze optie als u verwacht regelmatig updates uit te voeren, en u zich zorgen maakt over gebruik van systeembronnen. Er worden geen nieuwe gebruikersaccounts gemaakt als u alleen rollen bijwerkt.
- Rollen en aliassen bijwerken: met deze optie worden niet alleen koppelingen tussen rollen bijgewerkt, maar worden ook nieuwe gebruikersaccounts gemaakt in het BI-platform voor nieuwe gebruikersaliassen die zijn toegevoegd aan het ERP-systeem.

> ⓘ Opmerking
>
> Als u niet hebt opgegeven dat gebruikersaliassen automatisch worden gemaakt voor updates wanneer u verificatie hebt ingeschakeld, worden er geen accounts gemaakt voor nieuwe aliassen.

9.7.4.1 Gebruikersupdates plannen

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem deze rollen moet bijwerken.

1. Klik op het tabblad *Gebruikersupdate*.
2. Klik op *Plannen* in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

   > → Tip
   >
   > Klik op *Nu bijwerken* als u meteen een update wilt uitvoeren.

> → Tip
>
> Gebruik de optie *Alleen rollen bijwerken* als u regelmatig wilt bijwerken en u zich zorgen maakt over systeembronnen. Het systeem doet er langer over om zowel rollen als aliassen bij te werken.

Nu wordt het dialoogvenster *Terugkeerpatroon* weergegeven.

3. Selecteer een optie in de lijst *Object uitvoeren* en geef alle gevraagde planningsgegevens op.

   Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U kunt het tijdstip waarop het object wordt gestart, en een begin- en einddatum opgeven.
Dagelijks	De update wordt elke dag of om het opgegeven aantal dagen uitgevoerd. U kunt het tijdstip opgeven waarop het object wordt uitgevoerd, plus een begin- en einddatum.
Wekelijks	De update wordt elke week uitgevoerd. Het kan eenmaal of verschillende keren per week worden uitgevoerd. U kunt de dagen en het tijdstip waarop het object wordt uitgevoerd, en een begin- en einddatum opgeven.
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
Dag N van elke maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Op de Ne X van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

4. Klik op *Plannen* nadat u de planningsgegevens heb ingevoerd.
   De datum van de volgende geplande rolupdate wordt weergegeven op het tabblad *Gebruikersupdate*.

> ⓘ Opmerking
>
> U kunt altijd de volgende geplande update annuleren door op *Geplande updates annuleren* te klikken in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

9.8 Siebel-verificatie

9.8.1 Siebel-verificatie inschakelen

U kunt het BI-platform gebruik laten maken van Siebel-informatie door informatie te geven over verificatie in uw Siebel-systeem.

9.8.1.1 Siebel-verificatie inschakelen in het BI-platform

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied Beheren op *Verificatie*.
3. Dubbelklik op *Siebel*.
   De pagina *Siebel* wordt weergegeven. Deze heeft vier tabbladen: *Opties*, *Systemen*, *Verantwoordelijkheden* en *Gebruikersupdate*.
4. Op het tabblad *Opties* selecteert u het vakje *Siebel-verificatie inschakelen*.
5. Maak de gewenste wijzigingen onder *Nieuwe alias*, *Bijwerkopties* en *Opties voor nieuwe gebruiker* volgens uw BI-platformimplementatie. Klik op *Bijwerken* om de wijzigingen op te slaan voordat u naar het tabblad *Systemen* gaat.
6. Klik op het tabblad *Domeinen*.
7. Voer in het veld *Domeinnaam* de domeinnaam in voor het Siebel-systeem waarmee u verbinding wilt maken.
8. Voer onder *Verbinding* de verbindingsreeks voor dat domein in.
9. In het gebied *Gebruikersnaam* typt u een databasegebruikersnaam en -wachtwoord waarmee BI-platform zich bij uw Siebel-database moet aanmelden.
10. Voer in het gebied *Wachtwoord* het wachtwoord in voor de gebruiker die u hebt geselecteerd.
11. Klik op *Toevoegen* om de systeemgegevens toe te voegen aan de lijst *Huidige domeinen*.
12. Klik op *Bijwerken* om de wijzigingen op te slaan.

9.8.2 Rollen toewijzen aan het BI-platform

BI-platform maakt automatisch een groep voor elke Siebel-rol die u toewijst. Daarnaast maakt het programma aliassen voor de leden van de toegewezen Siebel-rollen.

U kunt een gebruikersaccount maken voor elke gemaakte alias.

Als u echter meerdere systemen uitvoert en de gebruikers accounts hebben in meer dan een systeem, kunt u iedere gebruiker toewijzen aan een alias met dezelfde naam voordat u de accounts maakt in BI-platform.

Op deze manier hoeft u minder accounts voor dezelfde gebruiker te maken in het programma.

Als u bijvoorbeeld een test- en productieomgeving voor Siebel eBusiness uitvoert en 30 van uw gebruikers hebben toegang tot beide systemen, worden er slechts 30 accounts gemaakt voor die gebruikers. Als u niet

iedere gebruiker toewijst aan een alias met dezelfde naam, worden er 60 accounts voor 30 gebruikers gemaakt in het BI-platform.

Als u echter meerdere systemen uitvoert waarbij gebruikersnamen elkaar overlappen, moet u een nieuwe lidaccount maken voor elke gemaakte alias.

Als u bijvoorbeeld uw testomgeving met een gebruikersaccount voor Russell Aquino (gebruikersnaam 'raquino') uitvoert en de productieomgeving met een gebruikersaccount voor Raoul Aquino (gebruikersnaam 'raquino'), moet u een afzonderlijke account voor de alias van iedere gebruiker maken. Doet u dit niet, dan worden de twee gebruikers aan dezelfde account toegevoegd, en kunnen ze zich niet bij BI-platform aanmelden met hun eigen Siebel eBusiness-referenties.

9.8.2.1 Een Siebel eBusiness-rol aan het BI-platform toewijzen

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik op *Verificatie*.
3. Dubbelklik op *Siebel*.
4. Kies het selectievakje *Siebel-verificatie inschakelen*.
5. Selecteer in het gebied *Opties voor nieuwe alias* een van de volgende opties:
   - *Elke toegevoegde alias toewijzen aan een account met dezelfde naam*
     Selecteer deze optie als u meerdere Siebel eBusiness-systemen hebt met gebruikers die accounts hebben op meer dan één systeem (waarbij geen twee gebruikers dezelfde gebruikersnaam voor verschillende systemen hebben).
   - *Een nieuwe account maken voor elke toegevoegde alias*
     Selecteer deze optie als u slechts één Siebel eBusiness-systeem hebt, als de meerderheid van de gebruikers slechts op één systeem een account heeft, of als de gebruikersnamen voor verschillende gebruikers elkaar overlappen op twee of meer systemen.
6. Selecteer in het gebied *Bijwerkopties van alias* een van de volgende opties:
   - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
     Selecteer deze optie als u een nieuwe alias wilt maken voor iedere gebruiker die is toegewezen aan BI-platform. Als u de optie Een nieuwe account maken voor elke toegevoegde alias hebt ingeschakeld, worden er nieuwe accounts toegevoegd voor gebruikers zonder BI-platformaccount of voor alle gebruikers.
   - *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
     Selecteer deze optie als de rol die u wilt toewijzen veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van BI-platform. Het programma maakt niet automatisch aliassen en accounts voor de gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers wanneer ze zich voor het eerst bij BI-platform aanmelden. Dit is de standaardoptie.
7. Geef in het gedeelte *Opties voor nieuwe gebruiker* op hoe nieuwe gebruikers worden gemaakt.

   Als uw licentieovereenkomst voor het BI-platform is gebaseerd op gebruikersrollen, selecteert u een van de volgende opties:

   Selecteer een van de volgende opties:

   - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van

hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

> **Opmerking**
>
> Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot BI-platform, kan een licentie voor gelijktijdige toegang bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

8. Klik op het tabblad *Rollen*.
9. Selecteer het domein dat overeenkomt met de Siebel-server waarvoor u rollen wilt toewijzen.
10. Selecteer onder *Beschikbare rollen* de rollen die u wilt toewijzen en klik op >.

> **Opmerking**
>
> Via het veld *Rollen zoeken die beginnen met:* kunt u uw zoekopdracht beperken als u een groot aantal rollen hebt. Voer de begintekens van de rol of rollen in, gevolgd door het jokerteken (%). Klik vervolgens op *Zoeken*.

> **Opmerking**
>
> De zoekfunctie werkt alleen als een JAR-bestand van een Siebel-invoegtoepassing wordt geïmplementeerd naar de Tomcat-libmap: `<INSTALLATIEMAP>\tomcat\webapps\BOE\WEB-INF\lib` en `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. Start de Tomcat-server en de Server Intelligence Agent vervolgens opnieuw.

11. Klik op *Bijwerken*.
    De rollen worden aan BI-platform toegewezen.

9.8.2.2 Overweging bij opnieuw toewijzen

Als u de synchronisatie van groepen en gebruikers tussen BI-platform en Siebel wilt afdwingen, schakelt u het selectievakje *Gebruikerssynchronisatie* forceren in.

> **Opmerking**
>
> U moet eerst *Nieuwe aliassen worden toegevoegd en nieuwe gebruikers worden gemaakt* selecteren om *Gebruikerssynchronisatie forceren* te kunnen selecteren.

Wanneer u de rol opnieuw toewijst, is de optie om gebruikers toe te wijzen als gebruikers op naam of gelijktijdige gebruikers alleen van invloed op de nieuwe gebruikers die u toevoegt aan de rol.

U wijst een rol bijvoorbeeld in eerste instantie toe aan BI-platform met de optie *Nieuwe gebruikers worden gemaakt als gebruikers op naam*. Later voegt u gebruikers aan dezelfde rol toe en wijst u de rol opnieuw toe met de optie Nieuwe gebruikers worden gemaakt als *gelijktijdige* gebruikers.

In dit geval worden alleen de nieuwe gebruikers in de rol toegewezen aan BI-platform als gelijktijdige gebruikers. De gebruikers die al zijn toegewezen, blijven gebruikers op naam. Hetzelfde geldt wanneer u gebruikers eerst toewijst als gelijktijdige gebruikers en vervolgens de instellingen wijzigt om nieuwe gebruikers opnieuw toe te wijzen als gebruikers op naam.

9.8.2.3 De toewijzing van een rol ongedaan maken

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied *Beheren* op *Verificatie*.
3. Dubbelklik op *Siebel*.
4. Selecteer op het tabblad *Domeinen* het Siebel-domein dat overeenkomt met de rol of rollen waarvoor u de toewijzing wilt opheffen.
5. Selecteer op het tabblad *Rollen* de rol die u wilt verwijderen en klik op <.
6. Klik op *Bijwerken*.

   De leden van de verantwoordelijkheid hebben geen toegang meer tot BI-platform, tenzij ze andere accounts of aliassen hebben.

   > **Opmerking**
   >
   > U kunt ook afzonderlijke accounts verwijderen of gebruikers uit rollen verwijderen voordat u ze toewijst aan BI-platform, om te voorkomen dat bepaalde gebruikers zich aanmelden.

9.8.3 Gebruikersupdates plannen

U kunt regelmatige gebruikersupdates plannen om ervoor te zorgen dat wijzigingen van uw gebruikersgegevens voor uw ERP-systeem worden weergegeven in uw BI-platformgebruikersgegevens. Deze updates synchroniseren automatisch uw ERP- en BI-platformgebruikers volgens de toewijzingsinstellingen die u hebt geconfigureerd in de CMC (Central Management Console).

Er bestaan twee opties voor het uitvoeren en plannen van updates voor geïmporteerde rollen:

- Alleen rollen bijwerken: met deze optie worden alleen de koppelingen bijgewerkt tussen de rollen die momenteel zijn toegewezen en die in het BI-platform zijn geïmporteerd. Gebruik deze optie als u verwacht

regelmatig updates uit te voeren, en u zich zorgen maakt over gebruik van systeembronnen. Er worden geen nieuwe gebruikersaccounts gemaakt als u alleen rollen bijwerkt.

- Rollen en aliassen bijwerken: met deze optie worden niet alleen koppelingen tussen rollen bijgewerkt, maar worden ook nieuwe gebruikersaccounts gemaakt in het BI-platform voor nieuwe gebruikersaliassen die zijn toegevoegd aan het ERP-systeem.

> ⓘ Opmerking
>
> Als u niet hebt opgegeven dat gebruikersaliassen automatisch worden gemaakt voor updates wanneer u verificatie hebt ingeschakeld, worden er geen accounts gemaakt voor nieuwe aliassen.

9.8.3.1 Gebruikersupdates plannen

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem deze rollen moet bijwerken.

1. Klik op het tabblad *Gebruikersupdate*.
2. Klik op *Plannen* in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

   > → Tip
   >
   > Klik op *Nu bijwerken* als u meteen een update wilt uitvoeren.

   > → Tip
   >
   > Gebruik de optie *Alleen rollen bijwerken* als u regelmatig wilt bijwerken en u zich zorgen maakt over systeembronnen. Het systeem doet er langer over om zowel rollen als aliassen bij te werken.

   Nu wordt het dialoogvenster *Terugkeerpatroon* weergegeven.
3. Selecteer een optie in de lijst *Object uitvoeren* en geef alle gevraagde planningsgegevens op.

   Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U kunt het tijdstip waarop het object wordt gestart, en een begin- en einddatum opgeven.
Dagelijks	De update wordt elke dag of om het opgegeven aantal dagen uitgevoerd. U kunt het tijdstip opgeven waarop het object wordt uitgevoerd, plus een begin- en einddatum.
Wekelijks	De update wordt elke week uitgevoerd. Het kan eenmaal of verschillende keren per week worden uitgevoerd. U kunt de dagen en het tijdstip waarop het object wordt uitgevoerd, en een begin- en einddatum opgeven.
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.

Terugkeerpatroon	Beschrijving
Dag N van elke maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Op de Ne X van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

4. Klik op *Plannen* nadat u de planningsgegevens heb ingevoerd.
   De datum van de volgende geplande rolupdate wordt weergegeven op het tabblad *Gebruikersupdate*.

> **Opmerking**
>
> U kunt altijd de volgende geplande update annuleren door op *Geplande updates annuleren* te klikken in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

9.9 Oracle EBS-verificatie

9.9.1 Oracle EBS-verificatie inschakelen

U kunt het BI-platform gebruik laten maken van Oracle EBS-informatie door het systeem informatie te geven over verificatie in uw Oracle EBS-systeem.

9.9.1.1 Oracle E-Business Suite-verificatie inschakelen

Voordat u de procedure uitvoert, moeten de DLL- en JAR-bestanden van Oracle worden geïmplementeerd op het BI-platform:

1. Download `ojdbc11.dll` van de Oracle-databaseclienttoepassing.
2. Kopieer het bestand naar deze locatie:
   - Windows: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
   - UNIX: `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/platform`
3. Download `ojdbc5.jar` van de Oracle-databaseclienttoepassing.
4. Kopieer het bestand naar deze locatie:

- Windows: `<INSTALLATIEMAP>\Tomcat\lib`
- UNIX: `<INSTALLATIEMAP>/sap_bobj/tomcat/lib`

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied Beheren op *Verificatie*.
3. Klik op *Oracle EBS*.
   De pagina *Oracle EBS* verschijnt nu. Deze heeft vier tabbladen: *Opties*, *Systemen*, *Verantwoordelijkheden* en *Gebruikersupdate*.
4. Selecteer op het tabblad *Opties* het vakje *Oracle EBS-verificatie is ingeschakeld*.
5. Maak de gewenste wijzigingen onder *Nieuwe alias*, *Bijwerkopties* en *Opties voor nieuwe gebruiker* volgens uw BI-platformimplementatie. Klik op *Bijwerken* om de wijzigingen op te slaan voordat u naar het tabblad *Systemen* gaat.
6. Klik op de tab *Systemen*.
7. In het gebied *Oracle EBS-systeemgebruiker* typt u een databasegebruikersnaam en -wachtwoord waarmee het BI-platform zich bij uw Oracle E-Business Suite-database moet aanmelden.
8. Typ in het gebied *Oracle EBS-services* de servicenaam die uw Oracle EBS-omgeving gebruikt, en klik op *Toevoegen*.
9. Klik op *Bijwerken* om de wijzigingen op te slaan.

Nu moet u Oracle EBS-rollen aan het systeem toewijzen.

Verwante informatie

Oracle E-Business Suite-rollen toewijzen [pagina 389]

9.9.2 Oracle E-Business Suite-rollen toewijzen aan het BI-platform

Voor elke Oracle EBS-rol (E-Business Suite) die u toewijst, maakt het BI-platform automatisch een groep. Het systeem maakt ook aliassen om de leden van de toegewezen Oracle E-Business Suite-rollen aan te duiden.

U kunt een gebruikersaccount maken voor elke gemaakte alias. Als u echter meerdere systemen uitvoert en de gebruikers accounts hebben in meer dan een systeem, kunt u iedere gebruiker toewijzen aan een alias met dezelfde naam voordat u de accounts maakt in het BI-platform.

Op deze manier hoeft u minder accounts voor dezelfde gebruiker te maken in het systeem.

Als u bijvoorbeeld een EBS-testomgeving uitvoert en 30 van uw gebruikers toegang hebben tot beide systemen, worden er slechts 30 accounts gemaakt voor die gebruikers. Als u niet iedere gebruiker toewijst aan een alias met dezelfde naam, worden er 60 accounts voor 30 gebruikers gemaakt in het BI-platform.

Als u echter meerdere systemen uitvoert waarbij gebruikersnamen elkaar overlappen, moet u een nieuwe lidaccount maken voor elke gemaakte alias.

Als u bijvoorbeeld uw testomgeving met een gebruikersaccount voor Russell Aquino (gebruikersnaam 'raquino') uitvoert en de productieomgeving met een gebruikersaccount voor Raoul Aquino (gebruikersnaam

'raquino'), moet u een afzonderlijke account voor de alias van iedere gebruiker maken. Anders worden de twee gebruikers toegevoegd aan dezelfde BI-platformaccount. Beide gebruikers kunnen zich met hun eigen Oracle EBS-referenties bij het systeem aanmelden en gegevens uit beide EBS-systemen opvragen.

9.9.2.1 Oracle E-Business Suite-rollen toewijzen

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied Beheren op *Verificatie*.
3. Klik op *Oracle EBS*.
   Op de pagina *Oracle EBS* wordt het tabblad *Opties* weergegeven.
4. Selecteer in het gebied *Opties voor nieuwe alias* een van de volgende opties:
   - *Elke toegevoegde Oracle EBS-alias toewijzen aan een account met dezelfde naam*
     Selecteer deze optie als u meerdere Oracle E-Business Suite-systemen hebt met gebruikers die accounts hebben op meer dan één systeem (en als geen twee gebruikers dezelfde gebruikersnaam voor verschillende systemen hebben).
   - *Een nieuwe account maken voor elke toegevoegde Oracle EBS-alias*
     Selecteer deze optie als u slechts één Oracle E-Business Suite-systeem hebt, als de meerderheid van de gebruikers accounts heeft op slechts één van uw systemen, of als de gebruikersnamen voor verschillende gebruikers elkaar overlappen op twee of meer systemen.
5. Selecteer in het gebied *Bijwerkopties* een van de volgende opties:
   - *Nieuwe aliassen maken wanneer Alias bijwerken optreedt*
     Selecteer deze optie als u een nieuwe alias wilt maken voor iedere gebruiker die is toegewezen aan BI-platform. Als u de optie *Een nieuwe account maken voor elke toegevoegde Oracle EBS-alias* hebt ingeschakeld, worden er nieuwe accounts toegevoegd voor gebruikers zonder BI-platformaccount of voor alle gebruikers.
   - *Alleen nieuwe aliassen maken wanneer de gebruiker zich aanmeldt*
     Selecteer deze optie als de rol die u wilt toewijzen veel gebruikers bevat, maar er slechts een paar gebruik zullen maken van BI-platform. Het platform maakt niet automatisch aliassen en accounts voor de gebruikers. In plaats daarvan worden alleen aliassen (en indien nodig accounts) gemaakt voor gebruikers wanneer ze zich voor het eerst bij BI-platform aanmelden. Dit is de standaardoptie.
6. In *Opties voor nieuwe gebruiker* geeft u op hoe nieuwe gebruikers worden gemaakt, en vervolgens klikt u op *Bijwerken*.

   Selecteer een van de volgende opties:

   - *Nieuwe gebruikers worden gemaakt als gebruikers op naam*
     Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties op naam. Gebruikerslicenties op naam horen bij specifieke gebruikers en geven personen toegang tot het systeem op basis van hun gebruikersnaam en wachtwoord. Deze licenties bieden de betreffende gebruikers toegang tot het systeem ongeacht hoeveel andere personen verbinding met het systeem hebben. Voor elke gebruikersaccount die met deze optie wordt gemaakt, moet een gebruikerslicentie op naam aanwezig zijn.

     > **Opmerking**
     >
     > Aantal gelijktijdige aanmeldingssessies voor een gebruiker op naam die is gemaakt met behulp van Licentie op naam is beperkt tot 10. Als zo'n gebruiker op naam zich bij de 11e gelijktijdige

> aanmeldingssessie probeert aan te melden, geeft het systeem een overeenkomstige foutmelding weer. U moet een van de bestaande sessies vrijgeven om zich te kunnen aanmelden.
>
> Er is echter geen beperking op het aantal gelijktijdige aanmeldingssessies voor gebruikers op naam die gemaakt zijn met behulp van Processorlicentie en Openbaar documentlicentie.

- *Nieuwe gebruikers worden gemaakt als gelijktijdige gebruikers*
  Nieuwe gebruikersaccounts worden ingesteld voor gebruikerslicenties voor gelijktijdige toegang. Met licenties voor gelijktijdige toegang wordt bepaald hoeveel personen tegelijkertijd verbinding met BI-platform kunnen maken. Dit type licenties is erg flexibel omdat met een beperkte licentie voor gelijktijdige toegang een groot aantal gebruikers het systeem kan gebruiken. Afhankelijk van hoe vaak en hoelang gebruikers toegang hebben tot het platform, kan een licentie voor gelijktijdige toegang bijvoorbeeld 250, 500 of 700 gebruikers ondersteunen.

De rollen die u hebt geselecteerd, verschijnen nu als groepen in BI-platform.

7. Klik op de tab *Verantwoordelijkheden*.
8. Onder *Huidige Oracle EBS-services* selecteert u de Oracle EBS-service met de rollen die u wilt toewijzen.
9. Onder *Toegewezen Oracle EBS-rollen* kunt u filters voor Oracle EBS-gebruikers opgeven.
   a. Selecteer in de lijst *Toepassing* de toepassingen die gebruikers voor de nieuwe rol kunnen gebruiken.
   b. Selecteer in de lijst *Verantwoordelijkheid* de toepassingen, functies, rapporten van Oracle, en gelijktijdige programma's die de gebruiker kan uitvoeren.
   c. Selecteer in de *Beveiligingsgroep* de beveiligingsgroep waaraan de nieuwe rol wordt toegewezen.
   d. Gebruik de knoppen *Toevoegen* en *Verwijderen* onder *Huidige rol* om de beveiligingsgroeptoewijzingen voor de rol te wijzigen.
10. Klik op *Bijwerken*.
    De rollen worden aan BI-platform toegewezen.

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem deze rollen moet bijwerken.

9.9.2.1.1 Oracle EBS-rollen en -gebruikers bijwerken

Nadat u Oracle EBS-verificatie heb ingeschakeld, is het noodzakelijk om regelmatig updates te plannen en uit te voeren voor toegewezen rollen die geïmporteerd zijn in het BI-platform. Hierdoor worden bijgewerkte gegevens van Oracle EBS-rollen correct weergegeven in het BI-platform.

Er bestaan twee opties voor het uitvoeren en plannen van updates voor Oracle EBS-rollen:

- Alleen rollen bijwerken: met deze optie worden alleen de koppelingen bijgewerkt tussen rollen die momenteel zijn toegewezen en die in het BI-platform zijn geïmporteerd. Het is raadzaam dat u deze optie gebruikt als u verwacht regelmatig updates uit te voeren, en u zich zorgen maakt over het gebruik van systeembronnen. Er worden geen nieuwe gebruikersaccounts gemaakt als u alleen Oracle EBS-rollen bijwerkt.
- Rollen en aliassen bijwerken: met deze optie worden niet alleen koppelingen tussen rollen bijgewerkt, maar worden ook nieuwe gebruikersaccounts gemaakt in het BI-platform voor gebruikersaliassen die zijn toegevoegd aan rollen in het Oracle EBS-systeem.

> **Opmerking**
>
> Als u niet hebt opgegeven dat gebruikersaliassen automatisch worden gemaakt voor updates wanneer u Oracle EBS-verificatie hebt ingeschakeld, worden er geen accounts gemaakt voor nieuwe aliassen.

9.9.2.1.2 Updates voor Oracle EBS-rollen plannen

Nadat u rollen hebt toegewezen aan het BI-platform, moet u opgeven hoe het systeem deze rollen moet bijwerken.

1. Klik op het tabblad *Gebruikersupdate*.
2. Klik op *Plannen* in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

   > **→ Tip**
   >
   > Klik op *Nu bijwerken* als u meteen een update wilt uitvoeren.

   > **→ Tip**
   >
   > Gebruik de optie *Alleen rollen bijwerken* als u regelmatig wilt bijwerken en u zich zorgen maakt over de systeembronnen. Het systeem doet er langer over om zowel rollen als aliassen bij te werken.

   Nu wordt het dialoogvenster *Terugkeerpatroon* weergegeven.
3. Selecteer een optie uit de vervolgkeuzelijst *Object uitvoeren* en geef alle gevraagde planningsgegevens op in de desbetreffende velden.

   Wanneer u een object plant, kunt u kiezen uit de terugkeerpatronen in de volgende tabel:

Terugkeerpatroon	Beschrijving
Elk uur	De update wordt elk uur uitgevoerd. U kunt het tijdstip waarop het object wordt gestart, en een begin- en einddatum opgeven.
Dagelijks	De update wordt elke dag of om het opgegeven aantal dagen uitgevoerd. U kunt het tijdstip opgeven waarop het object wordt uitgevoerd, plus een begin- en einddatum.
Wekelijks	De update wordt elke week uitgevoerd. De update kan eenmaal of verschillende keren per week worden uitgevoerd. U kunt de dagen en het tijdstip waarop het object wordt uitgevoerd, en een begin- en einddatum opgeven.
Maandelijks	De update wordt elke maand of om de paar maanden uitgevoerd. U kunt het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
Dag N van elke maand	De update wordt uitgevoerd op een bepaalde dag in de maand. U kunt de dag van de maand en het tijdstip waarop de update wordt uitgevoerd en een begin- en einddatum opgeven.
1e maandag van de maand	De update wordt op de eerste maandag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.

Terugkeerpatroon	Beschrijving
Laatste dag van de maand	De update wordt op de laatste dag van elke maand uitgevoerd. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Op de Ne X van de maand	De update wordt uitgevoerd op een opgegeven dag van een opgegeven week van de maand. U kunt het tijdstip opgeven waarop de update wordt uitgevoerd, plus een begin- en einddatum.
Agenda	De update wordt uitgevoerd op de datums die zijn opgegeven in een agenda die eerder is gemaakt.

4. Klik op *Plannen* nadat u de planningsgegevens heb ingevoerd.
   De datum van de volgende geplande rolupdate wordt weergegeven op het tabblad *Gebruikersupdate*.

> **Opmerking**
>
> U kunt altijd de volgende geplande update annuleren door op *Geplande updates annuleren* te klikken in de sectie *Alleen rollen bijwerken* of de sectie *Rollen en aliassen bijwerken*.

9.9.3 Toewijzing van rollen ongedaan maken

Als u wilt voorkomen dat bepaalde gebruikersgroepen zich aanmelden bij het BI-platform, kunt u de toewijzing opheffen van de rollen waartoe ze behoren.

9.9.3.1 De toewijzing van een rol ongedaan maken

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied Beheren op *Verificatie*.
3. Dubbelklik op de naam van het ERP-systeem waarvoor u de toewijzing van rollen ongedaan wilt maken.
   De ERP-systeempagina geeft het tabblad *Opties* weer.
4. Klik op de tab *Verantwoordelijkheden*.
5. Selecteer de *Huidige Oracle EBS-services*.
6. Selecteer een rol onder *Huidige rol* en klik op de knop *Verwijderen*.
7. Klik op *Bijwerken*.

   De leden van de rol hebben geen toegang meer tot BI-platform, tenzij ze andere accounts of aliassen hebben.

> **Opmerking**
>
> U kunt ook afzonderlijke accounts verwijderen of gebruikers uit rollen verwijderen voordat u ze toewijst aan BI-platform, om te voorkomen dat bepaalde gebruikers zich aanmelden.

9.9.4 Rechten aanpassen voor toegewezen Oracle EBS-groepen en -gebruikers

Wanneer u rollen toewijst aan het BI-platform, kunt u rechten instellen voor of machtigingen verlenen aan de groepen en gebruikers die zijn gemaakt.

9.9.4.1 Beheerdersrechten toewijzen

Als u wilt dat gebruikers het BI-platform kunnen beheren, moet u ze lid maken van de standaardgroep Administrators. Leden van deze groep krijgen volledig beheer over alle aspecten van het systeem, waaronder accounts, servers, mappen, objecten, instellingen, enzovoort.

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied *Ordenen* op *Gebruikers en groepen*.
3. Klik in de kolom *Naam* met de rechtermuisknop op *Beheerders* en klik op *Leden toevoegen aan groep*.

   De pagina *Beschikbare gebruikers of groepen* wordt weergegeven.
4. Selecteer in het gebied *Gebruikerslijst* of *Groepenlijst* de toegewezen rol waaraan u beheerdersrechten wilt toekennen.
5. Klik op > om de rol in te stellen als een subgroep van de groep Administrators en klik op *OK*.

De leden van de rol hebben nu beheerdersrechten in het BI-platform.

> ⓘ Opmerking
>
> U kunt ook een rol in Oracle EBS maken, de gewenste gebruikers aan de rol toevoegen en de rol toewijzen aan het BI-platform. Vervolgens maakt u van de toegewezen rol een subgroep van de standaardgroep Administrators om de leden van de rol beheerdersrechten te verlenen.

9.9.4.2 Publicatierechten toewijzen

Wanneer gebruikers van uw systeem zijn aangewezen als maker van inhoud in uw organisatie, kunt u ze machtiging verlenen om objecten te publiceren naar het BI-platform.

1. Meld u als beheerder aan bij de Central Management Console.
2. Klik in het gebied *Ordenen* op *Mappen* .
3. Ga naar de map waarin gebruikers objecten mogen toevoegen.
4. Klik op *Beheren*, *Beveiliging op hoogste niveau* en dan op *Alle mappen*.
5. Klik op *Principals toevoegen*.

   De pagina Principals toevoegen wordt weergegeven.
6. Selecteer in de lijst *Beschikbare gebruikers of groepen* de groep met de leden aan wie u publicatierechten wilt verlenen.
7. Klik op > om de groep toegang tot de map te verlenen en klik vervolgens op *Beveiliging toevoegen en toewijzen*.

De pagina Beveiliging toewijzen wordt weergegeven.

8. Selecteer het gewenste toegangsniveau in de lijst *Beschikbare toegangsniveaus* en klik op > om het toegangsniveau expliciet toe te wijzen.
9. Als de opties *Overnemen van bovenliggende map* en *Overnemen van bovenliggende groep* zijn geselecteerd, heft u de selectie op en klikt u op *Toepassen*.
10. Klik op *OK*.

Leden van de rol kunnen nu objecten toevoegen aan de map en alle bijbehorende submappen. Alas u de toegewezen machtigingen wilt verwijderen, selecteert u een groep en klikt u op *Verwijderen*.

9.9.5 Eenmalige aanmelding configureren voor SAP Crystal Reports en Oracle EBS

Het BI-platform wordt standaard zo geconfigureerd dat SAP Crystal Reports-gebruikers toegang hebben tot Oracle EBS-gegevens met eenmalige aanmelding.

9.9.5.1 SSO voor Oracle EBS en SAP Crystal Reports deactiveren

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Selecteer *crdb_oraapps*.
5. Klik op *Verwijderen*.
6. Klik op *Opslaan en sluiten*.
7. Ga naar de pagina *Servers* in de CMC en selecteer *Crystal Reports Services*.
8. Klik op de knop *Server opnieuw starten*.

9.9.5.2 SSO opnieuw activeren voor Oracle EBS en SAP Crystal Reports

Volg de onderstaande stappen om SSO opnieuw te activeren voor Oracle EBS en SAP Crystal Reports.

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Onder *SSO-context gebruiken voor aanmelding bij database met de volgende stuurprogramma's* typt u **`crdb_oraapps`**.
5. Klik op *Toevoegen*.

6. Klik op *Opslaan en sluiten*.
7. Ga naar de pagina *Servers* in de CMC en selecteer *Crystal Reports Services*.
8. Klik op de knop *Server opnieuw starten*.

9.10 X.509-verificatie

9.10.1 X.509-verificatie voor BI-startpunt

9.10.1.1 Certificaten en keystores maken en configureren

> **Opmerking**
>
> Er moet een gebruiker in het BI-platform bestaan om eenmalige aanmelding via X.509-verificatie te bewerkstelligen.

> **Opmerking**
>
> Download en installeer OpenSSL-toolkit om de onderstaande stappen uit te voeren.

> **Opmerking**
>
> Volg alle onderstaande stappen als u een CA-certificaat moet maken en zelf ondertekenen.

> **Opmerking**
>
> Als u een vertrouwde CA hebt, raadpleeg dan Met vertrouwde CA [pagina 397] voor het maken en configureren van certificaten en keystores.

1. Voer de opdracht uit om de bestanden voor certificeringsinstantie (CA)-sleutel (ca.key) en certificaataanvraag (ca.csr) te maken. `Openssl.exe req -newkey rsa:2048 -nodes -out c:\ssl\ca.csr -keyout c:\ssl\ca.key`
2. Voer de opdracht uit om een ondertekend certificaat ca.pem te maken. `Openssl.exe x509 -req -trustout -signkey c:\ssl\ca.key -days 365 -in c:\ssl\ca.csr -out c:\ssl\ca.pem`
3. Maak een serversleutelpaar, een certificaat en een keystore.
   a. Maak een bestand om de serienummers van de CA te bewaren door de volgende code uit te voeren: `Echo 02 >c:\ssl\ca.srl`
   b. Ga naar `C:\Program Files\Java\jre7\bin` en gebruik keytool.exe om serverkeystore, certificaat en privésleutel te maken.

      > **Opmerking**
      >
      > In de locatie van of Java keytool.exe kan 'jre7' afhankelijk van de Java-versie variëren.

      ```
      Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
      c:\ssl\serverkeystore.jks -storetype JKS
      ```

```
Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
keystore c:\ssl\serverkeystore.jks
```

> → Onthouden
>
> Voer tijdens het genereren van het certificaat de hostnaam van de servercomputer in wanneer daarom wordt gevraagd. Anders ontvangt u een certificaatfout voor de client als u verbinding maakt.

c. Voer het keystorewachtwoord in.

> → Onthouden
>
> U moet het aanvraagbestand server.csr in een teksteditor openen en “Nieuwe aanvraag Begin begincertificaat” in “Aanvraag begincertificaat” wijzigen en “Nieuwe aanvraag eindcertificaat” in “Aanvraag eindcertificaat” wijzigen.

4. Voer de opdracht uit om het ondertekend certificaat server.crt te maken. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
5. Importeer de certificeringsinstantie en het servercertificaat naar de serverkeystore.

```
Keytool.exe -import -alias ca -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\ca.pem
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\server.crt
```

6. Voer de opdracht uit om de clientcertificaten client.req en client.key te maken. `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> ⓘ Opmerking
>
> Kopieer het bestand sslc.cnf uit `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` naar C:\SSL en wijzig de parameters:
>
> Dir=c:/ssl # locatie voor alles
>
> Certificate= $dir/ca.pem # CA-certificaat
>
> Private_key= $dir/ca.key # privésleutel
>
> RANDFILE= $dir/.rand # privébestand met willekeurige getallen

7. Voer de opdracht uit om het clientcertificaat te ondertekenen. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`
8. Importeer de CA en het clientcertificaat naar de trustkeystore met de onderstaande opdracht. De opdracht creëert trustkeystore.jks.

```
Keytool.exe -import -alias ca -keystore c:\ssl\trustkeystore.jks -
trustcacerts -file c:\ssl\ca.pem
Keytool.exe -import -alias client -keystore c:\ssl\trustkeystore.jks -
trustcacerts -file c:\ssl\client.pem
```

9. Exporteer het clientcertificaat met de PKCS12-opmaak voor de clientprivésleutel. `Openssl.exe pkcs12 -export -clcerts -in c:\ssl\client.pem -inkey c:\ssl\client.key -out`

`c:\ssl\client.p12 -name "client certificate"`. Met de opdracht wordt het bestand client.p12 gemaakt.

10. Voer de opdracht uit om het CA/certificaat te exporteren en ca.crt te maken. `Openssl.exe x509 -in c:\ssl\ca.pem -inform PEM -out c:\ssl\ca.crt -outform DER`
11. Kopieer de bestanden .p12 en ca.crt naar de clientcomputer om de client en het CA-certificaat te installeren.

> **Opmerking**
>
> Ga voor het installeren van certificaten in Mozilla Firefox naar *Hulpprogramma´s* > *Opties* > *Geavanceerd* > en selecteer Certificaten weergeven op het tabblad Codering om het bestand client.p12 op het tabblad Uw certificaten en het bestand ca.crt file op het tabblad Instanties weer te geven.

9.10.1.1.1 Met vertrouwde CA

1. Maak een serversleutelpaar, een certificaat en een keystore.
   a. Maak een bestand om de serienummers van de CA op te slaan door de volgende code uit te voeren: `Echo 02 >c:\ssl\ca.srl`
   b. Ga naar `C:\Program Files\Java\jre7\bin` en gebruik keytool.exe om serverkeystore, certificaat en privésleutel te maken.

   > **Opmerking**
   >
   > In de locatie van of keytool.exe kan 'jre7' afhankelijk van de Java-versie variëren.

   ```
   Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   c:\ssl\serverkeystore.jks -storetype JKS
   Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
   keystore c:\ssl\serverkeystore.jks
   ```

   > **→ Onthouden**
   >
   > Voer tijdens het genereren van het certificaat de hostnaam van de servercomputer in wanneer daarom wordt gevraagd. Anders ontvangt u een certificaatfout voor de client als u verbinding maakt.

   c. Voer het keystorewachtwoord in.

   > **→ Onthouden**
   >
   > U moet het aanvraagbestand server.csr in een teksteditor openen en "Nieuwe aanvraag Begin begincertificaat" in "Aanvraag begincertificaat" wijzigen en "Nieuwe aanvraag eindcertificaat" in "Aanvraag eindcertificaat" wijzigen.

2. Voer de opdracht uit om het ondertekend certificaat server.crt te maken. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`

3. Importeer het servercertificaat naar de serverkeystore.

```
Keytool.exe –import –alias server –keystore c:\ssl\serverkeystore.jks –
trustcacerts –file c:\ssl\server.crt
```

4. Voer de opdracht uit om clientcertificaten client.req en client.key te maken. `Openssl.exe –newkey rsa:2048 –nodes –out c:\ssl\client.req –keyout c:\ssl\client.key –config c:\ssl\sslc.cnf`

> **Opmerking**
>
> Kopieer het bestand sslc.cnf uit `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` naar C:\SSL en wijzig de parameters:
>
> Dir=c:/ssl # locatie voor alles
>
> Certificate= $dir/ca.pem # CA-certificaat
>
> Private_key= $dir/ca.key # privésleutel
>
> RANDFILE= $dir/.rand # privébestand met willekeurige getallen

5. Voer de opdracht uit om het clientcertificaat te ondertekenen. `Openssl.exe x509 –CA c:\ssl\ca.pem –CAkey c:\ssl\ca.key –CAserial c:\ssl\ca.srl –req –in c:\ssl\client.req –out c:\ssl\client.pem –days 365`
6. Importeer het clientcertificaat naar de trustkeystore met de hieronder vermelde opdracht. De opdracht maakt trustkeystore.jks.

```
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

7. Exporteer het clientcertificaat met de PKCS12-opmaak voor de clientprivésleutel. `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. Met de opdracht wordt het bestand client.p12 gemaakt.
8. Kopieer het .p12-bestand naar de clientcomputer om het te installeren.

> **Opmerking**
>
> Ga voor het installeren van certificaten in Mozilla Firefox naar *Hulpprogramma´s* > *Opties* > *Geavanceerd* > en selecteer Certificaten weergeven op het tabblad Codering om het bestand client.p12 op het tabblad Uw certificaten en het bestand ca.crt op het tabblad Instanties weer te geven.

9.10.1.2 Tomcat SSL-server configureren

9.10.1.2.1 SSL-configuratie in één richting

1. Ga naar `<INSTALLDIR>\tomcat\conf\server.xml`
2. Bewerk de XML-tag: `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200"`

```
SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

> **Opmerking**
>
> Het wachtwoord (Password1) en de locatie (C:\ssl\serverkeystore.jks) van het keystorebestand gebruikt in de XML-tag hierboven zijn slechts voorbeelden. U kunt het wachtwoord en de locatie van uw keuze gebruiken.

3. Sla het bestand op en start de Tomcat-server opnieuw.

9.10.1.2.2 SSL-configuratie in twee richtingen

Configureer de Tomcat-server om clientverificatie aan te vragen door de onderstaande stappen uit te voeren.

1. Ga naar `<INSTALLDIR>\tomcat\conf\server.xml`
2. Bewerk server.xml met de onderstaande XML-tag:
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

> **Opmerking**
>
> Het wachtwoord (Password1) en de locatie (C:\ssl\serverkeystore.jks of C:\ssl\trustkeystore.jks) van het serverkeystore- en trustkeystorebestand gebruikt in de XML-tag hierboven zijn slechts voorbeelden. U kunt het wachtwoord en de locatie van uw keuze gebruiken.

3. Sla het bestand op en start de Tomcat-server opnieuw.

> **Opmerking**
>
> Schakel in Internet Explorer de optie “Niet vragen om een clientcertificaat te selecteren als er geen of slechts één certificaat bestaat” uit door te gaan naar *Internetopties* > *Beveiliging* > *Lokaal intranet* > *Aangepast niveau* > *Diversen*.

9.10.1.3 BI-startpunt configureren

9.10.1.3.1 Gedeelde geheime sleutel maken

De gedeelde geheime sleutel wordt gebruikt om de vertrouwde relatie tussen de client en de CMS vast te leggen. U moet de server vóór de client configureren voor vertrouwde verificatie.

1. Meld u aan bij de CMC.
2. Ga naar Verificatie en selecteer Enterprise.
3. Schakel Vertrouwde verificatie in.
4. Selecteer Nieuw gedeeld geheim.

> **Opmerking**
>
> De gedeelde geheime sleutel wordt gegenereerd en het downloadbericht wordt weergegeven.

5. Selecteer Gedeeld geheim downloaden.
6. Selecteer Opslaan in het downloaddialoogvenster en selecteer een van de volgende mappen:
   - `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
   - `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

9.10.1.3.2 De gedeelde geheime sleutel via het bestand TrustedPrincipal.conf doorgeven

1. Maak een nieuw tekstbestand in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory`.
2. Voeg de hieronder opgegeven tekst aan het nieuwe bestand toe.

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. Sla het bestand op en noem het 'global.properties'.

9.10.1.3.3 Het bestand custom.jsp bewerken

> **Opmerking**
>
> Maak een gebruiker met computernaam in CMC voordat u het bestand custom.jsp bewerkt.

1. Ga naar
   a. *<INSTALLATIEMAP>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* in *com.businessobjects.webpath.InfoView.jar* voor klassiek BI-startpunt.
   b. *<INSTALLATIEMAP>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* in *com.businessobjects.webpath.fioriBI.jar* voor Fiorified BI-startpunt.

2. Bewerk het bestand custom.jsp.

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code
request.getSession().setAttribute("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Opmerking**
>
> Vervang de <Shared_Secret_Key> door de nieuwe sleutel uit het bestand *TrustedPrincipal.conf*. Zie Gedeelde geheime sleutel maken [pagina 399] voor meer informatie over hoe u een sleutel voor een gedeeld geheim maakt.

9.10.1.3.4 Het bestand myScript.js maken

1. Ga naar *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* en maak myScript.js.
2. Voeg het volgende toe aan myScript.js:

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

3. Start de Tomcat-server opnieuw.

9.10.1.3.5 De interne BOE- en aangepaste eigenschappenbestanden instellen

1. Navigeer naar *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*
2. Open het bestand bilaunchpad.properties en wijzig de volgende eigenschappen:

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
```

```
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Start de Tomcat-server opnieuw.

9.10.1.3.6 De web.xml-bestanden van BOE instellen

1. Ga naar `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`
2. Bewerk het bestand web.xml op deze locatie met de hieronder weergegeven code:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Voeg de parameters aan het bestand web.xml toe door de onderstaande stappen te volgen:
   a. `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Voeg de onderstaande parameters toe:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Herhaal de stappen door te navigeren naar `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`

> → Tip
>
> Controleer of u Vertrouwde verificatie correct hebt geconfigureerd door via de volgende URL de toepassing BI-startpunt te openen: https://[cmsnaam]:8443/BOE/BI/logon.jsp, waarbij [cmsnaam] de naam is van de computer die de CMS host.

9.10.2 X.509-verificatie voor webservices

9.10.2.1 Voor SOAP-webservices

9.10.2.1.1 SSL in Tomcat configureren

Wanneer u webservices gebruikt, moet u SSL in Tomcat configureren voordat u het SAP Business Intelligence-platform configureert.

> **Opmerking**
>
> Er moet een gebruiker in het BI-platform bestaan om eenmalige aanmelding via X.509-verificatie te bewerkstelligen.

1. Ga naar `<INSTALLDIR>\tomcat\conf`.
2. Open server.xml in een XML-editor en bewerk de XML-tag:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```
3. Sla het bestand op.

   > **Opmerking**
   >
   > Het wachtwoord en de locatie van de hierboven genoemde bestanden zijn slechts voorbeelden. U kunt het wachtwoord en de locatie van uw keuze toevoegen.

   > **Opmerking**
   >
   > U kunt Certificaten en keystores maken en configureren [pagina 395] raadplegen voor meer informatie over het maken en configureren van keystorebestanden.

9.10.2.1.2 Het bestand axis2.xml configureren

> **Opmerking**
>
> Zorg er in Linux of Unix voor dat de OS BI-installatiegebruiker recursieve 755-rechten heeft op `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje` voordat de onderstaande stappen worden uitgevoerd. De rechten kunnen worden toegewezen via de opdracht `chmod -R 755`

1. Ga naar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

2. Open het bestand axis2.xml in een XML-editor.
3. Actualiseer de XML-tag met een nieuw poortnummer om een beveiligde verbinding toe te staan.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Opmerking**
>
> De standaardconfiguratie neemt aan dat AxisServlet alleen aanvragen via http ontvangt. Om https toe te staan, moet u AxisServletListener configureren met de naam = "https" en de poortparameter op beide ontvangers opgeven. Daarnaast kunt u meerdere poortnummers toevoegen of verwijderen door de XML-tags te actualiseren.

4. Sla axis2.xml op.
5. Start de Tomcat-server opnieuw.
6. Start een browser en ga naar https://<IP address>:<https port>/dswsbobje/services/listServices om de beveiligde verbinding te valideren. Nadat u naar de koppeling hebt genavigeerd, wordt rustedLoginWithX509 op het tabblad Sessie weergegeven.

9.10.2.1.3 Een waarde voor een gedeeld geheim genereren

1. Start de Central Management Console.
2. Ga naar *Verificatie* > *Enterprise.*
3. Schakel onder *Vertrouwde verificatie* het selectievakje *Vertrouwde verificatie is ingeschakeld* in.
4. Kies *Nieuw gedeeld geheim*. Dit genereert de sleutel van het gedeelde geheim.
5. Kies *Gedeeld geheim downloaden* en vervolgens *Bijwerken*.
6. Kopieer het gedownloade bestand TrustedPrincipal.conf naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` in Windows.

> **Opmerking**
>
> U kunt de gedeelde geheime waarde weergeven door TrustedPrincipal.conf in een XML-editor te openen.

9.10.2.1.4 Het bestand web.xml configureren

1. Ga naar `<INSTALLDIR>\tomcat\webapps\dswsbobje\WEB-INF.`

2. Open web.xml in een XML editor en werk de XML-tag bij met de naam van de CMS-hostcomputer:

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. Voeg de onderstaande XML-tag aan de waarde van het gedeeld geheim toe. Zie Een waarde voor een gedeeld geheim genereren [pagina 404] voor meer informatie over het genereren van een waarde voor een gedeeld geheim.

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. Sla het bestand web.xml op.

> **Opmerking**
>
> De in het bestand axis2.xml uitgevoerde configuraties worden genegeerd als u een upgrade uitvoert vanaf een lagere versie dan BI 4.2 SP04.

9.10.2.2 Voor RESTful-webservices

> **Opmerking**
>
> Er moet een gebruiker in het BI-platform bestaan om eenmalige aanmelding via X.509-verificatie te bewerkstelligen.

Raadpleeg het onderwerp HTTPS/SSL configureren in *Beheerdershandleiding voor Business Intelligence-platform* om vertrouwde verificatie voor RESTful-webservices in te stellen.

Als u vertrouwde verificatie wilt instellen met behulp van X.509-certificaten, moet u een gedeelde geheime sleutel genereren. Raadpleeg Een waarde voor een gedeeld geheim genereren in *Beheerdershandleiding voor Business Intelligence-platform* voor meer informatie.

Raadpleeg voor meer information over het REST SDK-eindpunt *API-referentie* > *Verificatie* > */v1//logon/trustedx509* in de *Ontwikkelaarshandleiding voor RESTful-webservice Business Intelligence-platform*.

9.10.2.2.1 X.509-verificatie voor RESTful-webservices op Tomcat

In cryptografie voor openbare sleutels is X.509 een norm waarmee de vereisten voor een beveiligd digitaal certificaat worden gedefinieerd. Een X.509-certificaat verifieert het bezit van een gebruiker of een service-identiteit van een openbare sleutel.

U kunt X.509-verificatie voor RESTful-webservices nu op de Tomcat-toepassingsserver inschakelen door de volgende stappen uit te voeren:

1. Schakel SSL op Tomcat in. Raadpleeg SSL in Tomcat configureren [pagina 403] voor meer informatie.
2. Genereer een gedeelde geheime sleutel. Raadpleeg Een waarde voor een gedeeld geheim genereren [pagina 404] voor meer informatie.
3. Open het bestand van de gedeelde geheime sleutel in een teksteditor.
4. Kopieer de gedeelde geheime sleutel.
5. Bewerk het bestand *biprws.properties*.
   a. Ga naar `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default`.
   b. Open het bestand *biprws.properties* in een teksteditor.
   c. Zoek naar *Trusted_Auth_Shared_Secret=*.
   d. Plak de gedeelde geheime sleutel de waarde *Trusted_Auth_Shared_Secret=*.
   e. Sla het bestand *biprws.properties* op.

9.10.3 X.509-verificatie voor CMC

> **Opmerking**
>
> Er moet een gebruiker in het BI-platform bestaan om eenmalige aanmelding via X.509-verificatie te bewerkstelligen.

U kunt eenmalige aanmelding via X.509-verificatie bewerkstellingen door deze stappen te volgen:

1. Certificaten en keystores maken en configureren [pagina 395]
2. SSL-configuratie in één richting [pagina 398]
3. SSL-configuratie in twee richtingen [pagina 399]
4. Gedeelde geheime sleutel maken [pagina 399]
5. De gedeelde geheime sleutel via het bestand TrustedPrincipal.conf doorgeven [pagina 400]
6. Het bestand Custom.jsp (voor CMC) bewerken [pagina 406]
7. Het bestand myScript.js (voor CMC) maken [pagina 407]
8. De interne BOE- en aangepaste eigenschappenbestanden (voor CMC) instellen [pagina 407]
9. Het bestand web.xml van BOE(voor CMC) instellen [pagina 408]

9.10.3.1 Het bestand Custom.jsp (voor CMC) bewerken

> **Opmerking**
>
> Maak een gebruiker met computernaam in CMC voordat u het bestand custom.jsp bewerkt. Als een gebruiker in een computer bestaat, kunt u direct doorgaan met de onderstaande stappen.

1. Ga naar `<INSTALLDIR>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` in com.businessobjects.webpath.InfoView.jar.

2. Het bestand custom.jsp bewerken

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code request.getSession().setAttribute("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Opmerking**
>
> U moet de gedeelde geheime waarde in deze code door de nieuwe sleutel vervangen en de gebruiker door de computernaam die in CMC is gemaakt vervangen.

9.10.3.2 Het bestand myScript.js (voor CMC) maken

1. Ga naar `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources` en maak myScript.js.
2. Voeg het volgende toe aan myScript.js:

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

3. Start de Tomcat-server opnieuw.

9.10.3.3 De interne BOE- en aangepaste eigenschappenbestanden (voor CMC) instellen

1. Navigeer naar `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Open het bestand CmcApp.properties en voeg de parameters toe:

   ```
   sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter,
   trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela,
   trustedX509, sapSSO, sitemindera
   ```

3. Start de Tomcat-server opnieuw.

9.10.3.4 Het bestand web.xml van BOE(voor CMC) instellen

1. Ga naar `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Bewerk het bestand web.xml op deze locatie met de hieronder weergegeven code:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Voeg de parameters aan het bestand web.xml toe door de onderstaande stappen te volgen:
   a. Ga naar `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Voeg de onderstaande parameters toe:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>Shared_Secret_Key</param-value>
</init-param>
```

   c. Herhaal de stappen door te navigeren naar `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`

> **Opmerking**
>
> Controleer of u Vertrouwde verificatie correct hebt geconfigureerd door via de volgende URL de toepassing BI-startpunt te openen: https://[cmsnaam]:8443/BOE/BI/logon.jsp, waarbij [cmsnaam] de naam is van de computer die de CMS host.

9.11 OpenID Connect-verificatie

U kunt OpenID Connect-verificatie inschakelen.

OpenID Connect-verificatie werkt op basis van verificatieserver (OAuth). Net als voor ondersteuning van cloud-drives is OpenID Connect-verificatie ook afhankelijk van de configuratie van de verificatieserver. Zie Configuratie verificatieserver [pagina 748] voor meer informatie over de configuratie van de verificatieserver.

OpenID Connect-verificatie is ontwikkeld bovenop Enterprise-verificatie.

Net als bij SAML-verificatie moeten gebruikers van tevoren als Enterprise-gebruikers (secEnterprise) in het BI-platform worden geïmporteerd.

> **Opmerking**
>
> Tijdens het importeren van gebruikers moet u ervoor zorgen dat de e-mail-ID van de gebruiker ook wordt toegevoegd.

In tegenstelling tot SAML-verificatie geldt het volgende voor OpenID Connect-verificatie:

- Alle configuraties moeten worden uitgevoerd in de back-end van het BI-platform, niet in de laag van de toepassingsserver.
- Het is niet afhankelijk van vertrouwde verificatie.

OpenID Connect-verificatie wordt alleen ondersteund voor het BI-startpunt en OpenDocument.

9.11.1 OpenID Connect-verificatie inschakelen

OpenID Connect-verificatie wordt alleen ondersteund voor het BI-startpunt en OpenDocument.

Zie Instellingen voor Enterprise-verificatie [pagina 236] voor informatie over het inschakelen van OpenID Connect-verificatie. Nadat u de OpenID Connection-verificatie hebt ingeschakeld in de invoegtoepassing voor Enterprise-verificatie in de back-end, moet u dezelfde toepassingslaag inschakelen voor de ondersteunde toepassingen (bijvoorbeeld het `FioriBI.properties` voor het BI-startpunt en het bestand `OpenDocument.properties` voor de OpenDocument-toepassingen onder `WEB-INF/config/custom`.

Stel `logon.webssoauthentication.framework` in op `OpenId` om de workflow Web SSO-verificatie in te schakelen in te schakelen.

Stel `openid.restful.url` in op de RESTful-webservices-URL van de omgeving (bijvoorbeeld `https://<server>:8443/biprws`).

U kunt zich via OpenID aanmelden bij het BI-startpunt met behulp van de `.../BO/BI`-URL. Wanneer u zich echter via de OpenID Connect-verificatie aanmeldt bij het BI-startpunt, kunt u zien dat de tijdelijke aanduiding voor een contextpad 'WEBSSO' aan de URL wordt toegevoegd. Dit blijft in het URL-pad staan, zelfs nadat u zich hebt afgemeld. Als u zich opnieuw wilt aanmelden vanuit hetzelfde venster met dezelfde URL, moet u 'WEBSSO' verwijderen uit de URL van de browser.

10 Gegevensbronverwijzing

10.1 Verbeterde functie Referentieverwijzingen

In BI 4.2.X en eerdere versies kon een beheerder slechts één set databasereferenties opslaan voor elke gebruiker in CMC.

Deze functionaliteit vereist dat de beheerder dezelfde referenties beheert voor alle verschillende databases. Vanaf BI 4.3 kunt u meerdere sets databasereferenties opslaan voor elke gebruiker via gegevensbronverwijzingen.

> ⓘ Opmerking
>
> De verbeterde functie voor referentieverwijzingen die is geïntroduceerd in SAP BusinessObjects Business Intelligence Platform 4.3 wordt alleen ondersteund in het hulpprogramma voor informatieontwerp. Verbeterde referentieverwijzingen worden niet ondersteund in het hulpprogramma voor universeontwerp.

Gegevensbronverwijzing in CMC

In CMC maakt een beheerder een gegevensbronverwijzing op het BI-platform. Deze gegevensbronverwijzing wordt vervolgens gebruikt in de gebruikerseigenschappen wanneer de beheerder er één set databasereferenties voor definieert. Deze gegevensbronreferentie wordt vervolgens gebruikt in Referentieverwijzingen, een verificatiemethode die beschikbaar is in de Verbindingen.

De beheerder beschikt over de optie om de gewenste gegevensbronverwijzing te selecteren wanneer Referentieverwijzingen wordt geselecteerd als de verificatiemethode. Op een soortgelijke manier kan een beheerder meerdere gegevensbronverwijzingen maken als deze meerdere databases heeft die verbinding maken met het BI-platform en unieke referenties voor elke gebruiker definieert.

> ⓘ Opmerking
>
> Wanneer u gebruikers importeert via een CSV-bestand, gebruikers doorgeeft via het hulpprogramma voor doorgiftebeheer of wanneer u ervoor kiest om de gegevensbronreferenties te synchroniseren tijdens aanmelding voor de verificatietypen Enterprise, LDAP of Windows AD, wijst het BI-platform de databasereferenties toe aan de standaardgegevensbronverwijzing.

Gegevensbronverwijzing in BI-startpunt

Gegevensbronverwijzing is ook beschikbaar in BI-startpunt, waar u uw gebruikersreferenties kunt bijwerken en toewijzen.

> **Opmerking**
>
> U kunt de details van de *Gegevensbronverwijzing* niet bewerken, maar u kunt de velden *Accountnaam*, *Wachtwoord* en *Wachtwoord bevestigen* bewerken.

Hoe werkt het?

We gaan uit van het volgende:

- Er zijn twee gegevensbronverwijzingen beschikbaar op het BI-platform, bijvoorbeeld, DSR1 voor uw verkoopdatabase en DSR2 voor uw financiële database.
- Voor elke gegevensbronverwijzing zijn databasereferenties gedefinieerd in de gebruikerseigenschappen van gebruiker A.
- Er zijn twee verbindingen, CN1 en CN2, die zijn geconfigureerd voor het gebruik van Referentieverwijzingen als de verificatiemethode.
- DSR1 is gekoppeld aan de verbinding CN1 en DSR2 is gekoppeld aan CN2.

Als gebruiker A nu probeert een rapport te vernieuwen dat toegang tot de verkoopdatabase vereist, zoekt het BI-platform naar DSR1 in de gebruikerseigenschappen en gebruikt het de databasereferenties die zijn gedefinieerd voor DSR1 om een verbinding tot stand te brengen.

U moet de volgende taken uitvoeren om een gegevensbronverwijzing te gebruiken.

1. Een gegevensbronverwijzing maken [pagina 411]
2. De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in CMC [pagina 412]
3. Een gegevensbronverwijzing koppelen aan een OLAP-verbinding [pagina 413]

> **Opmerking**
>
> Het is ook mogelijk Referentieverwijzingen te configureren voor relationele verbindingen en OLAP-verbindingen in het hulpprogramma voor informatieontwerp.

10.1.1 Een gegevensbronverwijzing maken

Een gegevensbronverwijzing fungeert als een variabele die een beheerder op het BI-platform maakt om een unieke set databasereferenties op te slaan voor elke gebruiker. Volg de onderstaande stappen om een gegevensbronverwijzing te maken.

1. Meld u aan bij CMC.
2. Ga onder Definiëren naar Gegevensbronverwijzingen.
3. Selecteer het pictogram (Nieuwe gegevensbronverwijzing maken).
4. Voeg de titel en een beschrijving voor de gegevensbronverwijzing toe.
5. Selecteer OK.

U hebt een gegevensbronverwijzing gemaakt.

10.1.2 De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in CMC

Voor een gegevensbronverwijzing moeten databasereferenties zijn gedefinieerd in de gebruikerseigenschappen zodat de gebruiker verbinding kan maken met een database. Voer de volgende stappen uit om de databasereferenties te definiëren in CMC:

1. Meld u aan bij CMC.
2. Ga naar *Gebruikers en groepen*.
3. Open het contextmenu van een gebruiker via de *Gebruikerslijst*.
4. Ga naar *Eigenschappen* en selecteer *Toevoegen* onder *Referenties gegevensbron*.
5. Selecteer de gewenste gegevensbronverwijzing.
6. Voer de waarden in voor *Accountnaam*, *Wachtwoord*, en *Wachtwoord bevestigen*.
7. Herhaal het proces vanaf stap 4 om nog een gegevensbronverwijzing toe te voegen.
8. Selecteer *Opslaan en sluiten*.

   U hebt de databasereferenties gedefinieerd voor een gegevensbronverwijzing.

10.1.3 De databasereferenties definiëren voor een gegevensbronverwijzing voor een gebruiker in BI-startpunt

Voor een gegevensbronverwijzing moeten databasereferenties zijn gedefinieerd in de gebruikerseigenschappen zodat de gebruiker verbinding kan maken met een database.

Gegevensbronverwijzing is nu ook beschikbaar in BI-startpunt, waar u uw gebruikersreferenties kunt bijwerken en toewijzen. De databasereferenties worden gesynchroniseerd tussen CMC en BI-startpunt.

Volg de onderstaande stappen om de databasereferenties te definiëren in het BI-startpunt.

1. Meld u aan bij het BI-startpunt.
2. Ga naar (Gebruikersinstellingen) en klik op de optie (*Instellingen*) in de vervolgkeuzelijst.

   Het venster *Instellingen* wordt weergegeven.
3. Klik op *Gebruikersaccount (administrator)*.

   De pagina Gebruikersaccount wordt geopend met twee tabbladen: *Accountinformatie*, *Databasereferenties* en *Verificatietokens*.
4. Klik op *Databasereferenties*.

   U kunt de gesynchroniseerde gegevens van de gebruiker uit CMC hier bekijken.

   > **Opmerking**
   >
   > U kunt de details van de *Gegevensbronverwijzing* niet bewerken.
   >
   > U kunt wel de velden *Accountnaam*, *Wachtwoord* en *Wachtwoord bevestigen* bewerken.

Als u uw wachtwoord wijzigt, wordt het bericht *Wijzigingen in een aantal voorkeuren worden doorgevoerd nadat de pagina opnieuw is geladen* op het scherm weergegeven.

5. Klik op *Opslaan* en *Sluiten* om de toegewezen referentiewijzigingen op te slaan.

10.1.4 De databasereferenties definiëren voor een gegevensbronverwijzing voor een groep

Voor een gegevensbronverwijzing moeten databasereferenties zijn gedefinieerd in de gebruikerseigenschappen zodat de gebruiker verbinding kan maken met een database.

> **Opmerking**
>
> Met deze taak worden de gegevensbronverwijzingen voor de leden van de subgroepen niet bijgewerkt. U kunt de volgende stappen voor de subgroep volgen om de gegevensbronverwijzingen voor de leden bij te werken.

Voer de volgende stappen uit om de databasereferenties te definiëren:

1. Meld u aan bij CMC.
2. Ga naar *Gebruikers en groepen*.
3. Open het contextmenu van een gebruikersgroep en selecteer *Accountmanager*.
4. Selecteer het selectievakje voor *Databasereferenties* en selecteer vervolgens *Toevoegen*.
5. Voer de waarden voor de vereiste velden in.
6. Selecteer *Opslaan en sluiten*.

U hebt een nieuwe gegevensbronverwijzing met de databasereferenties voor de leden van de gebruikersgroep gedefinieerd. U kunt naar de *Eigenschappen* van een willekeurige gebruiker in deze gebruikersgroep gaan om de gegevensbronverwijzing die u nu hebt bijgewerkt te controleren.

10.1.5 Een gegevensbronverwijzing koppelen aan een OLAP-verbinding

Een beheerder beschikt over de optie om de gewenste gegevensbronverwijzing te selecteren wanneer Referentieverwijzingen als de verificatiemethode voor een verbinding wordt geselecteerd.

Volg de onderstaande stappen om een gegevensbronverwijzing te koppelen aan een verbinding.

1. Meld u aan bij CMC.
2. Ga naar *OLAP-verbindingen*.
3. Open een bestaande verbinding of maak een nieuwe verbinding.
4. Kies in het veld *Verificatie* de optie *Referentieverwijzingen*.
   Het veld *Verwijzing gegevensbron* wordt weergegeven.
5. Kies een gegevensbronverwijzing.

6. Voer de andere vereiste gegevens in en selecteer *Opslaan*.

U hebt een gegevensbronverwijzing gekoppeld aan een OLAP-verbinding.

11 Serverbeheer

11.1 Werken met het beheergebied Servers in de CMC

Het beheergebied Servers in de CMC is het belangrijkste hulpprogramma voor serverbeheertaken. Dit gebied bevat een lijst met alle servers in uw implementatie. Voor de meeste beheer- en configuratietaken moet u een server selecteren in de lijst en een opdracht kiezen in het menu Beheren of Actie.

De navigatiestructuur

In de navigatiestructuur links van het beheergebied Servers kunt u verschillende manieren kiezen om de lijst Servers weer te geven. Selecteer items in de navigatiestructuur om de weergegeven informatie in het venster *Details* te wijzigen.

Optie in de navigatiestructuur	Beschrijving
Serverlijst	Hiermee geeft u een volledige lijst met alle servers in de implementatie weer.
Lijst met servergroepen	Hiermee geeft u een onbewerkte lijst van de beschikbare servergroepen weer in het venster Details. Selecteer deze optie als u de instellingen of beveiliging van een servergroep wilt configureren.
Servergroepen	Hiermee geeft u de servergroepen en de servers in elke servergroep weer. Wanneer u een servergroep selecteert, worden de servers en servergroepen die zich daarin bevinden weergegeven in een hiërarchische weergave in het venster Details.
Knooppunten	Hiermee geeft u een lijst met de knooppunten in de implementatie weer. U kunt knooppunten configureren in de CCM. U kunt een knooppunt selecteren door erop te klikken, zodat u de servers in het knooppunt kunt weergeven of beheren.

Optie in de navigatiestructuur	Beschrijving
Servicecategorieën	Hiermee geeft u een lijst weer met alle mogelijke typen services in de implementatie. Servicecategorieën worden onderverdeeld in BI-platformkernservices en services die aan specifieke SAP BusinessObjects-onderdelen zijn gekoppeld. De volgende servicecategorieën zijn beschikbaar: • *Connectivity-services* • *Kernservices* • *Crystal Reports-services* • *Data Federator-services* • *Doorgiftebeheerservices* • *Analysis-services* • *Web Intelligence-services* Selecteer een servicecategorie in de navigatielijst om de servers in de categorie weer te geven of te beheren. **Opmerking** Een server kan services hosten die tot meerdere servicecategorieën behoren. Een server kan daarom in verschillende servicecategorieën worden weergegeven.
Serverstatus	Hiermee worden de servers weergegeven op basis van de huidige status. Dit is een handig hulpprogramma als u wilt controleren welke servers actief zijn of zijn gestopt. Als de systeemprestaties bijvoorbeeld onvoldoende zijn, kunt u met de lijst *Serverstatus* snel bepalen welke servers een onjuiste status hebben. De volgende serverstatuswaarden zijn beschikbaar: • *Gestopt* • *Bezig met starten* • *Bezig met initialiseren* • *Actief* • *Bezig met stoppen* • *Wordt uitgevoerd met fouten* • *Mislukt* • *Wachten op bronnen*

Het venster Details

Afhankelijk van de opties die u in de navigatiestructuur hebt geselecteerd, wordt in het venster *Details* aan de rechterkant van het beheergebied Servers een lijst weergegeven met servers, servergroepen, statussen, categorieën of knooppunten. De voglende tabel bevat de servergegevens die in het venster *Details* worden weergegeven.

> **Opmerking**
>
> Voor knooppunten, servergroepen, categorieën en statussen worden in het venster *Details* gewoonlijk namen en beschrijvingen weergegeven.

Kolom in venster Details	Beschrijving
Servernaam of *Naam*	Geeft de naam van de server weer.
Status	Geeft de huidige status van de server weer. Aan de hand van de lijst *Serverstatus* in de navigatiestructuur kunt u de gegevens sorteren op serverstatus. De volgende serverstatuswaarden zijn beschikbaar: • *Gestopt* • *Bezig met starten* • *Bezig met initialiseren* • *Actief* • *Bezig met stoppen* • *Wordt uitgevoerd met fouten* • *Mislukt* • *Wachten op bronnen*
Ingeschakeld	Geeft aan of de server is in- of uitgeschakeld.
Oud	Wanneer de server wordt aangeduid als *Oud*, moet deze opnieuw worden gestart. Als u bijvoorbeeld bepaalde serverinstellingen in het venster *Eigenschappen* van de server hebt gewijzigd, moet u de server mogelijk opnieuw starten om de wijzigingen te activeren.
Type	Geeft het servertype weer.
Hostnaam	Geeft de hostnaam van de server weer.
Status	Hiermee wordt de algemene status van de server aangeduid. De volgende serverstatuswaarden zijn beschikbaar: • *Groen* (goede conditie) • *Oranje* (waarschuwing) • *Rood* (gevaar) De status van een server is afhankelijk van de status van de servercontrole. Zo is de status van de Central Management Server afhankelijk van de status van de `<NODENAME>.CentralManagementServer Watch`. U kunt de details van controles op de pagina *Toezicht* in de CMC oproepen: selecteer de controle op het tabblad *Controlelijst* en klik op *Bewerken*. U ziet de *Waarschuwingsregel* en *Gevarenregel* voor de controle, die respectievelijk naar de oranje en rode status wijzen.
PID	Hiermee geeft u de unieke proces-id van de server weer.

Kolom in venster Details	Beschrijving
Beschrijving	Geeft een beschrijving van de server weer. U kunt deze beschrijving wijzigen op de pagina *Eigenschappen* van de server.
Gewijzigd op	Hiermee geeft u de datum weer waarop de server de laatste keer is gewijzigd of waarop de status van de server is gewijzigd. Deze kolom is heel nuttig als u de status van recentelijk gewijzigde servers wilt bekijken.

11.2 Servers beheren via scripts in Windows

Met het uitvoerbare bestand `ccm.exe` kunt u de servers in uw Windows-implementatie via de opdrachtregel starten, stoppen, opnieuw starten, inschakelen en uitschakelen.

Verwante informatie

ccm.exe [pagina 1101]

11.3 Servers beheren op Unix

Met het uitvoerbare bestand `ccm.sh` kunt u de servers in uw Unix-implementatie via de opdrachtregel starten, stoppen, opnieuw starten, inschakelen en uitschakelen.

Verwante informatie

Ccm.sh [pagina 1094]

11.4 De status van een server weergeven en wijzigen

11.4.1 De status van de servers weergeven

De status van een server zegt iets over de werking van de server op een bepaald moment: een server kan actief zijn, bezig zijn met starten of stoppen, gestopt zijn, de status Mislukt hebben, bezig zijn met initialiseren, gestart met fouten of wachten op bronnen. Een server moet actief en ingeschakeld zijn om op

BI-platformaanvragen te kunnen reageren. Een server die is uitgeschakeld wordt nog wel als proces uitgevoerd, maar accepteert geen aanvragen uit het BI-platform. Een server die is gestopt, wordt niet langer als proces uitgevoerd.

In deze sectie wordt behandeld hoe u de status van servers met de CMC kunt wijzigen.

Verwante informatie

De status van een server weergeven [pagina 419]
De statussen van services weergeven [pagina 419]
Servers starten, stoppen en opnieuw starten [pagina 420]
Servers in- en uitschakelen [pagina 423]
Een Central Management Server stoppen [pagina 422]
Een server automatisch starten [pagina 422]

11.4.1.1 De status van een server weergeven

1. Ga naar het beheergebied *Servers* van de CMC.

   In het venster *Details* worden de servicecategorieën in uw implementatie weergegeven.
2. Als u een lijst met servers wilt weergeven in een bepaalde servergroep, servercategorie of in een bepaald knooppunt, klikt u in de navigatiestructuur op de servergroep, het knooppunt of de categorie.
   In het venster *Details* wordt de lijst met servers op uw implementatie weergegeven. In de kolom *Status* wordt de status van elke server in de lijst weergegeven.
3. Als u een lijst wilt weergeven met alle servers die op dat moment een bepaalde status hebben, vouwt u de optie *Serverstatus* in de navigatiestructuur uit en selecteert u de gewenste status.

   In het venster Details wordt een lijst weergegeven met servers met de geselecteerde status.

   > **Opmerking**
   >
   > Dit is met name handig als u snel een lijst wilt bekijken met servers die niet juist worden gestart of die onverwacht zijn gestopt.

11.4.1.2 De statussen van services weergeven

Als een service mislukt, wordt de status van de hostserver ingesteld op *Uitvoeren met fouten* (wat betekent dat ten minste één service goed is gestart) of *Mislukt* (wat betekent dat geen van de services goed zijn gestart). U kunt de serverstatussen in de CMC en CCM weergeven. U kunt echter ook de status van afzonderlijke services weergeven op de pagina *Eigenschappen* van de server in de CMC.

1. Ga naar het beheergebied *Servers* van de CMC.

   In het venster *Details* worden de servicecategorieën in uw implementatie weergegeven.

2. Als u een lijst met servers wilt weergeven in een bepaalde servergroep, servercategorie of in een bepaald knooppunt, klikt u in de navigatiestructuur op de servergroep, het knooppunt of de categorie.
   In het venster *Details* wordt de lijst met servers op uw implementatie weergegeven.
3. Dubbelklik op een server om de pagina *Eigenschappen* te openen.

   De pagina *Eigenschappen* geeft de eigenschappen voor de server, evenals de gehoste services. Voor mislukte services worden ook foutberichten weergegeven.

Verwante informatie

De status van de servers weergeven [pagina 418]

11.4.2 Servers starten, stoppen en opnieuw starten

Het starten, stoppen en opnieuw starten van servers zijn veelvoorkomende acties die u uitvoert als u servers configureert of offline zet. Als u bijvoorbeeld de naam van een server wilt wijzigen, moet u de server eerst stoppen. Nadat u de wijzigingen hebt aangebracht, start u de server opnieuw om de wijzigingen door te voeren. Wanneer u de configuratie-instellingen van een server wijzigt, wordt u vanuit de CMC gevraagd of de server opnieuw moet worden gestart.

In deze sectie wordt toegelicht voor welke configuratiewijziging de server eerst moet worden gestopt of opnieuw gestart. Omdat deze taken zo vaak moeten worden uitgevoerd, worden de begrippen en de verschillen eerst uitgelegd en worden de algemene procedures slechts als naslaginformatie gegeven.

Actie	Beschrijving
Een server stoppen	U moet BI-platformservers mogelijk stoppen voordat u bepaalde eigenschappen en instellingen kunt wijzigen.
Een server starten	Als u een server hebt gestopt om deze te configureren, moet u deze opnieuw starten voordat de wijzigingen van kracht worden en de server verder kan gaan met het verwerken van aanvragen.
Een server opnieuw starten	Een server opnieuw starten houdt in dat een server volledig wordt gestopt en vervolgens opnieuw wordt gestart. Als u een server opnieuw wilt starten nadat u een instelling op de server hebt gewijzigd, wordt u hierom gevraagd vanuit de CMC.
Een server automatisch starten	U kunt instellen dat servers automatisch worden gestart wanneer de Server Intelligence Agent wordt gestart.

Actie	Beschrijving
Beëindiging forceren	Hiermee wordt een server meteen gestopt (in tegenstelling tot het stoppen van een server, waarbij de server wordt gestopt wanneer de huidige verwerkingsactiviteiten zijn voltooid). Forceer het afsluiten alleen als het stoppen van de server is mislukt en u de server onmiddellijk moet stoppen.

→ Tip

Als u een server stopt (of opnieuw start), beëindigt u het proces van de server waardoor de server volledig wordt gestopt. Voordat u een server stopt, is het raadzaam het volgende te doen:

- Schakel de server uit zodat deze de verwerking van eventuele taken kan voltooien, en
- Zorg dat er geen controlegebeurtenissen meer in de wachtrij staan. Als u wilt zien hoeveel gebeurtenissen er in de wachtrij staan, gaat u naar het scherm *Gegevens* onder *Huidig aantal controlegebeurtenissen in wachtrij*.

Verwante informatie

Servers in- en uitschakelen [pagina 423]

11.4.2.1 Servers starten, stoppen of opnieuw starten met de CMC

1. Ga naar het beheergebied *Servers* van de CMC.

   In het venster *Details* worden de servicecategorieën in uw implementatie weergegeven.
2. Als u een lijst met servers wilt weergeven in een bepaalde servergroep, servicecategorie of in een bepaald knooppunt, selecteert u de groep, het knooppunt of de categorie in het navigatievenster.
   In het venster *Details* wordt een lijst met servers weergegeven.
3. Als u een lijst wilt weergeven met alle servers die op dat moment een bepaalde status hebben, vouwt u de optie *Serverstatus* in de navigatiestructuur uit en selecteert u de gewenste status.

   Een lijst met servers met de geselecteerde status wordt weergegeven in het venster *Details*.

   ⓘ Opmerking

   Dit is met name handig als u snel een lijst wilt bekijken met servers die niet juist worden gestart of die onverwacht zijn gestopt.
4. Klik met de rechtermuisknop op de server waarvan u de status wilt wijzigen en selecteer, afhankelijk van de actie die u moet uitvoeren, *Server starten*, *Server opnieuw starten*, *Server stoppen*, of *Gedwongen beëindigen*.

11.4.2.2 Een Windows-server starten, stoppen of opnieuw starten met de CCM

1. Klik in de CCM op de werkbalkknop *Servers beheren*
2. Meld u aan bij uw CMS met een beheerdersaccount wanneer dit wordt gevraagd.
3. Selecteer de server die u wilt starten, stoppen of opnieuw starten in het dialoogvenster *Servers beheren*.
4. Klik op *Starten*, *Stoppen*, *Opnieuw starten* of *Gedwongen beëindigen*.
5. Klik op *Sluiten* om terug te gaan naar de CCM.

11.4.2.3 Een server automatisch starten

Standaard worden servers in uw implementatie automatisch gestart wanneer de Server Intelligence Agent wordt gestart. In deze taak ziet u waar u de optie voor automatisch starten moet instellen.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de server die u automatisch wilt starten.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel onder *Algemene instellingen* het selectievakje*Deze server automatisch starten wanneer de Server Intelligence Agent wordt gestart* in en klik vervolgens op *Opslaan* of *Opslaan en afsluiten*.

> ⓘ Opmerking
>
> Als dit *selectievakje* is uitgeschakeld voor elke CMS in het culster, moet u de CCM gebruiken om het systeem opnieuw op te starten. Nadat u met de CCM de SIA hebt gestopt, klikt u met de rechtermuisknop op de SIA en selecteert u *Eigenschappen*. Klik op het tabblad *Opstarten* op *Eigenschappen* om de pagina Servereigenschappen voor de CMS te openen. Selecteer *Automatisch starten*, klik op *OK* om de pagina Servereigenschappen te starten, en klik nogmaals op *OK*. Start de SIA opnieuw. De optie *Automatisch starten* is alleen beschikbaar als het selectievakje *Deze server automatisch starten wanneer Server Intelligence Agent wordt gestart* is uitgeschakeld voor elke CMS in het cluster.

11.4.3 Een Central Management Server stoppen

Als uw BI-platforminstallatie meerdere actieve Central Management Servers (CMS) bevat, kunt u één CMS uitschakelen zonder gegevensverlies of invloed op de systeemfunctionaliteit. Een andere CMS op het knooppunt neemt de taken van de gestopte server over. Bij gebruik van een CMS-cluster kunt u de Central Management Servers onderhouden door de servers een voor een bij te werken terwijl het BI-platform continu beschikbaar blijft.

Als de implementatie van het BI-platform echter over één CMS beschikt en u deze afsluit, is het BI-platform niet meer beschikbaar voor de gebruikers en wordt de verwerking van rapporten en programma's onderbroken. Dit probleem kan worden opgelost met de Server Intelligence Agent, omdat er hiermee voor elk knooppunt voor wordt gezorgd dat er altijd minimaal één CMS actief is. U kunt een CMS nog steeds stoppen door de bijbehorende SIA te stoppen. Voordat u de SIA stopt, moet u echter de verwerkingsservers stoppen via

de CMC, zodat de actieve taken op deze servers kunnen worden voltooid voordat het BI-platform wordt afgesloten, omdat alle andere servers op het knooppunt ook worden afgesloten.

> **Opmerking**
>
> U kunt situaties tegenkomen waarin de CMS is gestopt en u het systeem opnieuw moet starten vanuit de CCM. Als u bijvoorbeeld elke CMS op een knooppunt uitschakelt en het selectievakje *Deze server automatisch starten wanneer Server Intelligence Agent wordt gestart* is uitgeschakeld voor elke CMS in het cluster op het moment dat de SIA wordt gestart, moet u de CCM gebruiken om het systeem opnieuw op te starten. Klik in de CCM met de rechtermuisknop op de SIA en kies *Eigenschappen*. Klik op het tabblad *Opstarten* op *Eigenschappen* om de pagina Servereigenschappen voor de CMS te openen. Selecteer *Automatisch starten*, klik op *OK* om de pagina Servereigenschappen te starten, en klik nogmaals op *OK*. Start de SIA opnieuw. De optie *Automatisch starten* is alleen beschikbaar als het selectievakje *Deze server automatisch starten wanneer Server Intelligence Agent wordt gestart* is uitgeschakeld voor elke CMS in het cluster.

Plaats de CMS op een apart knooppunt als u uw systeem zo wilt configureren dat u de CMS in het cluster kunt starten en stoppen zonder andere servers te starten en te stoppen: Maak een nieuw knooppunt en kloon de CMS naar dit knooppunt. Wanneer de CMS een eigen knooppunt heeft, kunt u eenvoudig het knooppunt afsluiten zonder dat dit invloed heeft op andere servers.

Verwante informatie

Knooppunten gebruiken [pagina 465]
Servers klonen [pagina 425]
CMS-servers onderbrengen in clusters [pagina 428]

11.4.4 Servers in- en uitschakelen

Wanneer u een BI-platformserver uitschakelt, voorkomt u dat deze nieuwe BI-platformaanvragen ontvangt en verwerkt, maar stopt u het serverproces niet. Dit is handig als u eerst alle huidige aanvragen op de server wilt voltooien, voordat de server wordt gestopt.

U wilt bijvoorbeeld een Job Server stoppen voordat u de computer waarop de server wordt uitgevoerd opnieuw opstart. U wilt echter wel dat de server eerst alle rapportaanvragen in de wachtrij verwerkt. Schakel in dat geval de Job Server uit zodat deze geen nieuwe aanvragen kan accepteren. Ga vervolgens naar de Central Management Console om te controleren of de server de lopende taken heeft voltooid. (Klik in het gebied *Servers*beheer met de rechtermuisknop op de server en selecteer *Servergegevens*.) Als alle huidige aanvragen zijn voltooid, kunt u de server veilig stoppen.

> **Opmerking**
>
> De CMS moet worden uitgevoerd om andere servers te kunnen inschakelen en/of uitschakelen.

> **Opmerking**
>
> Een CMS kan niet worden in- of uitgeschakeld.

11.4.4.1 Servers inschakelen en uitschakelen met de CMC

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik met de rechtermuisknop op de server waarvan u de status wilt wijzigen en klik, afhankelijk van de actie die u moet uitvoeren, op *Server inschakelen* of op *Server uitschakelen*.

11.4.4.2 Een Windows-server in- of uitschakelen met de CCM

1. Klik in de CCM op *Servers beheren*.
2. Wanneer u daarom wordt gevraagd, meldt u zich bij de CMS aan met de referenties die u beheerdersrechten voor het BI-platform geven.
3. Selecteer in het dialoogvenster *Servers beheren* de server die u wilt in- of uitschakelen.
4. Klik op *Inschakelen* of op *Uitschakelen*.
5. Klik op *Sluiten* om terug te gaan naar de CCM.

11.5 Servers toevoegen, klonen of verwijderen

11.5.1 Servers toevoegen, klonen en verwijderen

Als u nieuwe hardware wilt toevoegen aan het BI-platform door serveronderdelen te installeren op nieuwe, extra computers, moet u het installatieprogramma van het BI-platform op die computer uitvoeren. Met het installatieprogramma kunt u een aangepaste installatie uitvoeren. Geef tijdens de Aangepaste installatie de CMS voor uw bestaande installatie op en selecteer de onderdelen die u op de lokale computer wilt installeren. Zie de *Installatiehandleiding voor SAP BI-platform* voor meer informatie over de opties voor een aangepaste installatie.

11.5.1.1 Een server toevoegen

U kunt meerdere exemplaren van hetzelfde BI-platform op dezelfde computer uitvoeren. Een server toevoegen:

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik in het menu *Beheren* op *Nieuw* > *Nieuwe server*.
   Het dialoogvenster *Nieuwe server maken* wordt weergegeven.
3. Kies de *Servicecategorie*.
4. Selecteer het vereiste servicetype in de lijst *Service selecteren* en klik op *Volgende*.
5. Als u een extra service aan de server wilt toevoegen, selecteert u de service in de lijst *Beschikbare extra services* en klikt u op >.

> **Opmerking**
>
> Extra services zijn niet voor alle servertypen beschikbaar.

6. Nadat u alle extra services hebt toegevoegd, klikt u op *Volgende*.
7. Als uw BI-platformarchitectuur uit meerdere knooppunten bestaat, kiest u het knooppunt waar u de nieuwe server wilt toevoegen in de lijst *Knooppunt*.
8. Typ een naam voor de server in het vak *Servernaam*.

   Elke server op het systeem moet een unieke naam hebben. De standaardconventie voor naamgeving is `<NODENAME>.<servertype>` (er wordt een nummer toegevoegd als er meerdere servers van hetzelfde type op dezelfde hostcomputer voorkomen).
9. Geef desgewenst een beschrijving voor de server op in het vak *Beschrijving*.
10. Als u een nieuwe Central Management Server toevoegt, geeft u een poortnummer op in het veld *Name Server-poort*.
11. Klik op *Maken*.
    De nieuwe server wordt in de lijst met servers in het gebied *Servers* van de CMC weergegeven, maar wordt niet gestart of ingeschakeld.
12. Gebruik de CMC om de nieuwe server te starten en in te schakelen wanneer u wilt dat de server gaat reageren op aanvragen van het BI-platform.

11.5.1.2 Servers klonen

Wanneer u nu een nieuw serverexemplaar aan uw implementatie wilt toevoegen, kunt u een bestaande server klonen. De gekloonde server behoudt de configuratie-instellingen van de oorspronkelijke server, behalve de algemene instellingen en de opdrachtregelparameters. Dit is handig wanneer u uw implementatie uitbreidt en nieuwe serverexemplaren wilt maken met bijna dezelfde configuratie-instellingen als die van een bestaande server.

Met klonen wordt ook het verplaatsen van servers tussen knooppunten eenvoudiger. Als u een bestaande CMS naar een ander knooppunt wilt verplaatsen, kunt u deze klonen naar het nieuwe knooppunt. De gekloonde CMS wordt weergegeven op het nieuwe knooppunt en behoudt alle configuratie-instellingen van de oorspronkelijke CMS, behalve de algemene instellingen en opdrachtregelparameters.

Bij het klonen van servers moet u met een aantal zaken rekening houden. U hebt wellicht niet alle instellingen nodig. Controleer daarom of de gekloonde server aan uw behoeften voldoet.

> **Opmerking**
>
> Voordat u servers kloont, moet u controleren of alle computers in de implementatie dezelfde versie van BI-platform (en eventuele updates) bevatten.

> **Opmerking**
>
> U kunt servers van elke computer klonen. U kunt echter alleen servers klonen naar computers waarop de vereiste binaire bestanden voor de server zijn geïnstalleerd.

> **Opmerking**
>
> Wanneer u een server kloont, worden voor de nieuwe server niet automatisch dezelfde referenties voor het besturingssysteem gebruikt. De gebruikersaccount wordt beheerd door de SIA (Server Intelligence Agent) waaronder de server wordt uitgevoerd.

11.5.1.2.1 Tijdelijke aanduidingen gebruiken voor serverinstellingen

Tijdelijke aanduidingen zijn variabelen op knooppuntniveau en worden gebruikt door de servers die op dat knooppunt worden uitgevoerd. Tijdelijke aanduidingen worden vermeld op een speciaal daarvoor bestemde pagina in de CMC (Central Management Console). Als u in de CMC onder *Servers* op een willekeurige server dubbelklikt, verschijnt er in het navigatievenster aan de linkerkant een koppeling voor "Tijdelijke aanduidingen". Op de pagina *Tijdelijke aanduidingen* staan alle beschikbare tijdelijke aanduidingen vermeld plus de bijbehorende waarden voor de geselecteerde server. Tijdelijke aanduidingen bevatten alleen-lezenwaarden, en beginnen en eindigen met een percentteken `%`.

> **Opmerking**
>
> Op de *eigenschappenpagina* van de CMC-server kunt u een tijdelijke aanduiding altijd overschrijven met een specifieke tekenreeks.

Voorbeeld

Tijdelijke aanduidingen zijn nuttig wanneer u servers kloont. Voorbeeld: op computer A met meerdere stations is het `BI-platform` geïnstalleerd in C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0. De tijdelijke aanduiding `%DefaultAuditingDir%` is dan `D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

Een andere computer, computer B, heeft slechts één cd-station (geen station D) en het `BI-platform` is daar geïnstalleerd in C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0. De tijdelijke aanduiding `%DefaultAuditingDir%` is in dit geval `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

Als u de Event Server wilt klonen van computer A naar computer B en tijdelijke aanduidingen gebruikt voor de tijdelijke map Auditing, worden de tijdelijke aanduidingen automatisch omgezet en werkt de Event Server naar behoren. Gebruikt u geen tijdelijke aanduidingen, dan functioneert de Event Server niet, tenzij u de instelling van de tijdelijke map Auditing handmatig overschrijft.

11.5.1.2.2 Een server klonen

1. Ga op de computer waaraan u de gekloonde server wilt toevoegen, naar het beheergebied *Servers* van de CMC.

2. Klik met de rechtermuisknop op de server die u wilt klonen en selecteer *Server klonen*.
   Het dialoogvenster *Server klonen* verschijnt.
3. Typ een naam voor de server (of gebruik de standaardnaam) in het veld *Nieuwe servernaam*.
4. Als u een Central Management Server kloont, geeft u een poortnummer op in het veld *Name Server-poort*.
5. Kies in de lijst *Klonen naar knooppunt* het knooppunt waar u de gekloonde server wilt toevoegen en klik op *OK*.
   De nieuwe server wordt weergegeven in het beheergebied *Servers* van de CMC.

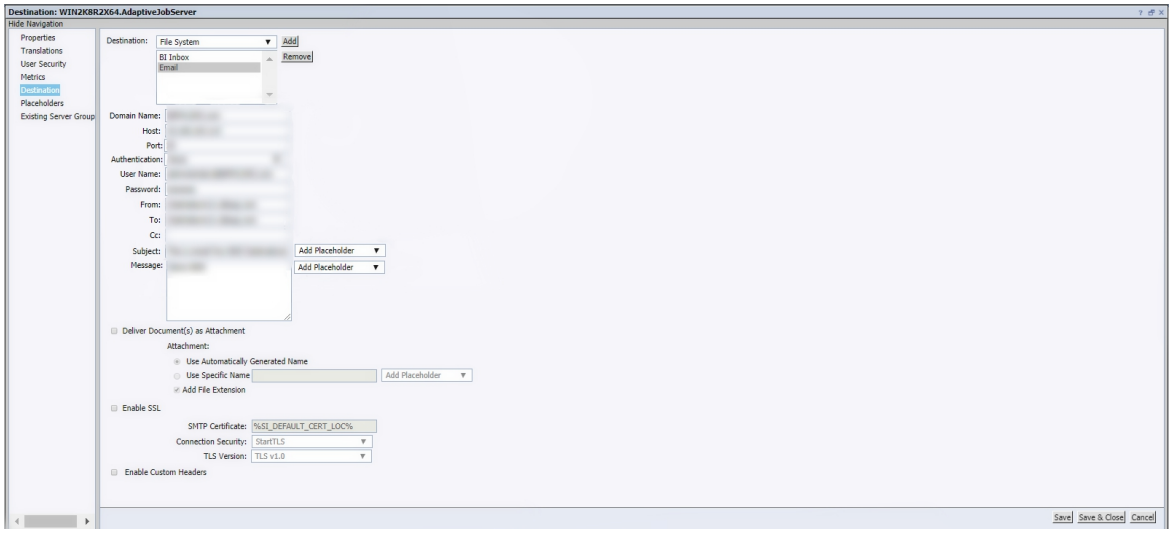
11.5.1.3 Een server verwijderen

1. Ga naar het beheergebied *Servers* van de CMC.
2. Stop de server die u wilt verwijderen.
3. Klik met de rechtermuisknop op de server en selecteer *Verwijderen*.
4. Klik op *OK* om het verwijderen te bevestigen.

11.6 Aangepaste internetkopteksten toevoegen

Een internetkoptekst van een e-mailbericht omvat informatie over de schrijver van het bericht, de e-mailserver waar het bericht doorheen gegaan is en het hulpprogramma of de software die gebruikt is om het bericht te schrijven. U kunt nu aangepaste internetkopteksten aan de e-mails toevoegen die vanuit SAP BusinessObjects BI-platform zijn gepland. Volg de onderstaande stappen om aangepaste kopteksten toe te voegen:

1. Meld u aan bij *CMC*.
2. Ga naar *Servers* en vervolgens *Lijst met servers*.
3. Open het contextmenu voor *Adaptive Job Server* en selecteer *Doelen*.
4. Selecteer in de wizard *Doel* de optie *E-mail* en voeg
   de vereiste details voor elk veld zoals hieronder weergegeven:



5. Schakel *Aangepaste kopteksten inschakelen* in en voeg de internetkopteksten aan het lege veld toe zoals hieronder weergegeven:

6. Klik op *Opslaan en sluiten*.

De e mails met geplande documenten bevatten nu de internetkopteksten.

> **Opmerking**
>
> - Selecteer *Standaardinstellingen gebruiken* tijdens het plannen om aangepaste internetkopteksten aan de geplande e-mails toe te voegen.
> - Elke *Adaptive Job Server* moet geconfigureerd zijn om ervoor te zorgen dat aangepaste kopteksten aan elke e-mail worden toegevoegd.

11.7 CMS-servers onderbrengen in clusters

11.7.1 CMS-servers onderbrengen in clusters

Als u een grote of zeer belangrijke implementatie van SAP BusinessObjects Business Intelligence-platform hebt, wilt u mogelijk meerdere CMS-computers in een cluster onderbrengen. Een cluster bestaat uit twee of meer CMS-servers die samenwerken tegenover één CMS-systeemdatabase. Als een CMS-computer niet meer werkt, worden de aanvragen van het BI-platform overgenomen door een computer met een andere CMS. Door deze hoge mate van beschikbaarheid kunnen gebruikers van het BI-platform nog steeds toegang tot gegevens krijgen als er zich storingen in de apparatuur voordoen.

In deze sectie kunt u lezen hoe u een nieuw CMS-clusterlid toevoegt aan een productiesysteem dat al is geïnstalleerd en wordt uitgevoerd. Wanneer u een nieuwe CMS aan een bestaand cluster toevoegt, geeft u de nieuwe CMS opdracht verbinding te maken met de bestaande CMS-systeemdatabase en de verwerkingstaken met bestaande CMS-computers te delen. Ga naar het beheergebied *Servers* van de CMC voor informatie over uw huidige CMS.

Voordat u CMS-computers in een cluster onderbrengt, moet u controleren of elke CMS is geïnstalleerd op een systeem dat voldoet aan de gedetailleerde vereisten (inclusief versieniveaus en patchniveaus) voor het besturingssysteem, de databaseserver, de methode voor databasetoegang, het databasestuurprogramma en de databaseclient die worden beschreven in de Product Availability Matrix.

Bovendien moet u voor het maken van clusters aan de volgende vereisten voldoen:

- Voor goede prestaties is het nodig dat de databaseserver voor de systeemdatabase kleine query's zeer snel kan verwerken. De CMS communiceert veelvuldig met de systeemdatabase en verzendt veel kleine query's naar deze database. Als de databaseserver deze aanvragen niet snel kan verwerken, heeft dit grote gevolgen voor de prestaties van het BI-platform.
- Voor goede prestaties moet u alle CMS-clusterleden uitvoeren op computers die dezelfde hoeveelheid geheugen en hetzelfde type CPU hebben.
- Configureer alle computers op dezelfde manier:
  - Installeer hetzelfde besturingssysteem, inclusief dezelfde versie van de service packs en patches voor het besturingssysteem.

    - Installeer dezelfde versie van het BI-platform (inclusief patches, indien van toepassing).
    - Zorg ervoor dat elke CMS op dezelfde manier verbinding maakt met de CMS-systeemdatabase, of u nu eigen of ODBC-stuurprogramma's gebruikt. Controleer of de stuurprogramma's op elke computer hetzelfde zijn en of er een ondersteunde versie van is geïnstalleerd.
    - Zorg ervoor dat elke CMS dezelfde databaseclient gebruikt om verbinding met de systeemdatabase te maken en dat de client een ondersteunde versie is.
    - Controleer of voor elke CMS dezelfde gebruikersaccount en hetzelfde wachtwoord voor de verbinding met de CMS-systeemdatabase worden gebruikt. Deze account moet de rechten Maken, Verwijderen en Bijwerken hebben voor de systeemdatabase.
    - Controleer of de knooppunten waarop elke CMS zich bevindt, worden uitgevoerd met dezelfde besturingssysteemaccount. (Onder Windows is dit standaard de account LocalSystem.)
    - Controleer of de huidige datum en tijd juist zijn ingesteld op alle CMS-computers (inclusief instellingen voor de zomertijd).
    - Zorg dat alle computers in een cluster (waaronder de computers die de CMS hosten) op dezelfde systeemtijd zijn ingesteld. Voor een optimaal resultaat synchroniseert u de computers op een tijdserver (zoals `time.nist.gov`) of gebruikt u een centrale toezichtsoplossing.
    - Zorg ervoor dat dezelfde WAR-bestanden zich op alle webtoepassingsservers in het cluster bevinden. Zie de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over de implementatie van het WAR-bestand.
- Zorg ervoor dat elke CMS in een cluster zich in hetzelfde LAN bevindt.
- Out-of-Band-threads (-oobthreads) worden gebruikt door clusterping-opdrachten en clustermeldingen. Aangezien beide bewerkingen snel zijn (meldingen zijn asynchroon), zijn in het BI-platform geen meervoudige oobthreads meer nodig en wordt daarom slechts één -oobthread gemaakt.
  Als uw cluster meer dan acht CMS-clusterleden bevat, moet u erop letten dat de opdrachtregel voor elke CMS de optie `-oobthreads <numCMS>` bevat, waarbij `<numCMS>` het aantal CMS-servers in het cluster is. Deze optie zorgt ervoor dat het cluster zwaar netwerkverkeer aankan. Zie de bijlage Opdrachtregels voor servers in de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor informatie over het configureren van opdrachtregels voor servers.
- Controle inschakelen voor één enkele CMS dient als configuratie in een geclusterde omgeving. U kunt ook de details van de controledatabase wijzigen op de pagina Controle-instellingen in CMC. De vereisten voor de controledatabase zijn gelijk aan de vereisten voor de systeemdatabase wat betreft databaseservers, clients, methoden voor het verkrijgen van toegang, stuurprogramma's en gebruikers-id's.

> → Tip
>
> De naam van een cluster is standaard de computerhostnaam van de eerste CMS die u installeert.

Verwante informatie

De naam van een CMS-cluster wijzigen [pagina 431]

11.7.1.1 Een CMS toevoegen aan een cluster

U kunt een nieuw CMS-clusterlid op verschillende manieren toevoegen. Volg de gewenste procedure:

- U kunt een nieuw knooppunt met een CMS op een nieuwe computer installeren.
- Als u al een knooppunt met binaire CMS-bestanden hebt, kunt u vanuit de CMC een nieuwe CMS-server toevoegen.
- Als u al een knooppunt met binaire CMS-bestanden hebt, kunt u een nieuwe CMS-server toevoegen door een bestaande CMS-server te klonen.

> ⓘ Opmerking
>
> Maak een back-up van uw huidige CMS-systeemdatabase, uw serverconfiguratie, en de inhoud van uw Input en Output File Repositories voordat u wijzigingen aanbrengt. Neem zo nodig contact op met uw databasebeheerder.

Verwante informatie

Een nieuw knooppunt toevoegen aan een cluster [pagina 430]
Een server toevoegen [pagina 424]
Servers klonen [pagina 425]
Overzicht van back-up en herstel [pagina 550]

11.7.1.2 Een nieuw knooppunt toevoegen aan een cluster

Wanneer u een knooppunt toevoegt (een knooppunt is een verzameling BI-platformservers die door één Server Intelligence Agent worden beheerd), wordt u gevraagd een nieuwe CMS te maken of om het knooppunt toe te voegen aan een cluster op een bestaande CMS.

Als u een knooppunt in een cluster op een bestaande CMS wilt plaatsen, kunt u ook het installatieprogramma gebruiken. Voer het installatieprogramma voor het BI-platform uit op de computer waarop u het nieuwe CMS-clusterlid wilt installeren. Met het installatieprogramma kunt u een aangepaste installatie uitvoeren. Geef tijdens de aangepaste installatie de bestaande CMS op waarvan u het systeem wilt uitbreiden en selecteer de onderdelen die u op de lokale computer wilt installeren. In dit geval geeft u de naam van de CMS op die op het bestaande systeem wordt uitgevoerd, kiest u ervoor een nieuwe CMS op de lokale computer te installeren, en geeft u het installatieprogramma de gegevens die nodig zijn om verbinding te maken met de bestaande CMS-systeemdatabase. Wanneer de nieuwe CMS op de lokale computer wordt geïnstalleerd, wordt de server automatisch aan het bestaande cluster toegevoegd.

> ⓘ Opmerking
>
> Voordat u een nieuw knooppunt in een cluster aan een bestaande CMS toevoegt, moet u zorgen dat de BI-platforminstallatie op die server hetzelfde patchniveau heeft als de bestaande BI-platformomgeving als het nieuwe knooppunt een nieuwe server is.

> ⓘ Opmerking
>
> Edge BI- en Crystal Server-licenties staan clustering of implementatie op meerdere knooppunten niet toe. Vanaf Edge BI 4.3 SP2 en Crystal Server 2020 SP2, als Edge BI en Crystal Server zijn geïmplementeerd op

Linux, is ÉÉN Windows-knooppunt met Crystal Reports 2020-services toegestaan. Zie SAP Crystal Reports 2020-services distribueren naar een Windows-server voor meer informatie.

Verwante informatie

Knooppunten gebruiken [pagina 465]

11.7.1.3 Clusters toevoegen aan de eigenschappenbestanden van de webtoepassing

Als u aanvullende CMS'en aan uw implementatie hebt toegevoegd, dan wordt die informatie opgeslagen in het bestand `clusterinfo.1400.properties` dat beschikbaar is in `C:/Users/<you_user>/.businessobjects`. Dit bestand wordt gegenereerd of geactualiseerd wanneer u de SIA opnieuw start.

> **Opmerking**
>
> In een stand-alone Tomcat-implementatie wordt het bestand `clusterinfo.1400.properties` alleen gegenereerd als u zich met een van de CMS-namen aanmeldt. Wanneer u het cluster actualiseert, wordt het bestand in een stand-alone Tomcat-implementatie niet geactualiseerd. U moet het bestand van uw CMS naar uw Tomcat-computer kopiëren.

11.7.1.4 De naam van een CMS-cluster wijzigen

Met deze procedure kunt u de naam wijzigen van een cluster dat al is geïnstalleerd. De Server Intelligence Agent configureert na het wijzigen van de CMS-clusternaam automatisch elke SAP Business Objects-server opnieuw, zodat deze met het CMS-cluster wordt geregistreerd in plaats van met een afzonderlijke CMS.

> **Opmerking**
>
> Ervaren beheerders van het BI-platform moeten er rekening mee houden dat de optie `-ns` niet meer op de serveropdrachtregel kan worden gebruikt om te configureren bij welke CMS een server moet worden geregistreerd. Dit wordt nu automatisch door de SIA verwerkt.

11.7.1.4.1 De clusternaam onder Windows wijzigen

1. Gebruik de CCM om de Server Intelligence Agent te stoppen voor het knooppunt dat een CMS bevat die lid is van het cluster waarvan u de naam wilt wijzigen.

2. Klik met de rechtermuisknop op de Server Intelligence Agent en kies *Eigenschappen*.
3. Klik op het tabblad *Configuratie* in het dialoogvenster Eigenschappen.
4. Schakel het selectievakje *Clusternaam wijzigen in* in.
5. Typ de nieuwe naam voor het cluster.
6. Klik op *OK* en start de Server Intelligence Agent opnieuw.

   De naam van het CMS-cluster is nu gewijzigd. De wijziging wordt dynamisch doorgevoerd in alle andere leden van het CMS-cluster (hoewel het enkele minuten kan duren voordat uw wijzigingen door alle clusterleden zijn overgenomen).
7. Ga naar het beheergebied *Servers* van de CMC en controleer of alle servers zijn ingeschakeld. Schakel zonodig servers opnieuw in als deze door uw wijzigingen zijn uitgeschakeld.

11.7.1.4.2 De clusternaam in UNIX wijzigen

Gebruik het script `cmsdbsetup.sh`. Zie het onderwerp "Unix-scripts" in het hoofdstuk Beheer van opdrachtregels in de *Beheerdershandleiding voor BI-platform* voor meer informatie.

Verwante informatie

Unix-scripts [pagina 1094]

11.8 Servergroepen beheren

Met servergroepen kunnen de BI-platformservers van uw systeem worden georganiseerd en beheerd. U kunt een bepaalde server of servergroep per publicatie selecteren (niet per gebruiker) en u kunt servers op regio of type groeperen.

Groepeer servers op regio om op een gemakkelijke manier standaardinstellingen en terugkerende planningen in te stellen en om doelen te plannen voor gebruikers die in een bepaald regionaal kantoor werken. U kunt een rapportobject (bijvoorbeeld een Crystal Report of een Web Intelligence-document) aan één enkele servergroep koppelen, zodat het object altijd door dezelfde servers wordt verwerkt, en u kunt geplande rapportobjecten aan een bepaalde servergroep koppelen om ervoor te zorgen dat geplande objecten naar de juiste printers, bestandsservers enzovoort worden gestuurd. Servergroepen zijn vooral handig bij het onderhoud van systemen die voor meerdere locaties en in meerdere tijdzones worden gebruikt.

Servergroepen zijn vooral handig bij het onderhoud van systemen die voor meerdere locaties en in meerdere tijdzones worden gebruikt. Gebruik servergroepen bijvoorbeeld om uw BI-platformsysteem aan te passen voor rapporten die op verschillende locaties worden weergegeven en voor verschillende rapporttypen. Als u servers per regio organiseert, kunt u de volgende acties uitvoeren voor servergroepen:

- Standaardverwerkingsinstellingen configureren
- Terugkerende planningen configureren

- Planningsdoelen configureren voor gebruikers die in een bepaald regionaal kantoor werken
- Een rapportobject (bijvoorbeeld een Crystal Report of een Web Intelligence-document) aan één enkele servergroep koppelen, zodat het object altijd door dezelfde servers wordt verwerkt
- Geplande rapportobjecten aan een bepaalde servergroep koppelen om ervoor te zorgen dat geplande objecten naar de juiste printers, bestandsservers, enzovoort worden verzonden.

Groepeer servers op type wanneer u configureert dat objecten worden verwerkt door servers die voor deze objecten zijn geoptimaliseerd.

Nadat u servergroepen hebt gemaakt, configureert u objecten voor het gebruik van bepaalde servergroepen bij het plannen, weergeven en wijzigen van rapporten. Gebruik de navigatiestructuur in het beheergebied *Servers* van de CMC om servergroepen weer te geven. Met de optie *Lijst met servergroepen* geeft u een lijst met servergroepen weer in het venster *Details*. Met de optie *Servergroepen* kunt u de servers in de de groep bekijken.

Voorbeeld: Verwerkingsservers op type groeperen

Verwerkingsservers bijvoorbeeld moeten veel communiceren met de database die gegevens voor gepubliceerde rapporten bevat. Als u verwerkingsservers dicht bij de databaseserver plaatst waartoe ze toegang moeten krijgen, worden de systeemprestaties verbeterd en het netwerkverkeer geminimaliseerd. Als u dus een aantal rapporten hebt die met gegevens uit een DB2-database worden uitgevoerd, kunt u een groep verwerkingsservers maken waarmee de rapporten alleen met de DB2-databaseserver worden verwerkt. Om de systeemprestatie bij het weergeven van rapporten te verbeteren kunt u configureren dat de rapporten altijd deze verwerkingsservergroep voor weergave gebruiken.

11.8.1 Servergroepen maken

Als u een servergroep maakt, moet u de naam en beschrijving van de groep opgeven en vervolgens servers aan de groep toevoegen.

11.8.1.1 Een niet-exclusieve servergroep maken

Niet-exclusieve servergroepen kunnen servers of servergroepen bevatten die deel uitmaken van een andere niet-exclusieve servergroep of de algemene serverpool.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Kies *Beheren* > *Nieuw* > *Servergroep maken*.

   Het dialoogvenster *Servergroep maken* wordt weergegeven.
3. Typ in het vak *Naam* een naam voor de nieuwe groep met servers.
4. Als u extra informatie over de servergroep wilt toevoegen, typt u deze in het veld *Beschrijving*
5. Klik op *OK*.

6. Klik in het beheergebied *Servers* op *Servergroepen* in de navigatiestructuur en selecteer de nieuwe servergroep.
7. Kies *Leden toevoegen* in het menu *Acties*.
8. Selecteer de servers die u aan deze groep wilt toevoegen en klik vervolgens op >.

   > **→ Tip**
   >
   > Houd `CTRL` + `ingedrukt en` klik op de verschillende servers die u wilt selecteren.

   > **ⓘ Opmerking**
   >
   > Vermelde servers omvatten alleen servers die geen deel uitmaken van een andere exclusieve servergroep.

9. Klik op *OK*.

   Het beheergebied *Servers* wordt opnieuw weergegeven. Hier ziet u nu alle servers die u aan de groep hebt toegevoegd. U kunt nu de status wijzigen, serverinformatie weergeven en de eigenschappen van de servers in de groep wijzigen.

11.8.1.2 Een exclusieve servergroep maken

Exclusieve servergroepen bevatten servers of servergroepen die geen deel uitmaken van een andere servergroep of algemene serverpool. Wanneer een servergroep als exclusieve servergroep wordt gemaakt, dan kunnen de servers die deel uitmaken van deze groep niet aan een andere servergroep (exclusief of niet-exclusief) worden toegewezen en servers die aan de exclusieve servergroep zijn toegevoegd worden uit de algemene pool uitgesloten. Hiermee kunt u servergroepen maken die van de algemene belasting van het BI-systeem zijn geïsoleerd.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Kies *Beheren* > *Nieuw* > *Servergroep maken*.

   Het dialoogvenster *Servergroep maken* wordt weergegeven.
3. Typ in het vak *Naam* een naam voor de nieuwe groep met servers.
4. Als u extra informatie over de servergroep wilt toevoegen, typt u deze in het veld *Beschrijving*
5. Schakel het selectievakje *Exclusieve servergroep* in.

   > **ⓘ Opmerking**
   >
   > U kunt een exclusieve servergroep alleen op hoofdniveau maken. Voor een onderliggend knooppunt kunt u alleen een exclusieve servergroep maken als de bovenliggende of hoofdservergroep exclusief is.
   >
   > > **Voorbeeld**
   > >
   > > Zie het volgende scenario om exclusieve servergroepen beter te begrijpen:
   > >
   > > Twee Job Servers: JS1 en JS2 maken deel uit van de algemene serverpool.
   > >
   > > U maakt een exclusieve servergroep: SG1.
   > >
   > > U voegt JS1 aan SG1 toe.

> U plant document (D) door de optie *Alleen gebruikersservers in de geselecteerde groep* te selecteren.
>
> Ga ervan uit dat op zowel JS1 als JS2 al taken worden uitgevoerd.
>
> **Resultaat:** JS1 is al geladen met enkele taken die moeten worden verwerkt. Aangezien JS1 nu echter deel uitmaakt van SG1 ontvangt JS1 alleen aanvragen om workflows te verwerken die aan SG1 zijn toegewezen. Met andere woorden: JS1 is vrij van de algemene systeembelasting.

6. Klik op *OK*.
7. Klik in het beheergebied *Servers* op *Servergroepen* in de navigatiestructuur en selecteer de nieuwe servergroep.
8. Kies *Leden toevoegen* in het menu *Acties*.
9. Selecteer de servers die u aan deze groep wilt toevoegen en klik vervolgens op >.

> → Tip
>
> Houd `CTRL` + `ingedrukt en` klik op de verschillende servers die u wilt selecteren.

> ⓘ Opmerking
>
> Er worden alleen servers weergegeven die niet al deel uitmaken van een andere servergroep of de algemene serverpool.

10. Klik op *OK*.

    Het beheergebied *Servers* wordt opnieuw weergegeven. Hier ziet u nu alle servers die u aan de groep hebt toegevoegd. U kunt nu de status wijzigen, serverinformatie weergeven en de eigenschappen van de servers in de groep wijzigen.

11.8.2 Een exclusieve servergroep naar een niet-exclusieve servergroep converteren en andersom

11.8.2.1 Een exclusieve servergroep naar een niet-exclusieve servergroep converteren

U kunt nu een bestaande exclusieve servergroep wijzigen om deze niet-exclusief te maken.

Voer de volgende handelingen uit om een exclusieve servergroep op hoofdniveau in niet-exclusief te converteren:

1. Klik met de rechtermuisknop op de exclusieve servergroep die u wilt converteren en selecteer *Eigenschappen* uit de vervolgkeuzelijst.

   Dialoogvenster *Eigenschappen* wordt weergegeven. U merkt dat het selectievakje *Exclusieve servergroep* is ingeschakeld.

2. Schakel het selectievakje *Exclusieve servergroep* uit.

   Er wordt een waarschuwingsbericht weergegeven.
3. Klik op *OK* om de conversie te bevestigen.
4. Kies *Opslaan en sluiten*.

   U hebt nu een exclusieve servergroep in een niet-exclusieve servergroep geconverteerd.

> ⓘ Opmerking
>
> U kunt alleen exclusieve servergroepen op hoofdniveau in niet-exclusief converteren.

11.8.2.2 Een niet-exclusieve servergroep naar een exclusieve servergroep converteren

U kunt nu een bestaande niet-exclusieve servergroep wijzigen om deze exclusief te maken.

Voer de volgende handelingen uit om een niet-exclusieve servergroep te converteren die **onafhankelijke** servers en servergroepen bevat:

1. Klik met de rechtermuisknop op de niet-exclusieve servergroep die u wilt converteren en selecteer *Eigenschappen* uit de vervolgkeuzelijst.

   Dialoogvenster *Eigenschappen* wordt weergegeven. U merkt dat het selectievakje *Exclusieve servergroep* niet is ingeschakeld.
2. Schakel het selectievakje *Exclusieve servergroep* in.

   Een successbericht wordt weergegeven.
3. Selecteer *OK*.
4. Kies *Opslaan en sluiten*.

   U hebt nu een niet-exclusieve servergroep in een exclusieve servergroep geconverteerd.

> ⓘ Opmerking
>
> U kunt alleen een niet-exclusieve servergroep in exclusief converteren die onafhankelijke servers en servergroepen heeft. Onafhankelijke servers en servergroepen zijn servers en servergroepen die geen deel uitmaken van een andere servergroep.

11.8.3 Werken met serversubgroepen

Servergroepen kunt u verder onderverdelen in subgroepen met servers. Een subgroep is gewoon een servergroep die lid is van een andere servergroep.

Als u bijvoorbeeld servers per regio en per land indeelt, wordt elke regionale servergroep een subgroep van de landelijke servergroep. Als u servers op deze manier wilt indelen, maakt u eerst de regionale servergroepen en voegt u de verschillende servers aan de juiste regionale servergroepen toe. Vervolgens maakt u landelijke servergroepen en voegt u de regionale servergroepen aan de juiste landelijke servergroepen toe.

U kunt subgroepen op twee manieren instellen: u kunt de subgroepen van een servergroep wijzigen of u kunt de ene servergroep lid maken van een andere servergroep. Het resultaat is hetzelfde, zodat u de methode kunt gebruiken die u het beste uitkomt.

11.8.3.1 Subgroepen aan een servergroep toevoegen

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik op *Servergroepen* in de navigatiestructuur en selecteer de servergroep waaraan u subgroepen wilt toevoegen.

   Deze groep is de bovenliggende groep.
3. Kies *Leden toevoegen* in het menu *Acties*.
4. Klik op *Servergroepen* in de navigatiestructuur, selecteer de servergroepen die u aan deze groep wilt toevoegen en klik op >.

   > → Tip
   >
   > Houd `CTRL` + `ingedrukt terwijl u op de verschillende servergroepen` klikt die u wilt selecteren.
5. Klik op *OK*.

   Het beheergebied *Servers* wordt opnieuw weergegeven. Hier ziet u nu de servergroepen die u aan de bovenliggende groep hebt toegevoegd.

11.8.3.2 Een servergroep lid maken van een andere servergroep

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik op de groep die u aan een andere groep wilt toevoegen.

   > ⓘ Opmerking
   >
   > Voor exclusieve servergroepen op hoofdniveau worden alle exclusieve servergroepen vermeld onder *Beschikbare servergroepen*. U kunt slechts één exclusieve servergroep selecteren en verplaatsen naar *Lid van servergroepen*, aangezien een exclusieve servergroep slechts één bovenliggende servergroep kan hebben.
   >
   > Onderliggende exclusieve servergroepen vermelden geen servergroepen onder *Beschikbare servergroepen*, aangezien een onderliggende exclusieve servergroep slechts één bovenliggende servergroep kan hebben.
3. Kies *Toevoegen aan servergroep* in het menu *Acties*.
4. Selecteer in de lijst *Beschikbare servergroepen* de andere groepen waaraan u de groep wilt toevoegen en klik vervolgens op >.

> → Tip
>
> Houd `CTRL` + `ingedrukt terwijl u op de verschillende servergroepen` klikt die u wilt selecteren.

5. Klik op *OK*.

11.8.4 Het groepslidmaatschap van een server wijzigen

U kunt het groepslidmaatschap van een server wijzigen om de server snel aan een groep of subgroep toe te voegen (of daaruit te verwijderen) die u al op het systeem hebt gemaakt.

Stel bijvoorbeeld dat u servergroepen hebt gemaakt voor een aantal regio's. Mogelijk wilt u één CMS (Central Management Server) gebruiken voor meerdere regionale servergroepen. In plaats van de CMS afzonderlijk toe te voegen aan elke regionale servergroep, kunt u op de koppeling *Lid van* van de server klikken om de CMS aan alle drie de regionale servergroepen tegelijk toe te voegen.

11.8.4.1 Het groepslidmaatschap van een server wijzigen

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik met de rechtermuisknop op de server waarvan u de informatie wilt wijzigen en selecteer *Bestaande servergroepen*.
   De lijst *Beschikbare servergroepen* in het gegevensvenster bevat de groepen waaraan u de server kunt toevoegen. De lijst *Lid van servergroepen* bevat de servergroepen waartoe de server behoort.

   > ⓘ Opmerking
   >
   > Voor servergroepen op hoofdniveau worden alle exclusieve servergroepen vermeld onder *Beschikbare servergroepen*. U kunt slechts één exclusieve servergroep selecteren en verplaatsen naar *Lid van servergroepen*, aangezien een exclusieve servergroep slechts één bovenliggende servergroep kan hebben. Nadat u een exclusieve servergroep uit *Beschikbare servergroepen* hebt geselecteerd en hebt verplaatst naar *Lid van servergroepen*, wordt de exclusieve servergroep uit zijn hoofdservergroep en naar een nieuwe servergroep verplaatst waaraan het is toegewezen.
   >
   > Voor onderliggende servergroepen worden bestaande bovenliggende servergroepen weergegeven onder *Lid van servergroepen* en andere exclusieve servergroepen worden vermeld onder *Beschikbare servergroepen*. U kunt de toewijzing van onderliggende servergroep van een exclusieve bovenliggende groep naar een andere wijzigen.

3. Als u de lijst met servergroepen waartoe de server behoort wilt wijzigen, gebruikt u de pijltoetsen om de servergroepen tussen de lijsten te verplaatsen. Klik op*OK* als u klaar bent.

> ⓘ Opmerking
>
> De optie *Verwijderen uit servergroep* wordt alleen vermeld voor exclusieve servergroepen op onderliggend niveau. Zodra een exclusieve servergroep op onderliggend niveau uit de bovenliggende servergroep is verwijderd, behoudt deze zijn exclusiviteit en wordt deze verplaatst naar het hoofdniveau.

> Servergroepen worden weergegeven in het BI-startpunt als de beveiligingsrechten voor de specifieke servergroepen aan de gebruiker zijn toegewezen door de beheerder van de CMC.

11.8.5 Beheerderstoegang tot servers en servergroepen voor gebruikers

Door beheerdersrechten aan gebruikers toe te kennen kunnen ze server- en servergroepstaken uitvoeren, zoals het starten en stoppen van servers.

Afhankelijk van uw systeemconfiguratie en beveiligingsoverwegingen kunt u het serverbeheer beperken tot de BI-platformbeheerder of moet u mogelijk beheerderstoegang verlenen aan anderen die deze servers gebruiken. Veel bedrijven hebben een IT-afdeling die verantwoordelijk is voor het beheer van de servers. Als de IT-medewerkers periodiek onderhoudstaken voor servers moeten uitvoeren waarbij ze servers moeten stoppen en opnieuw starten, kunt u deze groep het beste beheerdersrechten voor de servers verlenen. Mogelijk wilt u ook serverbeheertaken voor het BI-platform aan anderen delegeren of wilt u dat bepaalde groepen in uw organisatie hun eigen serverbeheer uitvoeren.

> ⓘ Opmerking
>
> U kunt een server of servergroep voor een publicatie selecteren (niet voor een bepaalde gebruiker). U kunt echter ook beheerdersrechten voor een bepaalde server of servergroep aan gebruikers of gebruikersgroepen toekennen.

11.8.5.1 Beheerderstoegangsrechten aan een server of servergroep toekennen

U kunt ook beheerdersrechten voor een bepaalde server of servergroep aan gebruikers of gebruikersgroepen toekennen.

> ⓘ Opmerking
>
> U kunt een server of servergroep voor een publicatie selecteren (niet voor een gebruiker).

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik met de rechtermuisknop op de server of servergroep waartoe u beheerderstoegang wilt verlenen en selecteer *Gebruikersbeveiliging*.
3. Klik op *Principals toevoegen* om gebruikers of groepen toe te voegen waaraan u toegang tot de server of servergroep wilt verlenen.
4. Selecteer in het dialoogvenster *Principals toevoegen* een gebruiker of groep waaraan u beheerdersrechten voor de server of servergroep wilt verlenen en klik op >.
5. Klik op *Beveiliging toevoegen en toewijzen*.
6. Selecteer op het scherm *Beveiliging toewijzen* beveiligingsinstellingen voor de gebruiker of groep en klik op *OK*.

Verwante informatie

Werking van rechten in BI-platform [pagina 123]

11.8.5.2 Objectrechten voor de Report Application Server

Als gebruikers rapporten via het web moeten kunnen maken of wijzigen met de RAS (Report Application Server), moeten RAS Report Modification-licenties beschikbaar zijn op het systeem. Ook moet u aan gebruikers een minimumset objectrechten toewijzen. Als u gebruikers de volgende rechten voor een rapportobject verleent, kunnen zij het rapport als gegevensbron voor een nieuw rapport selecteren of het rapport direct wijzigen:

- Objecten weergeven (of eventueel "Documentexemplaren weergeven").
- Objecten bewerken.
- De gegevens van het rapport vernieuwen.
- De gegevens van het rapport exporteren.

Gebruikers moeten tevens het recht hebben om objecten aan ten minste één map toe te voegen voordat ze nieuwe rapporten in het BI-platform kunnen opslaan.

U wordt aangeraden eerst het gewenste toegangsniveau toe te wijzen en vervolgens de gewenste wijzigingen aan te brengen. U weet dan zeker dat gebruikers de mogelijkheid behouden extra rapportagetaken (zoals kopiëren, plannen, afdrukken, enzovoort) uit te voeren. Selecteer vervolgens de optie Geavanceerd en voeg alle vereiste rechten toe die nog niet zijn verleend. Als gebruikers bijvoorbeeld al het toegangsniveau Weergeven op aanvraag voor een rapport hebben, kunt u ze toestaan het rapport te wijzigen door Geavanceerd te kiezen en expliciet het recht Objecten bewerken te verlenen.

Als gebruikers rapporten weergeven via de geavanceerde DHTML-viewer en de RAS, is het toegangsniveau Weergeven voldoende om het rapport weer te geven maar is Weergeven op aanvraag vereist om de geavanceerde zoekfuncties te kunnen gebruiken. Het extra recht Objecten bewerken is niet vereist.

11.8.6 Een gebruikersgroep aan een servergroep toewijzen

U kunt nu een gebruikersgroep aan een bepaalde servergroep toewijzen via de nieuwe optie *Standaardinstellingen*.

Voer de volgende stappen uit om een gebruikersgroep aan een servergroep toe te wijzen:

1. Meld u aan bij de CMC.
2. Selecteer *Gebruikers en groepen*.
3. Klik met de rechtermuisknop op de pagina *Gebruikers en groepen* op de vereiste gebruikersgroep (waaraan u de servergroep wilt toewijzen).
4. Selecteer *Standaardinstellingen*.
5. Stel op de pagina *Servergroep plannen* de standaardservers in die voor het plannen van de gebruikersgroep moeten worden gebruikt.

U kunt een van de volgende opties selecteren:

- (Standaard) Kies *De eerste beschikbare server gebruiken* om het object uit te voeren op de server die tijdens de planning de meeste bronnen beschikbaar heeft.
- Kies *Voorkeur geven aan servers in de geselecteerde groep* om het object op servers in een bepaalde servergroep uit te voeren. Selecteer vervolgens de vereiste servergroep uit de vervolgkeuzelijst om een voorkeur voor een bepaalde servergroep in te stellen. Als er geen servers in de geselecteerde servergroep beschikbaar zijn, wordt het object op de volgende beschikbare server uit de algemene serverpool uitgevoerd.
- Kies *Alleen servers gebruiken in de geselecteerde groep* om het object alleen op servers in een bepaalde servergroep uit te voeren en selecteer de vereiste servergroep uit de vervolgkeuzelijst om een servergroep exclusief te gebruiken. Als er geen servers beschikbaar zijn in de geselecteerde groep, wordt het object niet verwerkt. Als er bovendien geen taakserver in de toegewezen servergroep aanwezig is, blijft de taak in de status In behandeling.

Opmerking

U kunt ervoor kiezen een exclusieve of niet-exclusieve servergroep aan een gebruikersgroep toe te wijzen door een van de twee keuzerondjes te selecteren: *Voorkeur geven aan servers in de geselecteerde groep* of *Alleen servers gebruiken in de geselecteerde groep*.

Op dezelfde manier kunt u servergroepen toewijzen voor het weergeven of verwerken van Crystal Reports en Web Intelligence-documenten door respectievelijk naar *Standaardinstellingen* en *Crystal Reports-verwerkingsinstellingen* en *Web Intelligence-verwerkingsinstellingen* te navigeren.

Als een servergroep als vereist wordt gekoppeld, betekent dit dat **alleen** servers uit die bepaalde servergroep wordt gebruikt. Servers uit de algemene pool worden niet gebruikt. Als een servergroep als voorkeur wordt gekoppeld, dan worden, als de servers in de servergroep bezig zijn, servers uit de algemene serverpool gebruikt. De algemene serverpool omvat alle servers die geen deel uitmaken van een andere exclusieve servergroep. Zie Een exclusieve servergroep maken [pagina 434] voor meer informatie over het gebruik van exclusieve servergroepen.

Een servergroep aan een gebruikersgroep toewijzen kan ingewikkeld zijn, omdat een gebruiker deel kan uitmaken van verschillende gebruikersgroepen. Bovendien kan elke gebruikersgroep aan verschillende servergroepen worden toegewezen. Elke servergroep kan worden toegewezen als vereiste servergroep of voorkeursservergroep.

Voorbeeld

Zie het volgende scenario:

Een gebruiker (U) maakt deel uit van twee gebruikersgroepen: UG1 en UG2. En elke gebruikersgroep is aan een andere servergroep toegewezen - SG1 en SG2. De resultaten voor verschillende scenario's zijn dan als volgt:

Scenario	Resultaat
U plant een document (D) in. Servergroep 1 (SG1) is ingesteld op UG1 en servergroep 2 (SG2) is ingesteld op UG2. SG1 is ingesteld als Vereist (R). SG2 is ook ingesteld als Vereist (R).	Combinatie van de twee servergroepen (SG1 en SG2) doet dienst als vereiste servergroep (R). Aangezien beide servergroepen (SG1 en SG2) zijn ingesteld als Vereist, worden servers uit de algemene pool niet gebruikt.

Scenario	Resultaat
Geen servergroep is toegewezen op documentniveau (D).	
U plant een document (D) in. Servergroep 1 (SG1) is ingesteld op UG1 en servergroep 2 (SG2) is ingesteld op UG2. SG1 is ingesteld als voorkeursservergroep (P). SG2 is ook ingesteld als voorkeursservergroep (P). Geen servergroep is toegewezen op documentniveau (D).	Combinatie van de twee servergroepen (SG1 en SG2) doet dienst als voorkeursservergroep (P). Aangezien beide servergroepen (SG1 en SG2) zijn ingesteld als voorkeursservergroep, worden als er geen servers in de geselecteerde servergroep beschikbaar zijn, servers uit de algemene pool gebruikt.
U plant een document (D) in. Servergroep 1 (SG1) is ingesteld op UG1 en servergroep 2 (SG2) is ingesteld op UG2. SG is ingesteld als Vereist (R). SG2 is ingesteld als voorkeursservergroep (P). Geen servergroep is toegewezen op documentniveau (D).	Combinatie van de twee servergroepen (SG1 en SG2) doet dienst als vereiste server groep (R). Aangezien de combinatie (SG1 en SG2) als vereiste servergroep dienstdoet, worden servers uit de algemene pool niet gebruikt.

6. Kies *Opslaan en sluiten*.

U hebt nu een gebruikersgroep aan een servergroep toegewezen.

Opmerking

- Een gebruiker kan bij een of meerdere gebruikersgroepen horen en elke van deze gebruikersgroepen kan bij andere gebruikersgroepen horen. Als er geen servergroep is geassocieerd met de onmiddellijke gebruikersgroepen waarvan een gebruiker deel uitmaakt, controleert het programma of een servergroep is geassocieerd met de het volgende niveau van gebruikersgroepen.. Dit proces gaat door totdat het programma een gebruikersgroep vindt waaraan een servergroep is toegewezen. Wanneer het programma een servergroep vindt die op gebruikersgroepsniveau is gekoppeld, stopt het met zoeken. Als er meer dan één servergroepen op het gebruikersgroepsniveau zijn geassocieerd, wordt rekening gehouden met het gedrag van de combinatie van de twee servergroepen (zoals in de bovenstaande tabel uitgelegd). Bekijk het volgende scenario om servergroeptoewijzing te begrijpen:

  #### Voorbeeld

  Scenario: U plant document (D) in.

  Gebruiker (U) maakt deel uit van twee gebruikersgroepen (UG1 en UG2). Maar er is geen servergroep aan UG1 en UG2 toegewezen.

  UG1 hoort bij gebruikersgroep 3 (UG3) en UG2 hoort bij gebruikersgroep 4 (UG4).

  Servergroep 3 (SG3) is ingesteld op UG3.

  SG3 is ingesteld als Vereist (R).

Resultaat: Aangezien er geen servergroepen op het eerste niveau (UG1 en UG2) zijn ingesteld, controleert het programma of er servergroepen op het volgende niveau zijn ingesteld (UG3 en UG4). Omdat SG op UG3 is ingesteld en SG3 als Vereist is ingesteld, worden alleen servers in SG3 gebruikt om het object te verwerken en kunnen servers uit de algemene pool niet worden gebruikt.

Dit impliceert dat als geen servergroepen op het gebruikersgroepsniveau zijn ingesteld, het programma het eerstvolgende niveau controleert om te zien of er servergroepen zijn ingesteld. Als het programma identificeert dat een servergroep op een van de gebruikersgroepsniveaus is ingesteld, stopt het programma met zoeken naar servergroepen op het volgende niveau.

- Op documentniveau kan er slechts één servergroep zijn die kan worden toegewezen en deze kan of een Vereiste servergroep (R) of Voorkeursservergroep (P) zijn. Een gebruiker kan echter van een of meer gebruikersgroepen deel uitmaken en dit kan ertoe leiden dat er meer dan één servergroep aan een gebruiker wordt toegewezen. Als een servergroep op zowel documentniveau (D) als gebruikersgroepsniveau (UG) is ingesteld, dan wordt met de servergroepkoppeling op documentniveau altijd rekening gehouden boven de servergroepkoppeling op gebruikersgroepsniveau. Bekijk het volgende scenario om servergroeptoewijzing te begrijpen:

  Voorbeeld

  Scenario: U plant document (D) in.

  Servergroep 1 (SG1) is op D ingesteld en SG1 is als Vereist ingesteld.

  Servergroep 2 (SG1) is ingesteld op UG en SG2 is ingesteld op Voorkeursservergroep.

  Resultaat: SG1 wordt gebruikt. Aangezien SG1 als Vereist is ingesteld, kunnen servers uit de algemene pool niet worden gebruikt.

  Aangezien een servergroep (SG1) al op documentniveau (D) is ingesteld, negeert het programma de servergroeptoewijzing op het gebruikersgroepsniveau. Dit impliceert dat met servergroeptoewijzing op documentniveau wordt rekening gehouden boven gebruikersgroepsniveau.

- U moet ervoor zorgen dat alle vereiste servers deel uitmaken van de servergroep.
- Lees https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/ om meer in detail over servergroeptoewijzing op map- en gebruikersgroepniveau te begrijpen.

11.8.7 Een map aan een servergroep toewijzen

U kunt nu een map aan een bepaalde servergroep toewijzen via de nieuwe optie *Standaardinstellingen*.

Voer de volgende uit om een map aan een servergroep toe te wijzen:

1. Meld u aan bij de CMC.
2. Ga naar *Mappen* en klik met de rechtermuisknop op de gewenste map (waaraan u de servergroep wilt toewijzen).
3. Selecteer *Standaardinstellingen*.

4. Stel op de pagina *Servergroep plannen* de standaardservers in die voor het plannen op mapniveau moeten worden gebruikt.

   U kunt een van de volgende opties selecteren:

   - (Standaard) Kies *De eerste beschikbare server gebruiken* om het object uit te voeren op de server die tijdens de planning de meeste bronnen beschikbaar heeft.
   - Kies *Voorkeur geven aan servers in de geselecteerde groep* om het object op servers in een bepaalde servergroep uit te voeren. Selecteer vervolgens de vereiste servergroep uit de vervolgkeuzelijst om een voorkeur voor een bepaalde servergroep in te stellen. Als er geen servers in de geselecteerde servergroep beschikbaar zijn, wordt het object op de volgende beschikbare server uit de algemene serverpool uitgevoerd.
   - Kies *Alleen servers gebruiken in de geselecteerde groep* om het object alleen op servers in een bepaalde servergroep uit te voeren en selecteer de vereiste servergroep uit de vervolgkeuzelijst om een servergroep exclusief te gebruiken. Als er geen servers beschikbaar zijn in de geselecteerde groep, wordt het object niet verwerkt.

   > **Opmerking**
   >
   > U kunt ervoor kiezen een exclusieve of niet-exclusieve servergroep aan een map toe te wijzen door een van de twee keuzerondjes te selecteren: *Voorkeur geven aan servers in de geselecteerde groep* of *Alleen servers gebruiken in de geselecteerde groep*.
   >
   > Op dezelfde manier kunt u servergroepen toewijzen voor het weergeven of verwerken van Crystal Reports en Web Intelligence-documenten door respectievelijk naar *Standaardinstellingen* en *Crystal Reports-verwerkingsinstellingen* en *Web Intelligence-verwerkingsinstellingen* te navigeren.
   >
   > Als een servergroep als vereist wordt gekoppeld, betekent dit dat **alleen** servers uit die bepaalde servergroep wordt gebruikt. Servers uit de algemene pool worden niet gebruikt. Als een servergroep als voorkeur wordt gekoppeld, dan worden, als de servers in de servergroep bezig zijn, servers uit de algemene serverpool gebruikt. De algemene serverpool omvat alle servers die geen deel uitmaken van een andere exclusieve servergroep. Zie Een exclusieve servergroep maken [pagina 434] voor meer informatie over het gebruik van exclusieve servergroepen.

5. Kies *Opslaan en sluiten*.

   U hebt nu een map aan een servergroep toegewezen.

   > **Opmerking**
   >
   > - Op documentniveau kan er slechts één servergroep zijn die kan worden toegewezen en deze kan of een Vereiste servergroep (R) of Voorkeursservergroep (P) zijn. Als een servergroep op mapniveau (F), documentniveau (D) en gebruikersgroepniveau (UG) is ingesteld, dan wordt met de servergroepkoppeling op documentniveau altijd rekening gevolgd boven de servergroepkoppeling op mapniveau gevolgd door servergroepkoppeling op gebruikersgroepniveau. Daarom is de volgorde van prioriteit voor servergroeptoewijzing als volgt:
   > **document > map > gebruikersgroep**
   > - Een document kan bij een map horen die weer bij een andere bovenliggende map kan horen. Gezien het feit dat er geen servergroep op documentniveau is toegewezen: als er geen servergroep aan de directe map is toegewezen waartoe het document behoort, controleert het programma om te zien of een servergroep aan de volgende direct bovenliggende map is gekoppeld. Dit proces gaat door totdat het programma een bovenliggende map vindt waaraan een servergroep is toegewezen. Wanneer het programma een servergroep vindt die op mapniveau is gekoppeld, stopt het met zoeken. Bekijk het volgende scenario om servergroeptoewijzing te begrijpen:

Voorbeeld

Scenario: U plant document (D) in.

Maar er is geen servergroep op documentniveau toegewezen.

Document (D) hoort bij map (F). Maar er is geen servergroep op F toegewezen.

Map (F) maakt weer deel uit van een andere map: Bovenliggende map (PF). Servergroep (SG) is ingesteld op PF.

SG is ingesteld als Vereist (R).

Resultaat: Aangezien er geen servergroepen op het documentniveau (D) zijn ingesteld, controleert het programma om te zien of er servergroepen zijn die op mapniveau (F) zijn ingesteld. Omdat er weer er geen servergroepen op F zijn ingesteld, controleert het programma om te zien of er servergroepen zijn die op het volgende niveau - bovenliggende map (PF) - zijn ingesteld. Omdat SG op PF is ingesteld en SG als Vereist is ingesteld, worden alleen servers in SG gebruikt om het object te verwerken en kunnen servers uit de algemene pool niet worden gebruikt.

Dit impliceert dat als geen servergroepen op het documentniveau zijn ingesteld,. Het programma de directe map controleert om te zien of er servergroepen zijn ingesteld. Als het programma identificeert dat een servergroep op een van de mapniveaus is ingesteld, stopt het programma met zoeken naar servergroepen op het volgende niveau.

Als er geen servergroep op documentniveau is ingesteld en ook geen servergroep op mapniveau is ingesteld, dan zoekt het programma op dezelfde manier de servergroeptoewijzing op gebruikersgroepniveau.

- U moet ervoor zorgen dat alle vereiste servers deel uitmaken van de servergroep.
- Lees https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/ om meer in detail over servergroeptoewijzing op map- en gebruikersgroepniveau te begrijpen.

11.8.8 Rechtenbeheer servergroep begrijpen

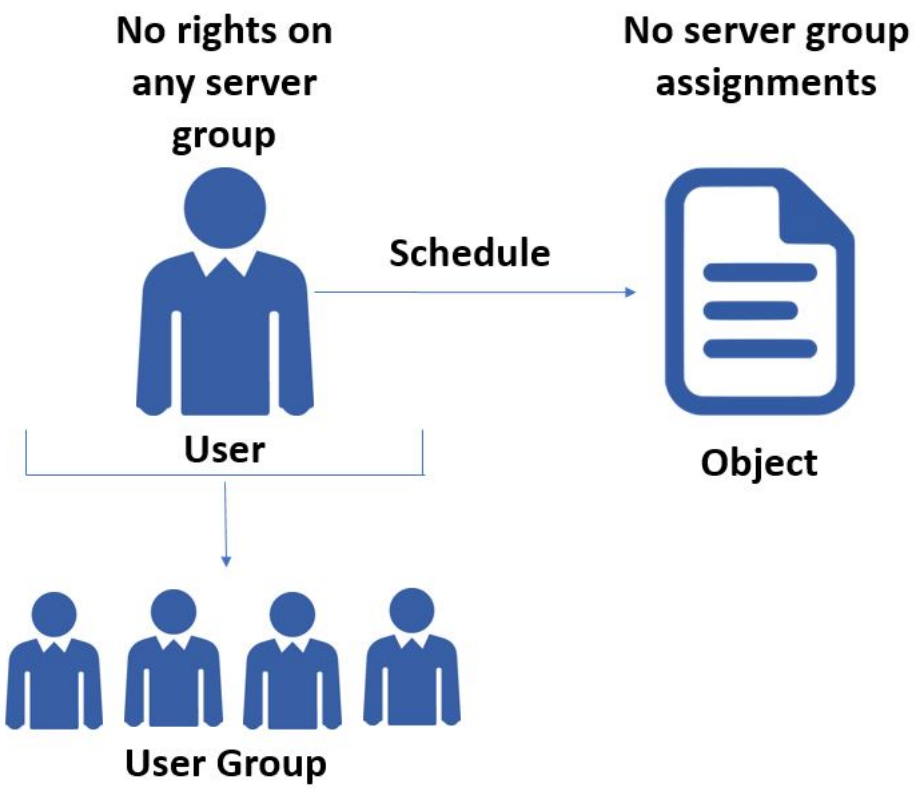
U kunt toegangsrechten voor servergroepen op gebruikers- of gebruikersgroepsniveau inschakelen. Dit wil zeggen dat u de toegang tot de servergroepen voor elke gebruiker of gebruikersgroep kunt controleren.

Opmerking

- In de onderstaande scenario's wordt planning als proces gebruikt om het rechtenbeheer voor servergroepen uit te leggen. Daarnaast wordt het rechtenbeheer voor servergroepen voor weergave en cachebeheer toegelicht.
- U kunt een object plannen als de servers beschikbaar zijn in een servergroep of combinatie van servergroepen. Planning mislukt als er geen servers beschikbaar zijn.

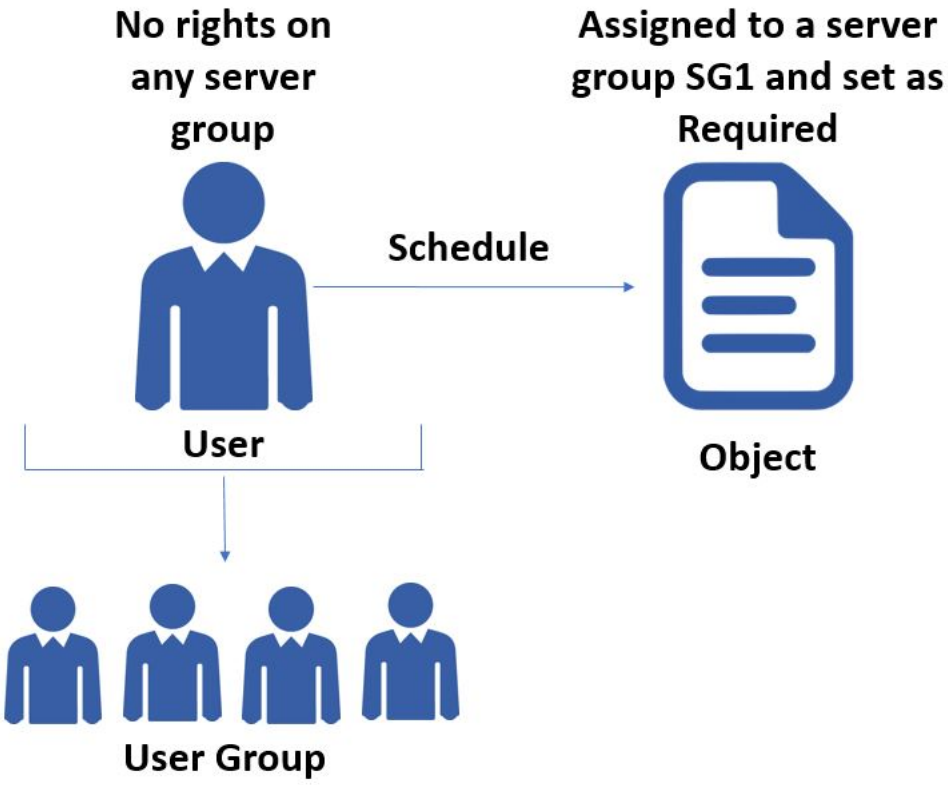
Scenario 1:

Ga uit van een ideaal scenario waarbij een gebruiker deel uitmaakt van een gebruikersgroep op het Business Intelligence-platform. De gebruiker en de bijbehorende gebruikersgroep hebben in geen enkele servergroep rechten. De gebruiker wil nu een object plannen dat ook niet aan een servergroep is toegewezen.



Scenario 2:

U wijzigt het bovenstaande scenario door een servergroep aan het object toe te wijzen; planning van het object mislukt.



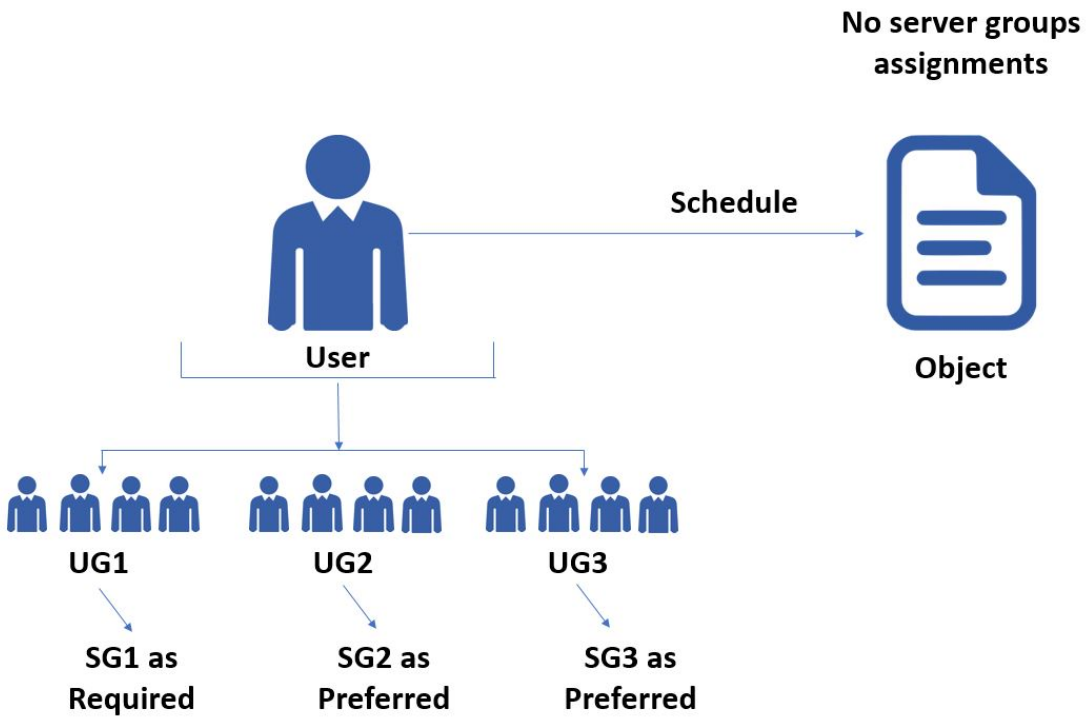
Wanneer een gebruiker een object plant, controleert het platform of er servergroepen aan het object zijn toegewezen. Als er een servergroep aan het object is toegewezen, controleert het platform of de gebruiker weergaverechten voor de servergroep heeft.

In het tweede scenario hebben de gebruiker en zijn gekoppelde gebruikersgroep geen rechten voor SG1. Daarom mislukt de planningstaak. Zorg ervoor dat de gebruiker of eventuele gekoppelde gebruikersgroepen weergaverechten voor SG1 hebben; alleen dan kan de gebruiker een object in dit scenario plannen.

Scenario 3:

> ⓘ Opmerking
>
> Voor de scenario's 3 en 4 gaan we ervan uit dat de gebruiker de rechten van gekoppelde gebruikersgroepen ontvangt.

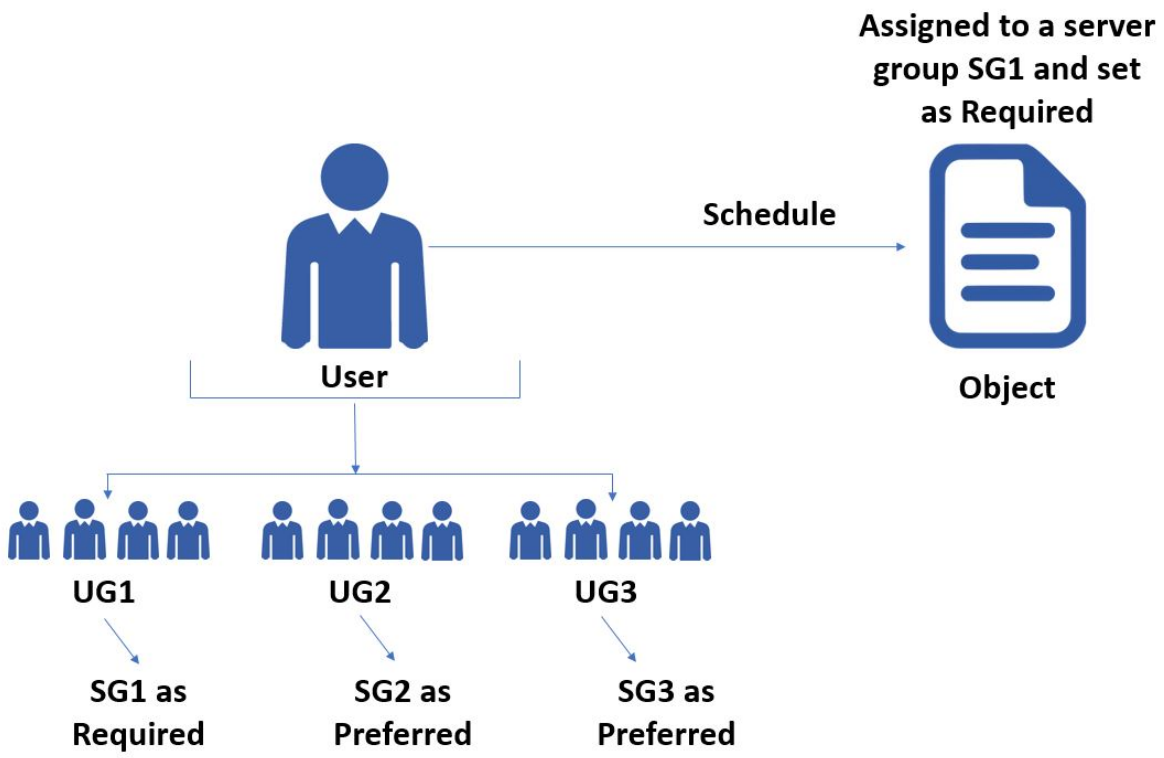
Een gebruiker maakt deel uit van drie gebruikersgroepen, UG1, UG2 en UG3, en u hebt elke gebruikersgroep toegewezen aan respectievelijk SG1, SG2 en SG3. SG1 is ingesteld als vereiste servergroep, en SG2 en SG3 zijn ingesteld als voorkeursservergroepen. Zie *Een gebruikersgroep toewijzen aan een servergroep* in *Beheerdershandleiding voor Business Intelligence-platform* voor meer informatie over het instellen van een servergroep als Vereist of Voorkeursservergroep.



Wanneer een gebruiker aan meerdere gebruikersgroepen is gekoppeld en elke gebruikersgroep aan een andere servergroep is toegewezen, berekent het platform de beschikbare servergroep. In het bovengenoemde scenario wordt de planningstaak succesvol uitgevoerd omdat het object geen servergroepstoewijzingen heeft en de beschikbare servergroep voor het plannen van het object een combinatie van SG1, SG2 en SG3 is.

Scenario 4:

Aanvullend op scenario 3 hebt u het object toegewezen aan SG1 en hebt u SG1 als Vereist ingesteld. Zie *MEen gebruikersgroep toewijzen aan een servergroep* in *Beheerdershandleiding voor Business Intelligence-platform* voor meer informatie over het instellen van een servergroep als Vereist of Voorkeursservergroep.



Wanneer een servergroep wordt toegewezen aan een object, controleert het platform of u de gebruiker weergaverechten voor de servergroep hebt gegeven. In dit scenario berekent het platform niet de beschikbare servergroep omdat een servergroeptoewijzing op objectniveau de hoogste prioriteit heeft. In scenario 4 wordt het object succesvol gepland omdat de UG1 weergaverechten voor SG1 heeft en de gebruiker deze rechten ontvangt van UG1.

> → Onthouden
>
> - Controleer voordat u een object plant de servergroeptoewijzingen aan alle gebruikersgroepen die aan de gebruiker zijn gekoppeld en bereken de beschikbare servergroep.
> - Een planningstaak wordt succesvol uitgevoerd wanneer de beschikbare servergroep voor een gebruiker de servergroep die is toegewezen aan het object omvat.

Zie de onderstaande tabel::

> ⓘ Opmerking
>
> Houd er rekening met dat SG1 en SG2 aan respectievelijk gebruikersgroepen UG1 en UG2 zijn toegewezen.

Toegangsniveau	Combinatie van servergroepen (SG1 + SG2)	Servers zoeken in algemene pool
Gebruiker heeft rechten op alle servergroepen.	Vereist + Vereist	Onwaar

Toegangsniveau	Combinatie van servergroepen (SG1 + SG2)	Servers zoeken in algemene pool
Gebruiker heeft rechten op alle servergroepen.	Vereist + Voorkeursserver	Onwaar
Gebruiker heeft rechten op alle servergroepen.	Voorkeursserver + Voorkeursserver	Waar
Gebruiker heeft op geen enkele servergroep rechten	Vereist + Vereist	Onwaar
Gebruiker heeft op geen enkele servergroep rechten	Vereist + Voorkeursserver	Onwaar
Gebruiker heeft op geen enkele servergroep rechten	Voorkeursserver + Voorkeursserver	Waar
Gebruiker heeft rechten op enkele servergroepen.	Vereist (Nee) + Vereist (Ja)	Onwaar
Gebruiker heeft rechten op enkele servergroepen.	Vereist (Nee) + Voorkeursservergroep (Ja)	Onwaar
Gebruiker heeft rechten op enkele servergroepen.	Vereist (Ja) + Voorkeursservergroep (Nee)	Onwaar
Gebruiker heeft rechten op enkele servergroepen.	Voorkeursservergroep (Nee) + Voorkeursservergroep (Ja)	Waar

11.9 Adaptive Processing Servers configureren voor productiesystemen

Het installatieprogramma installeert één APS (Adaptive Processing Server) per hostsysteem. Afhankelijk van de functies die u hebt geïnstalleerd, kan deze APS host zijn voor een groot aantal services, zoals de Toezichtservice, Service voor promotiebeheer, Multi-Dimensional Analysis Service (MDAS) en Publicatieservice.

Voor productie- of testsystemen kunt u het beste extra Adaptive Processing Servers maken en deze configureren om aan uw bedrijfsvereisten te voldoen.

U kunt op twee manieren extra Adaptive Processing Servers maken:

- Voer de wizard Systeemconfiguratie uit.
  De wizard helpt u bij basisconfiguratie van uw BI-platformsysteem, waaronder het configureren van Adaptive Processing Servers aan de hand van vooraf gedefinieerde implementatiesjablonen. De APS-configuratie van de wizard vormt een goed beginpunt. Er moet echter wel systeemkalibratie worden uitgevoerd.

- Gebruik de CMC om handmatig extra Adaptive Processing Servers te maken en configureren.

Voor meer informatie over het configureren van Adaptive Processing Servers voor productiesystemen raadpleegt u het volgende KBA-artikel op: 1694041.

> → Onthouden
>
> Het selecteren van een implementatiesjabloon in de wizard of handmatig extra Adaptive Processing Servers maken is geen vervanging van systeemkalibratie. Zorg dat kalibratie is uitgevoerd: http://www.sap.com/bisizing.

11.10 Systeemprestaties inventariseren

11.10.1 Toezicht op de BI-platformservers

Met de toepassing Toezicht kunt u historische en runtime-gegevens van BI-platformservers vastleggen voor rapportage en berichtgeving. Met deze toepassing kunnen systeembeheerders bepalen of servers normaal werken en of de verwachte reactietijden worden gehaald.

Verwante informatie

Toezicht [pagina 804]

11.10.2 Servergegevens analyseren

Via de CMC (Central Management Console) kunt u de gegevens van de servers in uw systeem bekijken. Deze gegevens bestaan uit algemene informatie over elke computer en gedetailleerde informatie die specifiek geldt voor het type server. Ook kunt u met de CMC systeemgegevens bekijken, zoals informatie over de versie van het product, de CMS en de huidige systeemactiviteit.

> ⓘ Opmerking
>
> U kunt alleen de gegevens weergeven voor servers die momenteel actief zijn.

11.10.2.1 Servergegevens weergeven

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik met de rechtermuisknop op de gegevens die u wilt weergeven en selecteer *Gegevens*.

Op het tabblad *Gegevens* wordt een lijst met gegevens voor de server weergegeven.

Verwante informatie

De eigenschappen van een server wijzigen [pagina 454]
Informatie over de bijlage Servergegevens [pagina 1193]

11.10.3 Systeemgegevens weergeven

In het beheergebied *Instellingen* van de CMC worden systeemgegevens met algemene informatie over uw BI-platforminstallatie weergegeven. De sectie *Eigenschappen* bevat informatie over de productversie en de build. U ziet hier ook de naam van de gegevensbron, de database en de gebruiker van de CMS-database. De sectie *Globale systeemgegevens weergeven* bevat informatie over de huidige accountactiviteit, samen met statistische gegevens over huidige en verwerkte taken. De sectie *Cluster* bevat de naam van de CMS waarmee u verbinding hebt, de naam van het CMS-cluster en de namen van andere clusterleden.

11.10.3.1 De systeemgegevens weergeven

1. Ga naar het beheergebied *Instellingen* van de CMC.
2. Klik op een pijl om de instellingen in het gebied *Eigenschappen*, *Globale systeemgegevens weergeven*, *Cluster* of *Dynamische back-up* uit te breiden en weer te geven.

11.10.4 Serveractiviteit registreren

Met het BI-platform kunt u specifieke informatie over BI-platformwebactiviteit registreren.

- Verder zijn de servers van het BI-platform zo ontworpen dat er berichten in het standaardsysteemlogboek van uw besturingssysteem worden vastgelegd.
  - In Windows registreert het BI-platform naar de service Gebeurtenislogboek. U kunt de resultaten bekijken met Logboekinzage (in het toepassingslogboek).
  - In UNIX registreert het BI-platform naar de syslog daemon als Gebruikerstoepassing. Elke server voegt de eigen naam en de PID toe aan alle berichten die worden geregistreerd.

Bovendien registreert elke server assertberichten in de registratiemap van de productinstallatie. De programma-informatie in deze bestanden wordt doorgaans alleen door ondersteuningsmedewerkers van SAP BusinessObjects gebruikt voor geavanceerde probleemoplossing. De locatie van deze logboekbestanden is afhankelijk van het besturingssysteem:

- In Windows is de standaardlogboekmap `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\Logging`.
- In UNIX is de standaardlogboekmap `<INSTALLATIEMAP>/sap_bobj/logging`.

Deze logboekbestanden worden automatisch opgeschoond, zodat er nooit meer dan ongeveer 1 MB aan logboekgegevens per server wordt bewaard.

> **Opmerking**
>
> Als u de logboekfunctie wilt inschakelen op UNIX-computers waarop "BI-platform"servers worden gehost, moet u de systeemlogboekregistratie zo instellen en configureren dat alle berichten voor de faciliteit "user" van het niveau info of hoger worden vastgelegd. U moet ook `SYSLOGD` configureren om externe logboekregistratie te accepteren.
>
> De instellingsprocedures verschillen per systeem. Raadpleeg de documentatie bij het besturingssysteem voor specifieke instructies.

11.11 Serverinstellingen configureren

Deze sectie bevat technische informatie en procedures waarin wordt uitgelegd hoe u instellingen voor BI-platformservers kunt wijzigen.

Met de meeste instellingen die in deze sectie worden besproken kunt u het BI-platform effectiever integreren met uw huidige hardware-, software- en netwerkconfiguraties. Welke instellingen u kiest, zal dan ook in grote mate afhangen van uw specifieke behoeften.

U kunt serverinstellingen op twee manieren wijzigen via de CMC (Central Management Console).

- Via het venster *Eigenschappen* voor de server.
- Via het venster *Algemene services bewerken* voor de server.

Houd er rekening mee dat niet alle wijzigingen onmiddellijk van kracht zijn. Als een instelling niet meteen kan worden gewijzigd, wordt in het dialoogvenster *Eigenschappen* of *Algemene services bewerken* de huidige instelling (in het rood) en de gewenste instelling weergegeven. In het beheergebied Servers zult u zien dat de server wordt aangeduid als Oud. Wanneer u de server opnieuw start, wordt de gewenste instellingen gebruikt en de aanduiding Oud van de server verwijderd.

> **Opmerking**
>
> Deze sectie bevat geen informatie over het configureren van de webtoepassingsserver om BI-platformtoepassingen te implementeren. Deze taak wordt over het algemeen uitgevoerd wanneer u het product installeert. Zie de*Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie.

Verwante informatie

Poortnummers configureren [pagina 463]
De eigenschappen van een server wijzigen [pagina 454]
De CMS-systeemdatabase opnieuw maken [pagina 503]
Een nieuwe of bestaande CMS-database selecteren [pagina 501]

11.11.1 De eigenschappen van een server wijzigen

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de server waarvan u de instellingen wilt wijzigen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Breng de gewenste wijzigingen aan en klik op *Opslaan* of *Opslaan en sluiten*.

> **Opmerking**
>
> Niet alle wijzigingen zijn onmiddellijk van kracht. Als een instelling niet meteen kan worden gewijzigd, wordt in het dialoogvenster Eigenschappen zowel de huidige instelling (in rood) als de gewenste instelling weergegeven. In het beheergebied Servers zult u zien dat de server wordt aangeduid als Oud. Wanneer u de server opnieuw start, wordt de gewenste instellingen uit het dialoogvenster Eigenschappen gebruikt en de aanduiding Oud wordt verwijderd.

11.11.2 Service-instellingen op meerdere servers toepassen

U kunt dezelfde instellingen toepassen op services die op meerdere servers worden gehost.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Houd `Ctrl` ingedrukt en klik op elke server die services host waarvoor u instellingen wilt wijzigen. Klik vervolgens met de rechtermuisknop en selecteer *Algemene services bewerken*.
   Het dialoogvenster *Algemene services bewerken* wordt geopend met een lijst met services die op de door u geselecteerde servers worden gehost en die instellingen hebben die u kunt wijzigen.
3. Als in het dialoogvenster *Algemene services bewerken* meerdere services worden weergegeven, selecteert u de gewenste service en klikt u op *Doorgaan*.
4. Breng de gewenste wijzigingen aan en klik op *OK*.

> **Opmerking**
>
> U wordt omgeleid naar het beheergebied *Servers* van de CMC. Als de server opnieuw moet worden opgestart, wordt deze als Oud gemarkeerd. Wanneer u de server opnieuw start, worden de nieuwe instellingen gebruikt en wordt de aanduiding Oud van de server verwijderd.

11.11.3 Werken met configuratiesjablonen

Met configuratiesjablonen kunt u makkelijk meerdere serverexemplaren configureren. Configuratiesjablonen bevatten een lijst met instellingen voor elk servicetype en kunnen worden gebruikt om extra serverexemplaren te configureren. Als u bijvoorbeeld een tiental Web Intelligence-verwerkingsservers hebt die u alle identiek wilt configureren, hoeft u de instellingen voor slechts één server op te geven. Vervolgens gebruikt u de geconfigureerde service om een configuratiesjabloon voor Web Intelligence-verwerkingsservers te maken en past u deze toe op de overige 9 service-exemplaren.

Elk type BI-platformservice heeft een eigen configuratiesjabloon. Er is bijvoorbeeld een configuratiesjabloon voor de Web Intelligence-verwerkingsservice, een voor de publicatieservice, enzovoort. De configuratiesjabloon wordt gedefinieerd in de servereigenschappen in de CMC (Central Management Console).

Als u een configuratiesjabloon hebt opgegeven voor een server, worden bestaande instellingen voor de server overschreven door de waarden uit de sjabloon. In geval u later besluit de sjabloon niet meer te gebruiken, worden de oorspronkelijke instellingen niet hersteld. Wijzigingen die u daarna in de configuratiesjabloon aanbrengt, hebben geen effect op de server.

Het aanbevolen gebruik van configuratiesjablonen is als volgt:

1. Stel de configuratiesjabloon in op één server.
2. Als u dezelfde configuratie gebruiken voor alle servers van hetzelfde type wilt gebruiken, schakelt u *Configuratiesjabloon gebruiken* in voor alle servers van hetzelfde type, ook voor de server waarop u de configuratiesjabloon hebt ingesteld.
3. Mocht u later de configuratie van alle services van dit type willen wijzigen, dan geeft u de eigenschappen van een van de services weer en schakelt u het selectievakje *Configuratiesjabloon gebruiken* uit. Wijzig de gewenste instellingen, selecteer *Configuratiesjabloon instellen* voor deze server en klik op *Opslaan*. Alle services van dat type worden bijgewerkt. Doordat er geen server is die altijd is ingesteld als de configuratiesjabloon, bent u ervan verzekerd dat u de configuratie van alle servers van dat type niet per ongeluk kunt wijzigen.

Verwante informatie

Een configuratiesjabloon instellen [pagina 455]
Een configuratiesjabloon toepassen op een server [pagina 456]

11.11.3.1 Een configuratiesjabloon instellen

U kunt voor type service een configuratiesjabloon instellen. U kunt maar één configuratiesjabloon instellen voor een service. Op de *eigenschappenpagina* van elke willekeurige server kunt u de instellingen opgeven die moeten worden gebruikt door de configuratiesjabloon voor een servicetype dat op de server wordt gehost.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de server die fungeert als host voor de services waarvoor u een configuratiesjabloon wilt instellen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Configureer de service-instellingen die u in de sjabloon wilt gebruiken, schakel het selectievakje *Configuratiesjabloon instellen* in en klik op *Opslaan* of *Opslaan en sluiten*.

De configuratiesjabloon voor het type service dat u hebt geselecteerd, wordt gedefinieerd op basis van de instellingen voor de huidige server. Andere servers van hetzelfde type die fungeren als host voor dezelfde services en waarvoor in de eigenschappen het selectievakje *Configuratiesjabloon gebruiken* is ingeschakeld, worden automatisch meteen opnieuw geconfigureerd aan de hand van de configuratiesjabloon.

> **Opmerking**
>
> Als u de instellingen voor de configuratiesjabloon niet expliciet opgeeft, worden de standaardinstellingen van de service gebruikt.

Verwante informatie

Een configuratiesjabloon toepassen op een server [pagina 456]

11.11.3.2 Een configuratiesjabloon toepassen op een server

Voordat u een configuratiesjabloon toepast, moet u de instellingen definiëren voor de configuratiesjabloon voor het type server waarop u de sjabloon wilt toepassen. Als u de instellingen voor de configuratiesjabloon niet expliciet hebt gedefinieerd, worden de standaardinstellingen voor de service gebruikt.

> **Opmerking**
>
> Servers waarvoor de instelling Configuratiesjabloon gebruiken niet is ingesteld, worden niet bijgewerkt wanneer u de instellingen van de configuratiesjabloon wijzigt.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de server die fungeert als host voor een service waarop u de configuratiesjabloon wilt toepassen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel het selectievakje *Configuratiesjabloon gebruiken* in en klik op *Opslaan* of *Opslaan en sluiten*.

   > **Opmerking**
   >
   > Als de server opnieuw moet worden gestart om de nieuwe instellingen te activeren, wordt de server in de lijst met servers aangeduid als Oud.

De gewenste configuratiesjabloon wordt op de actieve server toegepast. Wijzigingen die eventueel later in de configuratiesjabloon worden aangebracht, zijn van invloed op de configuratie van alle servers die gebruikmaken van deze configuratiesjabloon.

Als u de optie *Configuratiesjabloon gebruiken* uitschakelt, wordt de serverconfiguratie niet hersteld naar de waarden die golden toen de configuratiesjabloon werd geactiveerd. Wijzigingen die in de configuratiesjabloon worden aangebracht, hebben geen effect op de configuratie van de servers die gebruikmaken van de configuratiesjabloon.

Verwante informatie

Een configuratiesjabloon instellen [pagina 455]

11.11.3.3 Standaardwaarden herstellen

Mogelijk wilt u de configuratie van een service weer instellen op de waarden die van toepassing waren toen u de service installeerde, bijvoorbeeld wanneer u de servers niet correct hebt geconfigureerd of wanneer de prestaties te wensen overlaten.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de server die fungeert als host voor de service waarvan u de standaardwaarden wilt herstellen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel het selectievakje *Standaardwaarden herstellen* in en klik op *Opslaan* of *Opslaan en sluiten*.
   De standaardinstellingen voor het desbetreffende servicetype zijn hersteld.

11.12 Netwerkinstellingen van servers configureren

De netwerkinstellingen van BI-platformservers worden beheerd in de CMC. Deze instellingen kunnen in twee categorieën worden verdeeld: poortinstellingen en host-id's.

Standaardinstellingen

Tijdens de installatie worden de host-id's van servers ingesteld op *Automatisch toewijzen*. Aan elke server kan echter een specifiek IP-adres of een specifieke hostnaam worden toegewezen. Het standaard CMS-poortnummer is 6400. De andere BI-platformservers worden dynamisch gebonden aan beschikbare poorten. Poortnummers worden automatisch beheerd door het BI-platform, maar u kunt de CMC-instellingen gebruiken om poortnummers op te geven.

11.12.1 Opties voor netwerkomgeving

Het BI-platform ondersteunt Internet Protocol-versie 4 (IPv4) en gecombineerd IPv4/IPv6-netwerkverkeer. U kunt de server- en clientonderdelen in de volgende omgevingen gebruiken:

- IPv4-netwerk: alle server- en clientonderdelen worden met alleen het IPv4-protocol uitgevoerd.
- Gecombineerd IPv6/IPv4-netwerk: de server- en clientonderdelen worden met zowel het IPv6- als het IPv4-protocol uitgevoerd.
  Dat wil zeggen: hosts met
  - alleen IPv6 (met IPv6-stack ingeschakeld en IPv4-stack geïnstalleerd en uitgeschakeld);
  - gecombineerde IPv6/IPv4 (zowel met IPv6-stack als IPv4-stack ingeschakeld);
  - alleen IPv4 (met IPv4-stack ingeschakeld en IPv6-stack uitgeschakeld of niet geïnstalleerd).

> **Opmerking**
>
> - De netwerkconfiguratie moet bij voorkeur worden uitgevoerd door de systeem- en netwerkbeheerder. Het BI-platform bevat geen mechanisme voor toewijzing van een netwerkomgeving. Gebruik de CMC om een bepaald IPv6- of IPv4-adres te binden aan een van uw BI-platformservers.
> - Uitsluitend IPv6-stack (alleen IPv6 geïnstalleerd en ingeschakeld) wordt niet ondersteund. Gecombineerd IPv6-netwerk wordt wel ondersteund.

11.12.1.1 Gecombineerde IPv6/IPv4-omgeving

In een IPv6/IPv4-netwerkomgeving is het volgende mogelijk:

- BI-platformservers kunnen zowel IPv6- als IPv4-aanvragen verwerken wanneer ze worden uitgevoerd in de gecombineerde IPv6/IPv4-modus.
- Clientonderdelen kunnen samenwerken met servers als IPv4-knooppunt of IPv6/IPv4-knooppunt.

De gecombineerde modus is vooral handig in de volgende scenario's:

- U migreert van een IPv4- naar een gecombineerde IPv6-knooppuntomgeving. Alle client- en serveronderdelen blijven naadloos samenwerken totdat de overdracht is voltooid. Vervolgens kunt u de IPv4-instellingen voor alle servers uitschakelen.
- Software van derden die niet compatibel is met IPv6 blijft werken in de IPv6/IPv4-knooppuntomgeving.

11.12.2 Opties voor host-id van de server

In de CMC kunnen opties voor hostidentificatie worden opgegeven voor alle BI-platformservers. De volgende tabel bevat een beknopt overzicht van de opties in het gebied *Algemene instellingen*:

Optie	Beschrijving
Automatisch toewijzen	Dit is de standaardinstelling voor alle servers. Wanneer dit selectievakje is ingeschakeld, koppelt de server de serverpoort voor aanvragen automatisch aan de eerste netwerkinterface op de computer. **Opmerking** Het is verstandig het selectievakje *Automatisch toewijzen* in te schakelen voor de hostnaam. In sommige gevallen, bijvoorbeeld als de server wordt uitgevoerd op een multi-homed computer of als de server moet werken met een bepaalde firewallconfiguratie, kunt u beter een specifieke hostnaam of specifiek IP-adres opgeven. Raadpleeg de hoofdstukken over het configureren van een

Optie	Beschrijving
	multihomed-computer en het werken met firewalls in de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform*.
Hostnaam	De hostnaam van de netwerkinterface waarop de server luistert naar aanvragen. Voor de CMS geeft deze instelling de hostnaam van de netwerkinterface aan waaraan de Name Server-poort en de poort voor aanvragen op de CMS zijn toegewezen.
IP-adres	Het IP-adres van de netwerkinterface waarop de server luistert naar aanvragen. Voor de CMS geeft deze instelling het adres van de netwerkinterface aan die de CMS gebruikt om de Name Server-poort te binden aan de poort voor aanvragen. Voor elke server zijn aparte velden beschikbaar waarin een IPv4- en/of een IPv6-adres kan worden opgegeven.

⚠ Let op

Als u het selectievakje *Automatisch toewijzen* inschakelt op multihomed-computers, wordt de CMS mogelijk automatisch aan de verkeerde netwerkinterface gekoppeld. Als u dit wilt voorkomen, controleert u of de netwerkinterfaces op de hostcomputer worden weergegeven in de juiste volgorde (via de besturingssysteemprogramma's op de computer). U moet ook de hostnaam opgeven voor de CMS in de CMC.

ⓘ Opmerking

Als u werkt met multihomed-computers of in bepaalde configuraties met een NAT-firewall, moet u mogelijk de hostnaam opgeven met volledige domeinnamen (FQDN-namen) in plaats van met hostnamen.

Verwante informatie

Het systeem configureren voor firewalls [pagina 204]
Een multihomed-computer configureren [pagina 460]
Problemen met meerdere netwerkinterfaces oplossen [pagina 462]

11.12.2.1 De host-id van een server wijzigen

1. Ga naar het beheergebied *Servers* van de CMC.
2. Selecteer de server en kies *Server stoppen* in het menu *Acties*.

3. Kies *Eigenschappen* in het menu *Beheren*.
4. Selecteer een van de volgende opties onder *Algemene instellingen*:

Optie	Beschrijving
Automatisch toewijzen	De server wordt gekoppeld aan een van de beschikbare netwerkinterfaces.
Hostnaam	Voer de hostnaam in van de netwerkinterface waarop de server luistert naar aanvragen.
IP-adres	Typ in de beschikbare vakken een IPv4- of een IPv6-adres voor de netwerkinterface waarop de server luistert naar aanvragen. **Opmerking** Typ een geldig IP-adres in beide vakken als u de server als gecombineerd IPv4/IPv6-knooppunt wilt uitvoeren.

5. Klik op *Opslaan* of op *Opslaan en sluiten*.
   De wijzigingen worden weergegeven op de opdrachtregel op het tabblad *Eigenschappen*.
6. Start de server en schakel deze in.

11.12.3 Een multihomed-computer configureren

Een multihomed-computer is een computer met meerdere netwerkadressen. U hebt hiervoor meerdere netwerkinterfaces nodig die elk een of meer IP-adressen hebben, of één netwerkinterface waaraan meerdere IP-adressen zijn toegewezen.

Als u meerdere netwerkinterfaces met elk één IP-adres hebt, wijzigt u de koppelingsvolgorde zo dat de netwerkinterface waaraan u de BI-platformservers wilt koppelen bovenaan staat. Als de interface meerdere IP-adressen heeft, gebruikt u de optie Host-id's in de CMC om een netwerkinterface op te geven voor de BI-platformserver. U kunt de hostnaam of het IP-adres opgeven. Voor meer informatie over het configureren van de instelling *Host-id's* raadpleegt u “Problemen met meerdere netwerkinterfaces oplossen”.

> **→ Tip**
>
> In deze sectie wordt behandeld hoe u alle servers tot hetzelfde netwerkadres beperkt, maar het is ook mogelijk afzonderlijke servers aan verschillende adressen te koppelen. U kunt bijvoorbeeld de File Repository Servers koppelen aan een privé-adres dat niet routeerbaar is vanaf de computers van gebruikers. Bij dergelijke geavanceerde configuraties moet de DNS-configuratie het gegevensverkeer effectief routeren tussen alle BI-platformserveronderdelen. In dit voorbeeld moet de DNS-server het gegevensverkeer vanaf de andere BI-platformservers naar het privé-adres van de File Repository Servers routeren.

Verwante informatie

Problemen met meerdere netwerkinterfaces oplossen [pagina 462]

11.12.3.1 De CMS koppelen aan een netwerkadres

> **Opmerking**
>
> Op een multi-homed computer kunt u de host-id instellen op de volledige domeinnaam of het IP-adres van de interface waaraan u de server wilt koppelen.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de CMS.
3. Selecteer een van de volgende opties onder *Algemene instellingen*:
   - *Hostnaam*
   - Typ de hostnaam van de netwerkinterface waaraan u de server wilt koppelen.
   - *IP-adres*
   - Typ in de beschikbare vakken een IPv4- of een IPv6-IP-adres voor de netwerkinterface waaraan u de server wilt koppelen.

     > **Opmerking**
     >
     > Typ een geldig IP-adres in beide vakken als u de server als gecombineerd IPv4/IPv6-knooppunt wilt uitvoeren.

   > **Let op**
   >
   > Schakel het selectievakje Automatisch toewijzen niet in.
4. Voor *Poort voor aanvragen* kunt u een van de volgende handelingen uitvoeren:
   - Selecteer de optie *Automatisch toewijzen*.
   - Typ een geldig poortnummer in het veld *Poort voor aanvragen*.
5. Controleer of u een poortnummer hebt opgegeven in het dialoogvenster Name Server-poort.

   > **Opmerking**
   >
   > De standaardpoort is 6400.

11.12.3.2 De overige servers koppelen aan een netwerkadres

Voor de resterende BI-platformservers worden de poorten standaard dynamisch geselecteerd. Zie voor meer informatie over het uitschakelen van de instelling Automatisch toewijzen waarmee deze gegevens dynamisch worden doorgevoerd “De poort wijzigen waarop een server aanvragen accepteert”.

Verwante informatie

De poort wijzigen waarop een server aanvragen accepteert [pagina 465]

11.12.3.3 Problemen met meerdere netwerkinterfaces oplossen

Op een multi-homed computer wordt de CMS mogelijk gekoppeld aan een onjuiste netwerkinterface. U kunt dit voorkomen door ervoor te zorgen dat de netwerkinterfaces op de hostcomputer in de juiste volgorde zijn vermeld (gebruik hiervoor de hulpprogramma's van het besturingssysteem op de computer) en de hostnaam voor de CMS op te geven in de CMC. Als de primaire netwerkinterface niet routeerbaar is, kunt u de volgende procedure gebruiken om het BI-platform te koppelen aan een niet-primaire routeerbare netwerkinterface. Voer deze stappen direct na de installatie van het BI-platform op de lokale computer uit, voordat u het BI-platform op andere computers installeert.

1. Open de CCM en stop de SIA voor het knooppunt op de computer die meerdere netwerkinterfaces heeft.
2. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*.
3. Klik in het dialoogvenster *Eigenschappen* op het tabblad *Configuratie*.
4. Als u de SIA aan een specifieke netwerkinterface wilt koppelen, voert u het poortnummer van de doelnetwerkinterface in het veld *Poort* in.
5. Klik op *OK* en selecteer het tabblad *Opstarten*.
6. Selecteer de CMS in de lijst *Lokale CMS-servers* en klik op *Eigenschappen.*
7. Als u de CMS aan een specifieke netwerkinterface wilt koppelen, voert u het poortnummer van de doelnetwerkinterface in het veld *Poort* in.
8. Klik op *OK* om de nieuwe instellingen toe te passen.
9. Start de SIA en wacht totdat de servers worden gestart.
10. Start de CMC (Central Management Console) en ga naar het beheergebied *Servers*. Herhaal de stappen 11 tot en met 14 voor elke server.
11. Selecteer de server en kies *Server stoppen* in het menu *Acties*.
12. Kies *Eigenschappen* in het menu *Beheren*.
13. Selecteer een van de volgende opties onder *Algemene instellingen*:
    - Hostnaam: typ de hostnaam van de netwerkinterface waaraan u de server wilt koppelen.
    - IP-adres: typ in de beschikbare vakken een IPv4- of een IPv6-IP-adres voor de netwerkinterface waaraan u de server wilt koppelen.

      > **Opmerking**
      >
      > Typ een geldig IP-adres in beide vakken als u de server als gecombineerd IPv4/IPv6-knooppunt wilt uitvoeren.

    > **Let op**
    >
    > Schakel het selectievakje Automatisch toewijzen niet in.
14. Klik op *Opslaan* of op *Opslaan en sluiten*.
15. Ga terug naar de CCM en start de SIA opnieuw.

    Alle servers in het knooppunt worden opnieuw gestart door de SIA. Alle servers op de computer worden nu aan de juiste netwerkinterface gekoppeld.

11.12.4 Poortnummers configureren

Tijdens de installatie gebruikt de CMS standaardpoortnummers. De standaard CMS-poort is 6400. Deze poort valt binnen het bereik dat door SAP BusinessObjects voor poorten wordt gereserveerd (6400 tot en met 6410). De communicatie via deze poorten zou niet tegenstrijdig moeten zijn met eventuele toepassingen van derden.

Alle andere servers van het BI-platform worden bij het starten en inschakelen dynamisch aan een beschikbare poort (hoger dan 1024) gekoppeld. Vervolgens wordt deze poort bij de CMS geregistreerd en wordt er via deze poort op BI-platformaanvragen gecontroleerd. U kunt zo nodig voor elk serveronderdeel opgeven dat er via een speciale poort wordt gecontroleerd (in plaats van dat er dynamisch een beschikbare poort wordt geselecteerd). U moet bijvoorbeeld handmatig een aanvraagpoort voor elke BI-platformserver configureren die via een firewall moet communiceren.

U kunt poortnummers opgeven op het tabblad Eigenschappen voor elke server in de CMC. In de volgende tabel wordt een overzicht gegeven van de opties in het gebied *Algemene instellingen* voor poortgebruik bij specifieke typen servers.

Instelling	CMS	Andere servers
Poort voor aanvragen	De poort die de CMS gebruikt voor het accepteren van alle aanvragen van andere servers (behalve aanvragen van Name Server-computers). Hiervoor wordt dezelfde netwerkinterface gebruikt als voor de Name Server-poort. Wanneer *Automatisch toewijzen* is ingeschakeld, wordt op de server automatisch een poortnummer gebruikt dat is toegewezen door het besturingssysteem.	De poort waarop de server luistert naar alle aanvragen. Wanneer *Automatisch toewijzen* is geselecteerd, gebruikt de server automatisch een poortnummer dat door het besturingssysteem is toegewezen.
Name Server-poort	Hiermee geeft u de BI-platformpoort op waarop de CMS luistert naar naamservice-aanvragen. De standaardwaarde is 6400.	Niet van toepassing.

11.12.4.1 De standaardpoort voor de CMS wijzigen in de CMC

indien reeds een CMS in het cluster wordt uitgevoerd, kunt u de CMC gebruiken om de standaardpoort voor de CMS te wijzigen. Als er geen CMS op het cluster wordt uitgevoerd, gebruikt u de CCM onder Windows of het script `serverconfig.sh` onder UNIX om het poortnummer te wijzigen.

> **Opmerking**
>
> op de CMS wordt dezelfde netwerkinterfacekaart gebruikt voor de poort voor aanvragen en de Name Server-poort.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de CMS in de serverlijst.
3. Vervang het nummer van de *Name Server-poort* door het nummer van de poort waarop de CMS moet luisteren. (De standaardpoort is 6400.)
4. Klik op *Opslaan en sluiten*.

5. Start de CMS opnieuw.

   De CMS luistert op de opgegeven poort. Met de Server Intelligence Agent worden de nieuwe instellingen dynamisch doorgevoerd naar de andere servers op het knooppunt als voor deze servers de optie *Automatisch toewijzen* is ingeschakeld voor de poort voor aanvragen. (Het kan enkele minuten duren voordat de wijzigingen worden weergegeven in de eigenschapsinstellingen van alle knooppuntleden.)

   De instellingen die u opgeeft op de pagina *Eigenschappen* worden weergegeven op de serveropdrachtregel, die zich ook op de pagina *Eigenschappen* bevindt.

11.12.4.2 De standaard CMS-poort wijzigen in de CCM onder Windows

Als er geen CMS toegankelijk is op het cluster en u de standaardpoort voor CMS voor een of meer CMS-en in de implementatie wilt wijzigen, gebruikt u de CCM om het CMS-poortnummer te wijzigen.

1. Open de CCM en stop de SIA voor het knooppunt.
2. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*.
3. Klik in het dialoogvenster *Eigenschappen* op het tabblad *Opstarten*.
4. Selecteer in de lijst *Lokale CMS-servers* de CMS waarvan u het poortnummer wilt wijzigen en klik op *Eigenschappen*.
5. Als u de CMS aan een specifieke poort wilt binden, voert u het poortnummer in het veld *Poort* in.
6. Klik op *OK* om de nieuwe instellingen toe te passen.
7. Start de SIA en wacht totdat de servers worden gestart.

11.12.4.3 De standaard CMS-poort wijzigen in de CCM in Unix

Als er geen CMS toegankelijk is op het cluster en u de standaardpoort voor CMS voor een of meer CMS's in de implementatie wilt wijzigen, gebruikt u het script `serverconfig.sh` om het CMS-poortnummer te wijzigen.

1. Gebruik het script `ccm.sh` om de SIA (Server Intelligence Agent) te stoppen waarop de CMS waarvan u het poortnummer wilt wijzigen, wordt gehost.
2. Voer het script `serverconfig.sh` uit.

   Dit script bevindt zich standaard in de map `<InstallDir>/sap_bobj`.
3. Selecteer *3 - Knooppunt verwijderen* en druk op `Enter`.
4. Selecteer het knooppunt waarop de CMS wordt gehost die u wilt wijzigen en druk op `Enter`.
5. Selecteer *3 - Een lokale CMS wijzigen* en druk op `Enter`.
   Er wordt een lijst weergegeven met CMS-exemplaren die op het knooppunt worden gehost.
6. Selecteer de CMS die u wilt wijzigen en druk op `Enter`.
7. Typ het nieuwe poortnummer voor de CMS en druk op `Enter`.
8. Geef op of de CMS automatisch moet worden gestart als de SIA wordt gestart en druk op `Enter`.
9. Typ de opdrachtregelargumenten voor de CMS of accepteer de huidige argumenten en druk op `Enter`.
10. Typ **`quit`** om het script af te sluiten.

11. Start de SIA met het script `ccm.sh` en wacht tot de servers worden gestart.

11.12.4.4 De poort wijzigen waarop een CMS aanvragen accepteert

1. Ga naar het beheergebied *Servers* van de CMC.
2. Selecteer de CMS en kies *Eigenschappen* in het menu *Beheer*.
3. Schakel onder *Algemene instellingen* het selectievakje *Automatisch toewijzen* voor *Poort voor aanvragen* uit en typ het nummer van de poort waarop de server moet luisteren.
4. Klik op *Opslaan* of op *Opslaan en sluiten*.
5. Start de CMS opnieuw.

De CMS wordt gekoppeld aan de nieuwe poort en begint met controleren op aanvragen van andere servers.

11.12.4.5 De poort wijzigen waarop een server aanvragen accepteert

> **Opmerking**
>
> Deze stappen kunnen niet worden gebruikt om de poort voor aanvragen voor de CMS (Central Management Server) te wijzigen. Zie in plaats daarvan "De poort wijzigen waarop een CMS aanvragen accepteert".

1. Ga naar het beheergebied *Servers* van de CMC.
2. Selecteer de server en kies *Server stoppen* in het menu *Acties*.
3. Dubbelklik op de server.
   Het scherm *Eigenschappen* wordt weergegeven.
4. Schakel onder *Algemene instellingen* het selectievakje *Automatisch toewijzen* voor *Poort voor aanvragen* uit en typ het nummer van de poort waarop de server moet luisteren.
5. Klik op *Opslaan* of op *Opslaan en sluiten*.
6. Start de server en schakel deze in.

De server wordt gekoppeld aan de nieuwe poort. Na registratie bij de CMS luistert de server naar BI-platformaanvragen op de nieuwe poort.

11.13 Knooppunten beheren

11.13.1 Knooppunten gebruiken

Een knooppunt is een groep BI-platformservers die op dezelfde host worden uitgevoerd en door dezelfde SIA (Server Intelligence Agent) worden beheerd. Alle servers op een knooppunt worden onder dezelfde

gebruikersaccount uitgevoerd. Eén computer kan vele knooppunten bevatten, zodat u processen onder verschillende gebruikersaccounts kunt uitvoeren. Met één SIA worden alle servers op een knooppunt beheerd en gecontroleerd, om ervoor te zorgen dat deze correct werken.

> **Opmerking**
>
> U moet een beheerdersaccount met Enterprise-verificatie gebruiken om alle procedures voor knooppuntbeheer veilig uit te voeren. Als SSL-communicatie tussen servers echter is geactiveerd, moet u SSL uitschakelen voordat u beheerprocedures voor knooppunten uit kunt voeren.

> **Opmerking**
>
> Zorg dat alle databasestuurprogramma's aanwezig zijn die BI-platformservers nodig hebben om verbinding te maken met hun gegevensbronnen (bijvoorbeeld zodat de CMS verbinding kan maken met de CMS-database), en dat de juiste omgeving al is ingesteld (dat bijvoorbeeld toepasselijke omgevingsvariabelen zijn ingesteld).

11.13.1.1 Variabelen

Variabele	Beschrijving
`<INSTALLDIR>`	De map waarin het SAP BusinessObjects Business Intelligence-platform is geïnstalleerd. In Windows: `C:\Program Files (x86)\SAP BusinessObjects`
`<SCRIPTDIR>`	De map waarin de scripts voor knooppuntbeheer zich bevinden. • In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` • In Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`
`<PLATFORM32>`	De naam van uw Unix-besturingssysteem. Geldige waarden zijn: • `aix_rs6000` • `linux_x86` • `solaris_sparc` • `win32_x86`
`<PLATFORM64>`	De naam van uw Unix-besturingssysteem. Geldige waarden zijn: • `aix_rs6000_64`

Variabele	Beschrijving
	• `linux_x64` • `solaris_sparcv9` • `win64_x64`

11.13.1.2 Een Unix-computer voorbereiden voor SQL Anywhere

U moet een `odbc.ini`-bestand aanmaken en activeren voordat u SQL Anywhere kunt gebruiken als een ODBC-gegevensbron op een Unix-computer.

> **Opmerking**
>
> Deze procedure is niet nodig als u de gebundelde SQL Anywhere gebruikt die bij het BI-platform is geïnstalleerd.

1. Maak `odbc.ini` in `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM64>`.
2. Voer de naam van de gegevensbron (DSN), de naam van de database en server voor SQL Anywhere in, evenals het IP-adres en poortnummer van de computer waarop de SQL Anywhere-databaseserver wordt gehost.
3. Sla `odbc.ini` op.
4. Breng de SQL Anywhere-omgeving naar uw huidige omgeving.

   Als u bijvoorbeeld Bash als uw opdrachtregel-shell gebruikt, zoekt u de 64-bits bronversie van `sa_config.sh`.
5. Definieer een omgevingsvariabele met de naam `ODBCINI` die wijst naar de locatie waar het bestand `odbc.ini` is gemaakt.

   Stel die omgevingsvariabele zo in dat onderliggende processen de omgevingsvariabele `ODBCINI` kunnen zien.

Voorbeeld

Een voorbeeld van een `odbc.ini`-bestand:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0
[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Een voorbeeld van een `source`-opdracht:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Verwante informatie

Variabelen [pagina 466]

11.13.2 Een nieuw knooppunt toevoegen

Het installatieprogramma maakt één knooppunt wanneer u het BI-platform voor het eerst installeert.

U hebt mogelijk extra knooppunten nodig als u servers onder verschillende gebruikersaccounts wilt uitvoeren.

U kunt een nieuw knooppunt toevoegen met de CCM (Central Configuration Manager) of door gebruik te maken van een script voor knooppuntbeheer. Als u een firewall gebruikt, moet u ervoor zorgen dat de poorten van uw SIA (Server Intelligence Agent) en CMS (Central Management Server) open zijn.

> **ⓘ Opmerking**
>
> Gebruik de CCM of het script voor knooppuntbeheer op de computer waarop u een knooppunt wilt toevoegen. U kunt niet een knooppunt op een externe computer toevoegen.

Een BI-platforminstallatie is een uniek exemplaar van de BI-platformbestanden die door het installatieprogramma op een computer zijn gemaakt. Een exemplaar van een BI-platforminstallatie kan alleen in één cluster worden gebruikt. Knooppunten die tot verschillende clusters behoren met dezelfde BI-platforminstallatie, worden niet ondersteund, omdat er geen patch of update op dit type implementatie kan worden toegepast. Alleen Unix-platforms ondersteunen meerdere installaties van de software op dezelfde computer, en alleen als elke installatie wordt uitgevoerd onder een unieke gebruikersaccount en in een aparte map, zodat de installaties geen bestanden delen.

Alle computers in het cluster moeten dezelfde versie en hetzelfde patchniveau hebben.

> **→ Aanbeveling**
>
> Voor het toevoegen van knooppunten aan een BI-platformimplementatie waarin FIPS is ingeschakeld en CORBA SSL is geconfigureerd, wordt aangeraden om de optie "Een nieuwe tijdelijke CMS starten" te gebruiken.
>
> Voor het toevoegen van knooppunten aan een BI-platformimplementatie waarin FIPS niet is ingeschakeld en CORBA SSL is geconfigureerd, wordt aangeraden om de optie "Een nieuwe tijdelijke CMS starten" te gebruiken.
>
> Voor het toevoegen van knooppunten aan een BI-platformimplementatie waarin FIPS is ingeschakeld en CORBA SSL niet is geconfigureerd, wordt aangeraden om de bestaande CMS te gebruiken.

11.13.2.1 Een nieuw knooppunt aan een computer toevoegen voor een bestaande implementatie.

U kunt automatisch het eerste knooppunt op een computer maken wanneer u het installatieprogramma gebruikt om een nieuwe computer aan een bestaande implementatie toe te voegen.

> → Tip
>
> Klik tijdens de installatie op *Uitvouwen* en geef uw bestaande Central Management Server op.

Gebruik de Central Configuration Manager of het script `serverconfig.sh` als u extra knooppunten wilt maken.

Zie de *Installatiehandleiding voor SAP BI-platform* voor meer informatie over de installatie.

11.13.2.2 Een knooppunt toevoegen in Windows.

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt toevoegt.

1. Klik op *Knooppunt toevoegen* op de werkbalk in de CCM (Central Configuration Manager).
2. Voer in de *wizard Knooppunt toevoegen* de knooppuntnaam en het poortnummer in voor de nieuwe SIA (Server Intelligence Agent).
3. Bepaal of u servers wilt maken op het nieuwe knooppunt.
   - *Knooppunt toevoegen zonder servers*
   - *Knooppunt toevoegen met CMS*
   - *Knooppunt toevoegen met standaardservers*
     Met deze optie worden alleen de servers gemaakt die op deze computer zijn geïnstalleerd. Dit omvat niet alle mogelijke servers.
4. Selecteer een CMS.
   - Als uw implementatie actief is, selecteert u *Bestaande actieve CMS gebruiken* en klikt u op *Volgende*. Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS, de beheerdersreferenties, de naam van de gegevensbron, de referenties voor de systeemdatabase en de clustersleutel.
   - Als uw implementatie gestopt is, selecteert u *Een nieuwe tijdelijke CMS starten* en klikt u op *Volgende*. Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de tijdelijke CMS, de beheerdersreferenties, de naam van de gegevensbron, de referenties voor de systeemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > ⚠ Let op
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is. Zorg ervoor dat de bestaande en nieuwe CMS andere poorten gebruiken.

5. Controleer de bevestigingspagina en klik op *Voltooien*.
   De CCM maakt een knooppunt. Als er een fout optreedt, raadpleeg dan het logbestand.

U kunt nu de CMS gebruiken om het nieuwe knooppunt te starten.

11.13.2.2.1 Een knooppunt toevoegen in Windows met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt toevoegt.

U kunt `AddNode.bat` gebruiken om een knooppunt toe te voegen op een Windows-computer. Voor meer informatie raadpleegt u de sectie “Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten”.

Voorbeeld

Vanwege de beperkingen van de opdrachtprompt moet u het dakje (^) gebruiken om een escape uit te voeren op spaties, het gelijkteken (=) en de puntkomma (;) in deze parameters, tenzij u de tekst omsluit met aanhalingstekens.

```
<SCRIPTDIR>\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
```

> ⓘ Opmerking
>
> Als u de caret niet wilt gebruiken in lange tekenreeksen, kunt u de naam van het script en alle bijbehorende parameters naar een tijdelijk `response.bat`-bestand schrijven om vervolgens het `response.bat`-bestand zonder parameters uit te voeren.

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.2.3 Een knooppunt toevoegen in Unix

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt toevoegt.

1. `<INSTALLATIEMAP>/sap_bobj/serverconfig.sh` uitvoeren
2. Selecteer *1 - Add node* en druk op `Enter`.
3. Typ de naam van het nieuwe knooppunt en druk op `Enter`.
4. Typ het poortnummer van de nieuwe SIA in en druk op `Enter`.
5. Bepaal of u servers wilt maken op het nieuwe knooppunt.
   - *no servers*
     Hiermee wordt een knooppunt gemaakt dat geen servers bevat.
   - *cms*
     Hiermee wordt een CMS op het knooppunt gemaakt, maar geen andere servers.
   - *default servers*
     Hiermee worden alleen de servers gemaakt die op deze computer zijn geïnstalleerd. Dit omvat niet alle mogelijke servers.
6. Selecteer een CMS.
   - Als uw implementatie actief is, selecteert u *existing* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS, de beheerdersreferenties, de databaseverbindingsgegevens en de referenties voor de systeemdatabase en de clustersleutel.
   - Als uw implementatie gestopt is, selecteert u *temporary* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de tijdelijke CMS, de beheerdersreferenties, de databaseverbindingsgegevens en de referenties voor de systeemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > ⚠ Let op
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is. Zorg ervoor dat de bestaande en nieuwe CMS andere poorten gebruiken.
7. Controleer de bevestigingspagina en druk op `Enter`.
   De CCM maakt een knooppunt. Als er een fout optreedt, raadpleeg dan het logbestand.

U kunt nu `<INSTALLATIEMAP>/sap_bobj/ccm.sh -start <knooppuntnaam>` uitvoeren om een nieuwe knooppunt te starten.

11.13.2.3.1 Een knooppunt toevoegen in Unix met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt toevoegt.

U kunt `addnode.sh` gebruiken om een knooppunt toe te voegen op een Unix-computer. Voor meer informatie raadpleegt u de sectie "Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten".

Voorbeeld

```
<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=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.3 Een knooppunt opnieuw maken

U kunt een knooppunt opnieuw maken met de CCM (Central Configuration Manager) of een script voor knooppuntbeheer, nadat u de serverconfiguratie voor het hele cluster hebt hersteld, of als de computer waarop uw implementatie wordt gehost vastloopt, beschadigd raakt of een beschadigd bestandsysteem heeft. Volg hierbij de volgende richtlijnen:

- Het is niet nodig om een knooppunt opnieuw te maken als u de implementatie opnieuw installeert op een vervangende computer met identieke installatieopties en knooppuntnaam. Het installatieprogramma maakt het knooppunt automatisch opnieuw.
- Een knooppunt hoeft alleen opnieuw gemaakt te worden op een computer met een bestaande implementatie met identieke installatieopties en identiek patchniveau.

- U mag knooppunten alleen opnieuw maken als ze niet op de computers in uw implementatie voorkomen. Zorg ervoor dat andere computers niet hetzelfde knooppunt hosten.
- Hoewel u met de implementatie knooppunten kunt uitvoeren op verschillende besturingssystemen, mag u knooppunten alleen opnieuw maken op computers met hetzelfde besturingssysteem.
- Als u een firewall gebruikt, moet u ervoor zorgen dat de poorten van uw SIA (Server Intelligence Agent) en CMS (Central Management Server) open zijn.

> ⓘ Opmerking
>
> Alle servers behalve de CMS moeten worden gestopt voordat u een knooppunt opnieuw kunt maken.

> → Onthouden
>
> U kunt een knooppunt alleen opnieuw maken op de computer waarop het knooppunt zich bevindt.

11.13.3.1 Een knooppunt maken in Windows

1. Klik op *Knooppunt toevoegen* op de werkbalk in de CCM (Central Configuration Manager).
2. Voer in de *wizard Knooppunt toevoegen* de knooppuntnaam en het poortnummer in voor de opnieuw gemaakte SIA (Server Intelligence Agent).

   > ⓘ Opmerking
   >
   > De namen van de oorspronkelijke en opnieuw gemaakte knooppunten moeten identiek zijn.

3. Selecteer *Knooppunt opnieuw maken* en klik op *Volgende*.
   - Als het knooppunt voorkomt in de systeemdatabase van de CMS (Central Management Server), wordt het opnieuw gemaakt op de lokale host.

     > ⚠ Let op
     >
     > Gebruik deze optie alleen als het knooppunt niet voorkomt op andere hosts in het cluster.

   - Als het knooppunt niet aanwezig is in de systeemdatabase van de CMS, wordt er een nieuw knooppunt met standaardservers toegevoegd. Standaardservers omvatten alle servers die op de host geïnstalleerd zijn.
4. Selecteer een CMS.
   - Als uw CMS actief is, selecteert u *Bestaande actieve CMS uitvoeren* en klikt u op *Volgende*.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS, de beheerdersreferenties, de naam van de gegevensbron, de referenties voor de systeemdatabase en de clustersleutel.
   - Als uw CMS gestopt is, selecteert u *Een tijdelijke CMS starten* en klikt u op *Volgende*.
     Als hierom wordt gevraagd, voert u de hostnaam in voor de tijdelijke CMS, de beheerdersreferenties, de naam van de gegevensbron, de referenties voor de systeemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > ⚠ Let op
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is.

5. Controleer de bevestigingspagina en klik op *Voltooien*.
   De CCM maakt het knooppunt opnieuw en voegt informatie over het knooppunt toe aan de lokale computer. Als er een fout optreedt, raadpleeg dan het logbestand.

U kunt nu de CCM gebruiken om het opnieuw gemaakte knooppunt te starten.

11.13.3.1.1 Een knooppunt opnieuw maken in Windows met behulp van een script

U kunt `AddNode.bat` gebruiken om een knooppunt opnieuw te maken op een Windows-computer. Voor meer informatie raadpleegt u de sectie "Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten".

Voorbeeld

Vanwege de beperkingen van de opdrachtprompt moet u het dakje (^) gebruiken om een escape uit te voeren op spaties, het gelijkteken (=) en de puntkomma (;) in deze parameters, tenzij u de tekst omsluit met aanhalingstekens.

```
<SCRIPTDIR>\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
```

> ⓘ Opmerking
>
> Als u de caret niet wilt gebruiken in lange tekenreeksen, kunt u de naam van het script en alle bijbehorende parameters naar een tijdelijk `response.bat`-bestand schrijven om vervolgens het `response.bat`-bestand zonder parameters uit te voeren.

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.3.2 Een knooppunt opnieuw maken in Unix

1. `<INSTALLATIEMAP>/sap_bobj/serverconfig.sh` uitvoeren
2. Selecteer *1 - Add node* en druk op `Enter`.
3. Typ de naam van het nieuwe knooppunt en druk op `Enter`.

   > **Opmerking**
   >
   > De namen van de oorspronkelijke en opnieuw gemaakte knooppunten moeten identiek zijn.

4. Typ het poortnummer van de nieuwe SIA in en druk op `Enter`.
5. Selecteer *Knooppunt opnieuw maken* en druk op `Enter`.
   - Als het knooppunt voorkomt in de systeemdatabase van de CMS (Central Management Server), wordt het opnieuw gemaakt op de lokale host.

     > **Let op**
     >
     > Gebruik deze optie alleen als het knooppunt niet voorkomt op andere hosts in het cluster.

   - Als het knooppunt niet aanwezig is in de systeemdatabase van de CMS, wordt er een nieuw knooppunt met standaardservers toegevoegd. Standaardservers omvatten alle servers die op de host geïnstalleerd zijn.
6. Selecteer een CMS.
   - Als uw implementatie actief is, selecteert u *existing* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS, de beheerdersreferenties, de databaseverbindingsgegevens en de referenties voor de systeemdatabase en de clustersleutel.
   - Als uw implementatie gestopt is, selecteert u *temporary* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam in voor de tijdelijke CMS, de beheerdersreferenties, de databaseverbindingsgegevens en de referenties voor de systeemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > **Let op**
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is.

7. Controleer de bevestigingspagina en druk op `Enter`.
   De CCM maakt het knooppunt opnieuw en voegt informatie over het knooppunt toe aan de lokale computer. Als er een fout optreedt, raadpleeg dan het logbestand.

U kunt nu `<INSTALLATIEMAP>/sap_bobj/ccm.sh -start <knooppuntnaam>` uitvoeren om het opnieuw gemaakte knooppunt te starten

11.13.3.2.1 Een knooppunt opnieuw maken in Unix met behulp van een script

U kunt `addnode.sh` gebruiken om een knooppunt opnieuw te maken op een Unix-computer. Voor meer informatie raadpleegt u de sectie “Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten”.

Voorbeeld

```
<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
```

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.4 Een knooppunt verwijderen

U kunt een gestopt knooppunt verwijderen met een actieve CCM (Central Configuration Manager) of met behulp van een script voor knooppuntbeheer. Volg hierbij de volgende richtlijnen:

- Wanneer u een knooppunt verwijdert, worden ook de servers op het knooppunt permanent verwijderd.
- Als uw cluster meerdere computers omvat, verwijdert u de knooppunten voordat u een computer uit een cluster verwijdert en verwijder de software van de computer. Als u een computer uit een cluster verwijdert voordat u een knooppunt verwijdert, of als het bestandsysteem op een computer slecht werkt, moet u het knooppunt opnieuw maken op een andere computer met dezelfde servers, in hetzelfde cluster, om vervolgens het knooppunt te verwijderen.

> → Onthouden
>
> U kunt een knooppunt alleen verwijderen op de computer waarop het knooppunt zich bevindt.

Verwante informatie

Een knooppunt opnieuw maken [pagina 472]

11.13.4.1 Een knooppunt verwijderen in Windows

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt verwijdert.

1. De CCM (Central Configuration Manager) uitvoeren.
2. Stop in de CCM het knooppunt dat u wilt verwijderen.
3. Selecteer het knooppunt en klik op de werkbalk op *Knooppunt verwijderen*.
4. Als u daarom gevraagd wordt, voert u de hostnaam, de poort en de beheerdersreferenties voor de CMS in.

In de CCM worden het knooppunt en alle servers op het knooppunt verwijderd.

> ⓘ Opmerking
>
> U kunt een nieuw toegevoegd knooppunt verwijderen na het configureren van SSL op de volgende twee manieren:
>
> - Verwijder de SSL-parameters uit het nieuw gemaakte knooppunt en het SIA-knooppunt waarvan u CMSes probeert te verbinden.
> - Voeg de volgende SSL-parameters toe aan RemoveNode.bat vóór de declaratie van de hoofdklasse en voer het bestand uit: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Pad naar de map van SSL-certificaat" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.1.1 Een knooppunt verwijderen in Windows met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt verwijdert.

U kunt `RemoveNode.bat` gebruiken om een knooppunt te verwijderen van een Windows-computer. Voor meer informatie raadpleegt u de sectie “Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten”.

Voorbeeld

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.4.2 Een knooppunt verwijderen van Unix

Maak een back-up van de serverconfiguratie voor het gehele cluster voor en nadat u een knooppunt verwijdert.

1. Voer `<INSTALLATIEMAP>/sap_bobj/ccm.sh -stop <knooppuntnaam>` uit om het knooppunt dat u wilt verwijderen, te stoppen.
2. `<INSTALLATIEMAP>/sap_bobj/serverconfig.sh` uitvoeren
3. Selecteer *2 - Knooppunt verwijderen* en druk op `Enter`.
4. Selecteer het knooppunt dat u wilt verwijderen en druk op `Enter`.
5. Als u daarom gevraagd wordt, voert u de hostnaam, het poortnummer en de beheerdersreferenties voor de CMS in.

Het knooppunt en alle servers op het knooppunt worden verwijderd.

> **Opmerking**
>
> U kunt een nieuw toegevoegd knooppunt verwijderen na het configureren van SSL op de volgende twee manieren:
>
> - Verwijder de SSL-parameters uit het nieuw gemaakte knooppunt en het SIA-knooppunt waarvan u CMSes probeert te verbinden.
> - Voeg de volgende SSL-parameters toe aan RemoveNode.bat vóór de declaratie van de hoofdklasse en voer het bestand uit: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Pad naar de map van SSL-certificaat" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.2.1 Een knooppunt verwijderen in Unix met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u een knooppunt verwijdert.

U kunt `removenode.sh` gebruiken om een knooppunt van een Unix-computer te verwijderen. Voor meer informatie raadpleegt u de sectie "Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten".

Voorbeeld

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten [pagina 485]

11.13.5 De naam van een knooppunt wijzigen

U kunt de naam van een knooppunt wijzigen met de CCM (Central Configuration Manager). Als u de naam van een knooppunt wilt wijzigen, maakt u een nieuw knooppunt met de nieuwe naam, kopieert u de servers van het oorspronkelijke knooppunt naar het nieuwe knooppunt en verwijdert u vervolgens het oorspronkelijke knooppunt. Volg hierbij de volgende richtlijnen:

- Als u de naam wijzigt van de computer waarop het knooppunt zich bevindt, hoeft u de naam van het knooppunt niet te wijzigen. U kunt de bestaande naam van het knooppunt blijven gebruiken.
- Als u een firewall gebruikt, moet u ervoor zorgen dat de poorten van uw SIA (Server Intelligence Agent) en CMS (Central Management Server) open zijn.

> → Onthouden
>
> U kunt de naam van een knooppunt alleen wijzigen op de computer waarop het knooppunt zich bevindt.

Verwante informatie

Een nieuw knooppunt toevoegen [pagina 468]
Een knooppunt verwijderen [pagina 476]

11.13.5.1 De naam van een knooppunt wijzigen in Windows

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u de naam van een knooppunt wijzigt.

1. Start de CCM (Central Configuration Manager).
2. Klik op *Knooppunt toevoegen* op de werkbalk in de CCM (Central Configuration Manager).
3. Voer in de *wizard Knooppunt toevoegen* de knooppuntnaam en poortnummer in voor de nieuwe SIA (Server Intelligence Agent), de beheerdersreferenties, de databaseverbindingsgegevens, de referenties voor de systeemdatabase en de clustersleutel.
4. Selecteer *Knooppunt toevoegen zonder servers*
5. Nadat het knooppunt is gemaakt, gebruikt u de pagina *Serverbeheer* van de CMC (Central Management Console) om alle servers van het oorspronkelijke knooppunt naar het nieuwe knooppunt te kopiëren.

   > ⓘ Opmerking
   >
   > Zorg ervoor dat de gekloonde servers geen poortconflicten hebben met de servers op het oude knooppunt.

6. Start het nieuwe knooppunt in de CCM.
7. Gebruik de CCM om het oorspronkelijke knooppunt te verwijderen als het nieuwe knooppunt vijf minuten actief is.

Verwante informatie

Een nieuw knooppunt toevoegen [pagina 468]
Een knooppunt verwijderen [pagina 476]

11.13.5.2 De naam van een knooppunt in Unix wijzigen

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u de naam van een knooppunt wijzigt.

1. Voer `<INSTALLATIEMAP>/sap_bobj/serverconfig.sh` uit.
2. Selecteer *1 - Add node* en druk op `Enter`.
3. Typ de naam van het nieuwe knooppunt en druk op `Enter`.
4. Typ het poortnummer van de nieuwe SIA in en druk op `Enter`.
5. Als u hierom wordt gevraagd, voert u de beheerdersreferenties, de databaseverbindingsgegevens, de referenties voor de systeemdatabase en de clustersleutel in.
6. Selecteer *geen servers* en druk op `Enter.`
7. Nadat het knooppunt is gemaakt, gebruikt u de pagina *Serverbeheer* van de CMC (Central Management Console) om alle servers van het oorspronkelijke knooppunt naar het nieuwe knooppunt te kopiëren.

   > **Opmerking**
   >
   > Zorg ervoor dat de gekloonde servers geen poortconflicten hebben met de servers op het oude knooppunt.

8. Voer `<INSTALLATIEMAP>/sap_bobj/ccm.sh -start <knooppuntnaam>` uit om het nieuwe knooppunt te starten.
9. Gebruik `serverconfig.sh` om het oorspronkelijke knooppunt te verwijderen als het nieuwe knooppunt vijf minuten actief is.

Verwante informatie

Een nieuw knooppunt toevoegen [pagina 468]
Servers klonen [pagina 425]
Een knooppunt verwijderen [pagina 476]

11.13.6 Een knooppunt verplaatsen

U kunt een gestopt knooppunt verplaatsen van het ene naar het andere cluster met behulp van de CCM (Central Configuration Manager) of met een script voor knooppuntbeheer. Volg hierbij de volgende richtlijnen:

- Zorg dat het doelcluster geen knooppunt bevat met dezelfde naam.
- Zorg dat alle servertypen die op de computer zijn geïnstalleerd waar het bronknooppunt zich bevindt, ook op het doelcluster zijn geïnstalleerd.
- Als u een nieuwe computer wilt toevoegen aan een productiecluster, maar de computer pas wilt gebruiken als u deze getest hebt, installeert u het BI-platform op een aparte computer, test u de computer en verplaatst u het knooppunt vervolgens naar een productiecluster.
- De versie en het servicepackniveau van het BI-platform voor deze computer moeten consistent zijn met de rest van het cluster.

> **→ Onthouden**
>
> U kunt een knooppunt alleen verplaatsen op de computer waarop het knooppunt zich bevindt.

11.13.6.1 Een bestaand knooppunt verplaatsen in Windows

In dit voorbeeld is het knooppunt dat u wilt verplaatsen geïnstalleerd op het bronsysteem. De computer van het bronsysteem was eerst onderdeel van een zelfstandig cluster, maar wordt nu toegevoegd aan het doelcluster.

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u het knooppunt verplaatst.

1. Stop het knooppunt in de CCM (Central Configuration Manager).
2. Klik met de rechtermuisknop op het knooppunt en selecteer *Verplaatsen*.
3. Als hierom wordt gevraagd, selecteert u de naam van de gegevensbron en voert u de hostnaam, de poort, de databaseverbindingsgegevens, de beheerdersreferenties voor de doel-CMS en de clustersleutel in.
4. Selecteer een CMS.
   - Als uw bronimplementatie actief is, selecteert u *Bestaande actieve CMS gebruiken* en klikt u op *Volgende*.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS en beheerdersreferenties van het bronsysteem.
   - Als uw bronimplementatie is gestopt, selecteert u *Een nieuwe tijdelijke CMS starten* en klikt u op *Volgende*.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de tijdelijke CMS van het bronsysteem, de beheerdersreferenties, de naam van de gegevensbron, de referenties voor de bronsysteemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > ⚠ Let op
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is.
5. Controleer de bevestigingspagina en klik op *Voltooien*.
   De CCM maakt een nieuw knooppunt op het doelcluster, met dezelfde naam en dezelfde servers als het knooppunt op het doelcluster. Een kopie van het knooppunt blijft in het broncluster staan. De configuratiesjablonen voor de servers in het knooppunt worden niet verplaatst. Als er een fout optreedt, raadpleeg dan het logbestand.

   > ⚠ Let op
   >
   > Gebruik het broncluster niet nadat het knooppunt verplaatst is.
6. Start het verplaatste knooppunt in de CCM.

11.13.6.1.1 Een knooppunt verplaatsen in Windows met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u het knooppunt verplaatst.

U kunt `MoveNode.bat` gebruiken om een knooppunt op een Windows-computer te verplaatsen. Zie de sectie "Scriptparameters voor het verplaatsen van knooppunten" voor meer informatie.

Voorbeeld

Vanwege de beperkingen van de opdrachtprompt moet u het dakje (^) gebruiken om een escape uit te voeren op spaties, het gelijkteken (=) en de puntkomma (;) in deze parameters, tenzij u de tekst omsluit met aanhalingstekens.

```
<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
```

> ⓘ Opmerking
>
> Als u de caret niet wilt gebruiken in lange tekenreeksen, kunt u de naam van het script en alle bijbehorende parameters naar een tijdelijk `response.bat`-bestand schrijven om vervolgens het `response.bat`-bestand zonder parameters uit te voeren.

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het verplaatsen van knooppunten [pagina 488]

11.13.6.2 Een bestaand knooppunt verplaatsen in Unix

In dit voorbeeld is het knooppunt dat u wilt verplaatsen geïnstalleerd op het bronsysteem. De computer van het bronsysteem was eerst onderdeel van een zelfstandig cluster, maar wordt nu toegevoegd aan het doelcluster.

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u het knooppunt verplaatst.

1. Voer `<INSTALLATIEMAP>/sap_bobj/ccm.sh -stop <knooppuntnaam>` uit om het knooppunt te stoppen.
2. `<INSTALLATIEMAP>/sap_bobj/serverconfig.sh` uitvoeren
3. Selecteer *4 - Knooppunt verplaatsen* en druk op `Enter`.
4. Selecteer het knooppunt dat u wilt verplaatsen en druk op `Enter`.
5. Als hierom wordt gevraagd, selecteert u de verbindingsgegevens voor de systeemdatabase en voert u de hostnaam, de poort, de beheerdersreferenties voor de doel-CMS en de clustersleutel in.
6. Selecteer een CMS.
   - Als uw bronimplementatie actief is, selecteert u *bestaand* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam en het poortnummer in voor de bestaande CMS en beheerdersreferenties van het bronsysteem.
   - Als uw bronimplementatie gestopt is, selecteert u *tijdelijk* en drukt u op `Enter`.
     Als hierom wordt gevraagd, voert u de hostnaam en poort in voor de tijdelijke CMS van het bronsysteem, de beheerdersreferenties, de databaseverbindingsgegevens en de referenties voor de bronsysteemdatabase en de clustersleutel. Een tijdelijke CMS wordt gestart. (Deze stopt wanneer dit proces voltooid wordt.)

     > ⚠ Let op
     >
     > Probeer de implementatie niet te gebruiken als de tijdelijke CMS actief is. Zorg ervoor dat de bestaande en tijdelijke CMS andere poorten gebruiken.
7. Controleer de bevestigingspagina en druk op `Enter`.
   De CCM maakt een nieuw knooppunt op het doelcluster, met dezelfde naam en dezelfde servers als het knooppunt op het doelcluster. Een kopie van het knooppunt blijft in het broncluster staan. De configuratiesjablonen voor de servers in het knooppunt worden niet verplaatst. Als er een fout optreedt, raadpleeg dan het logbestand.

   > ⚠ Let op
   >
   > Gebruik het broncluster niet nadat het knooppunt verplaatst is.
8. Voer `<INSTALLATIEMAP>/sap_bobj/ccm.sh -start <knooppuntnaam>` uit om het verplaatste knooppunt te starten.

11.13.6.2.1 Een knooppunt verplaatsen in Unix met behulp van een script

> ⚠ Let op
>
> Maak een back-up van de serverconfiguratie voor het volledige cluster, voor en nadat u het knooppunt verplaatst.

U kunt `movenode.sh` gebruiken om een knooppunt op een Unix-computer te verplaatsen. Zie de sectie "Scriptparameters voor het verplaatsen van knooppunten" voor meer informatie.

Voorbeeld

```
<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
```

Verwante informatie

Variabelen [pagina 466]
Scriptparameters voor het verplaatsen van knooppunten [pagina 488]

11.13.7 Scriptparameters

11.13.7.1 Scriptparameters voor het toevoegen, opnieuw maken en verwijderen van knooppunten

Parameter	Beschrijving	Voorbeeld
`-adopt`	Hiermee wordt het knooppunt opnieuw gemaakt als het al bestaat in de CMS.	`-adopt`

Parameter	Beschrijving	Voorbeeld
`-cms`	De naam en het poortnummer van de CMS (Central Management Server). **⚠ Let op** Gebruik deze parameter niet als u `-usetempcms` gebruikt **ⓘ Opmerking** U moet een poortnummer opgeven als de CMS niet wordt uitgevoerd op de standaardpoort (6400).	`-cms mycms:6409`
`-cmsport`	• Het poortnummer van de CMS wanneer een tijdelijke CMS wordt gestart. **⚠ Beperking** U moet ook de parameters `-usetempcms`, `-dbdriver`, `-connect` en `-dbkey` gebruiken. • Het poortnummer van de CMS wanneer een nieuwe CMS wordt gemaakt. **⚠ Beperking** U moet ook de parameters `-dbdriver`, `-connect` en `-dbkey` gebruiken.	`-cmsport 6401`
`-connect`	De verbindingsreeks van de systeemdatabase van de (tijdelijke) CMS. **ⓘ Opmerking** Laat de attributen `HOSTNAME` en `PORT` weg wanneer u verbinding maakt met DB2-, Oracle-, SQL Anywhere-, SQL Server- of Sybase-databases.	`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`

Parameter	Beschrijving	Voorbeeld
`-dbdriver`	Het databasestuurprogramma van de CMS. Geaccepteerde waarden: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	De clustersleutel.	**`-dbkey abc1234`**
`-name`	De naam van een knooppunt.	**`-name mynode2`**
`-noservers`	Hiermee maakt u een knooppunt zonder servers. **Opmerking** Met de extra parameter `-createcms` maakt u een knooppunt met een CMS, maar zonder andere servers. Laat deze parameters weg om een knooppunt met alle standaard-servers te maken.	**`-noservers`**
`-password`	Het wachtwoord van de beheerdersaccount.	**`-password Password1`**
`-siaport`	Het poortnummer van de Server Intelligence Agent voor het knooppunt.	**`-siaport 6409`**
`-username`	De gebruikersnaam van de beheerdersaccount.	**`-username Administrator`**
`-usetempcms`	**Let op** Gebruik deze parameter niet als u `-cms` gebruikt Hiermee start en gebruikt u de tijdelijke CMS. **Opmerking** Gebruik een tijdelijke CMS wanneer uw implementatie niet actief is.	**`-usetempcms`**

Verwante informatie

Een knooppunt toevoegen in Windows met behulp van een script [pagina 470]
Een knooppunt toevoegen in Unix met behulp van een script [pagina 472]
Een knooppunt opnieuw maken in Windows met behulp van een script [pagina 474]

Een knooppunt opnieuw maken in Unix met behulp van een script [pagina 476]
Een knooppunt verwijderen in Windows met behulp van een script [pagina 477]
Een knooppunt verwijderen in Unix met behulp van een script [pagina 479]

11.13.7.2 Scriptparameters voor het verplaatsen van knooppunten

Parameter	Beschrijving	Voorbeeld
`-cms`	De naam van de bron-CMS (Central Management Server). **⚠ Let op** Gebruik deze parameter niet als u `-usetempcms` gebruikt **ⓘ Opmerking** U moet een poortnummer opgeven als de CMS niet wordt uitgevoerd op de standaardpoort (6400).	`-cms sourceMachine:6409`
`-cmsport`	• Het poortnummer van de CMS wanneer een tijdelijke CMS wordt gestart. **⚠ Beperking** U moet ook de parameters `-usetempcms`, `-dbdriver`, `-connect` en `-dbkey` gebruiken. • Het poortnummer van de CMS wanneer een nieuwe CMS wordt gemaakt. **⚠ Beperking** U moet ook de parameters `-dbdriver`, `-connect` en `-dbkey` gebruiken.	`-cmsport 6401`
`-connect`	De verbindingsreeks van de systeemdatabase van de (tijdelijke) CMS. **ⓘ Opmerking** Laat de attributen HOSTNAME en PORT weg wanneer u verbinding maakt met DB2-, Oracle-, SQL Anywhere-, SQL Server- of Sybase-databases.	`-connect "DSN=Source BOEXI40;UID=gebruikersnaam;PWD=wachtwoord;HOSTNAME=database;PORT=3306"`

Parameter	Beschrijving	Voorbeeld
`-dbdriver`	Het databasestuurprogramma van de bron-CMS. Geaccepteerde waarden: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-dbdriver mysqldatabasesubsystem`**
`-dbkey`	De clustersleutel van de bron.	**`-dbkey abc1234`**
`-destcms`	De naam van de doel-CMS. **Opmerking** U moet een poortnummer opgeven als de CMS niet wordt uitgevoerd op de standaardpoort (6400).	**`-destcms destinationMachine:6401`**
`-destconnect`	De verbindingsreeks van de systeemdatabase van de doel-CMS. **Opmerking** Laat de attributen `HOSTNAME` en `PORT` weg wanneer u verbinding maakt met DB2-, Oracle-, SQL Anywhere-, SQL Server- of Sybase-databases.	**`-destconnect "DSN=Destin BOEXI40;UID=gebruikersnaam;PWD=w achtwoord;HOSTNAME=database;PORT =3306"`**
`-destdbdriver`	Het databasestuurprogramma van de doel-CMS. Geaccepteerde waarden: • **`db2databasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`newdbdatabasesubsystem`**	**`-destdbdriver sybasedatabasesubsystem`**
`-destdbkey`	De clustersleutel van het doel.	**`-destdbkey def5678`**
`-destpassword`	Het wachtwoord van de beheerdsaccount op de doel-CMS.	**`-destpassword Password2`**
`-destusername`	De gebruikersnaam van de beheerdersaccount op de doel-CMS.	**`-destusername Administrator`**

Parameter	Beschrijving	Voorbeeld
`-password`	Het wachtwoord van de beheerdsaccount op de bron-CMS.	`-password Password1`
`-username`	De gebruikersnaam van de beheerdersaccount op de bron-CMS.	`-username Administrator`
`-usetempcms`	⚠ Let op Gebruik deze parameter niet als u `-cms` gebruikt Hiermee start en gebruikt u de tijdelijke CMS. ⓘ Opmerking Gebruik een tijdelijke CMS wanneer uw implementatie niet actief is.	`-usetempcms`

Verwante informatie

Een knooppunt verplaatsen in Windows met behulp van een script [pagina 483]
Een knooppunt verplaatsen in Unix met behulp van een script [pagina 485]

11.13.8 Windows-serverafhankelijkheden toevoegen

In een Windows-omgeving is elk exemplaar van SIA (Server Intelligence Agent) afhankelijk van het gebeurtenislogboek en RPC-services (Remote Procedure Call).

Als de SIA niet juist werkt, zorg er dan voor dat beide services worden weergegeven op het tabblad *Afhankelijkheid* van de SIA.

11.13.8.1 Windows-serverafhankelijkheden toevoegen

1. De CCM (Central Configuration Manager) gebruiken om de SIA (Server Intelligence Agent) te stoppen.
2. Klik met de rechtermuisknop op de SIA en selecteer *Eigenschappen*.
3. Klik op het tabblad *Afhankelijkheid*.
4. Klik op *Toevoegen*.
   Het dialoogvenster *Afhankelijkheid toevoegen* verschijnt en toont een lijst met alle beschikbare afhankelijkheden.
5. Selecteer een afhankelijkheid en klik op *Toevoegen*.
6. Klik op *OK*.

7. Gebruik de CCM om de SIA opnieuw te starten.

11.13.9 De gebruikersreferenties voor een knooppunt wijzigen

U kunt de CCM (Central Configuration Manager) gebruiken op de gebruikersreferenties voor de SIA (Server Intelligence Agent) op te geven of bij te werken als het wachtwoord van het besturingssysteem wordt gewijzigd, of als u alle servers op een knooppunt wilt uitvoeren onder een andere gebruikersaccount.

Alle servers beheerd door de SIA worden onder dezelfde account uitgevoerd. Als u een server wilt uitvoeren met een niet-systeemaccount, moet u ervoor zorgen dat de account lid is van de groep Lokale beheerder op de servercomputer en dat deze het volgende recht heeft: "Token op procesniveau vervangen".

> **⚠ Beperking**
>
> Op een Unix-computer moet u het BI-platform uitvoeren met de account die gebruikt is om het platform te installeren. Als u een andere account wilt gebruiken, moet u de implementatie opnieuw installeren met een andere account.

11.13.9.1 De gebruikersreferenties voor een knooppunt wijzigen in Windows.

1. De CCM (Central Configuration Manager) gebruiken om de SIA (Server Intelligence Agent) te stoppen.
2. Klik met de rechtermuisknop op de SIA en selecteer *Eigenschappen*.
3. Schakel het selectievakje *Systeemaccount* uit.
4. Voer een gebruikersnaam en wachtwoord in en klik op *OK*.
5. Gebruik de CCM om de SIA opnieuw te starten.

De SIA en de serverprocessen melden zich met de nieuwe gebruikersaccount aan bij de lokale computer.

11.14 Namen van computers in BI-platformimplementaties wijzigen

11.14.1 Clusternamen wijzigen

Als u clusternamen wilt wijzigen, moet u als volgt te werk gaan:

> **⚠ Let op**
>
> Implementeer nooit meerdere clusters met dezelfde naam.

Voorwaarde	Actie
De naam van het cluster wordt gewijzigd.	Stel de gebruikers op de hoogte van de nieuwe clusternaam en vraag hen deze te gebruiken (nadat voor het eerst verbinding is gemaakt met de CMS met syntaxis `<hostnaam>:<poort>`). Wijzig op de weblaag de clusternaam in de eigenschappenbestanden van alle webtoepassingsservers.
U installeert een andere versie van het BI-platform op een computer waarop voorheen een CMS werd uitgevoerd of voegt de computer toe aan een ander cluster.	• Zorg ervoor dat de nieuwe CMS op een andere poort wordt uitgevoerd. • Gebruik per cluster een uniek wachtwoord om te voorkomen dat gebruikers zich aanmelden bij het verkeerde cluster.

11.14.2 IP-adressen wijzigen

Om wijzigingen in de configuratie te voorkomen als gevolg van wijzigingen in het IP-adres van de computer, selecteert u *Servereigenschappen* op het tabblad *Servers* van de CMC en zorgt u er vervolgens voor dat alle servers verbinding maken met hostnamen of kiest u de optie *Automatisch toewijzen*. Ga verder als volgt te werk:

Voorwaarde	Actie
U gebruikt ODBC voor de CMS-database of de controledatabase.	Zorg ervoor dat de DSN de hostnaam van de CMS-databaseserver gebruikt.
U gebruikt een ander databaseverbindingstype voor de CMS-database of de controledatabase.	Gebruik de CCM om de hostnaam van de database in te stellen voor de database.
De CMS-database of de controledatabase bevindt zich op dezelfde host als de CMS.	Gebruik `localhost` als computernaam.
U gebruikt de URL voor webtoepassingen van BI-platform die gebruikers met webbrowsers benaderen (bijvoorbeeld de CMC).	Gebruik in standaard-URL's hostnamen in plaats van IP-adressen. Als u de URL voor de standaardviewer wilt bijwerken, selecteert u *Verwerkingsinstellingen* voor de geselecteerde toepassing. Voor OpenDocument bijvoorbeeld klikt u op het tabblad *Toepassingen* in de CMC, klikt u met de rechtermuisknop op *Open Document* en seletceert u *Verwerkingsinstellingen*.
U gebruikt de URL voor BI-platformclients die zijn gebaseerd op webservices (bijvoorbeeld Crystal Reports voor Java of LiveOffice).	
U gebruikt OpenDocument.	

Alternatieve richtlijnen

> **Opmerking**
>
> Volg deze richtlijnen alleen als u de bovenstaande aanbevelingen niet kunt volgen.

Voor computers waarop servers worden gehost

Voorwaarde	Actie
De host bevat BI-platformservers en de servers zijn gebonden aan specifieke IP-adressen.	Wijzig de IP-adressen op het tabblad *Servers* van de CMC, maar start de servers niet opnieuw tot alles op de computer is bijgewerkt. Start vervolgens de computer opnieuw op, niet de afzonderlijke BI-platformservers.
Voor een databaseverbinding is een IP-adres vereist.	Wijzig het IP-adres.
Voor een statisch IP-netwerk is het vereist om het IP-adres te wijzigen.	Wijzig het IP-adres van de computer waarop BI-platform wordt uitgevoerd. → Tip Meld u aan bij de CMC en controleer of het BI-platform naar behoren werkt.

→ Onthouden

Start de computer opnieuw op nadat u een actie hebt uitgevoerd.

Voor computers waarop de webtoepassingsserver wordt gehost

Voorwaarde	Actie
De URL van de standaardviewer voor OpenDocument moet een IP-adres bevatten	Wijzig het IP-adres in het veld *Standaardviewer-URL instellen* van de sectie *Verwerkingsinstellingen* van het tabblad *Toepassingen* van de CMC.
Gebruikers benaderen webtoepassingen van het BI-platform (bijvoorbeeld de CMC) door een URL met een IP-adres in hun browsers op te geven.	Geef het nieuwe IP-adres door aan de gebruikers.
IP-adressen zijn vereist voor BI-platformclients die zijn gebaseerd op webservices (bijvoorbeeld Crystal Reports voor Java of LiveOffice).	Stel de nieuwe IP-adressen in voor alle clients.

Verwante informatie

Een nieuwe of bestaande CMS-database selecteren [pagina 501]

11.14.3 Computernamen wijzigen

U kunt computers in een implementatie van het BI-platform te allen tijde een andere naam geven door alle BI-platformservers op de computer te stoppen en vervolgens de computer een andere naam te geven. Als u computernamen wilt wijzigen, moet u als volgt te werk gaan:

Voorwaarde	Actie
U meldt zich voor het eerst aan.	Gebruik de CMS-computernaam (niet de clusternaam).
U hebt een implementatie met meerdere computers.	Zorg dat alle CMS-servers op alle andere computers actief zijn tijdens het wijzigen van de naam.

11.14.3.1 Serverlaag

> **Opmerking**
>
> Voordat u de naam van de CMS-computer wijzigt, moet u de configuratie van alle servers op de desbetreffende computer controleren op het tabblad "Serverbeheer" van de CMC. Als in de eigenschap *Hostnaam* de oude CMS-hostnaam wordt gebruikt, moet u deze wijzigen in de nieuwe hostnaam.

> **→ Onthouden**
>
> Start de servers pas opnieuw op als u alle procedures voor het wijzigen van de computernaam hebt voltooid.

Volg de onderstaande instructies voor het wijzigen van computernamen op de serverlaag:

Voorwaarde	Actie
Op de computer waarvan de naam is gewijzigd wordt een CMS gehost en gebruikers hebben zich eerder aangemeld door de oude naam op te geven.	Geef de nieuwe CMS-computernaam door aan de gebruikers en vraag en deze naam te gebruiken.
Op de computer waarvan de naam is gewijzigd wordt een CMS gehost en de bestanden met de standaardeigenschappen voor de webtoepassingen van BI-platform bevatten de oude CMS-hostnaam (in de eigenschap `cms.default`).	Wijzig de CMS-computernaam in de eigenschap `cms.default` in alle aangepaste eigenschappenbestanden op alle computers op de weblaag. Op Tomcat staan de eigenschappenbestanden die u maakt standaard in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`. **Opmerking** Als er geen aangepaste eigenschappenbestanden zijn, moet u deze maken. Kopieer hiertoe de standaardeigenschappenbestanden naar een aangepaste map en verwijder alle inhoud uit de bestanden behalve de regel `cms.default`.
U gebruikt Portal Integration Kits of aangepaste toepassingen.	Geef de nieuwe CMS-hostnaam op in de instellingen voor de Portal Integration Kits of aangepaste toepassingen.

Voorwaarde	Actie
De implementatie voldoet aan alle onderstaande voorwaarden: • Een cluster heeft meerdere knooppunten. • Alle CMS-servers worden alleen uitgevoerd op de computer waarvan de naam is gewijzigd. • Op ten minste één knooppunt wordt de CMS niet gehost. • U wijzigt de naam van een computer met ten minste één knooppunt. • Tijdens het wijzigen van de naam verandert ook het IP-adres.	Gebruik de CCM om de werkstroom "Knooppunt opnieuw maken" uit te voeren voor alle knooppunten behalve het knooppunt waarop de CMS wordt gehost en start vervolgens alle BI-platformknooppunten in de implementatie. Raadpleeg het hoofdstuk "Knooppunten beheren" voor meer informatie.

→ Onthouden

Start de webtoepassing of toepassingsserver opnieuw op nadat u de actie hebt uitgevoerd.

Verwante informatie

Een knooppunt opnieuw maken [pagina 472]

11.14.3.2 Weblaag

Volg de onderstaande instructies als u de naam van de computer wilt wijzigen waarop de webtoepassingsserver van het BI-platform wordt gehost:

Voorwaarde	Actie
U wijzigt de naam van de computer waarop de webtoepassingsserver van het BI-platform wordt gehost en de URL van de standaardviewer voor OpenDocument bevat de hostnaam van een webtoepassingsserver.	Meld u aan bij de CMC en wijzig de standaardviewer-URL in *Toepassingen* > *CMC* > *Verwerkingsinstellingen*.
U wijzigt de naam van de computer waarop de webtoepassingsserver van het BI-platform wordt gehost en de gebruikers benaderen webtoepassingen van het BI-platform met behulp van een URL die een hostnaam van een webtoepassingsserver bevat.	Vraag de gebruikers de webtoepassingen van het BI-platform te benaderen via een URL die de nieuwe hostnaam voor de webtoepassingsserver bevat.
U wijzigt de naam van de computer waarop de webtoepassingsserver van het BI-platform wordt gehost en de URL's van BI-platformclients op basis van webservices bevatten hostnamen van webtoepassingsservers.	Configureer alle BI-platformclients die op webservices zijn gebaseerd, opnieuw om de nieuwe hostnaam van de webtoepassingsserver te gebruiken.

11.14.3.3 Databases

Als u de computer waarop de CMS-systeemdatabase of de controledatabase wordt gehost een andere naam wilt geven, gaat u als volgt te werk:

Voorwaarde	Actie
U wilt wijzigingen in het IP-adres vermijden.	Gebruik de computernaam van de CMS-database of de controledatabase in de DSN (Naam gegevensbron).
De CMS-database of controledatabase bevindt zich op dezelfde host als de CMS.	Gebruik `localhost` in de DSN om te voorkomen dat u deze moet wijzigen als de hostnaam wordt gewijzigd.

CMS-systeemdatabase

Voorwaarde	Actie
U wijzigt de naam van de computer waarop de CMS-systeemdatabase wordt gehost en u gebruikt ODBC.	Geef de nieuwe hostnaam van de databaseserver op in de DSN van de CMS-database.
U wijzigt de naam van een computer waarop de CMS-systeemdatabase wordt gehost en u gebruikt een niet-ODBC-verbindingstype.	Gebruik de CCM om de nieuwe hostnaam van de databaseserver in de CMS-database te definiëren voor elk knooppunt in het cluster.

Controledatabase

Voorwaarde	Actie
U wijzigt de naam van de computer waarop de controledatabase wordt gehost en u gebruikt ODBC.	Geef de nieuwe hostnaam van de databaseserver op in de DSN van de controledatabase.
U wijzigt de naam van een computer waarop de controledatabase wordt gehost en u gebruikt een niet-ODBC-verbindingstype.	Geef de nieuwe hostnaam van de databaseserver op op het tabblad *Controle* van de CMC.

11.14.3.4 File Repository Servers

Als u de naam van de computer wilt wijzigen waarop de FRS-bestandsopslag wordt gehost, moet u de *Input File Repository*- en *Output File Repository*-servers op de pagina "Serverbeheer" van de CMC bijwerken en moet u in de eigenschappen voor de *Map voor bestandsopslag* en de *Tijdelijke map* het nieuwe pad naar de bestandsopslag opgeven. Vervolgens start u de servers opnieuw op.

11.15 32-bits en 64-bits bibliotheken van derden gebruiken in BI-platform

BI-platformservers zijn een combinatie van 32- en 64-bits processen. Een aantal servers start tevens 32-bits en 64-bits onderliggende processen. Om de juiste versie van bibliotheken van derden (32-bits of 64-bits) in BI-platformprocessen te gebruiken, moet u afzonderlijke omgevingsvariabelen instellen voor elke versie op de computer waarop het BI-platform wordt gehost. Vervolgens moet u een extra omgevingsvariabele instellen met een door komma's gescheiden lijst van alle omgevingsvariabelen die gelden voor 32-bits en 64-bits versies. Wanneer een proces wordt gestart door het BI-platform, zal de juiste variabele worden geselecteerd, afhankelijk van of het proces 32-bits of 64-bits is.

- `<FIRST_ENV_VAR>`=De waarde die moet worden gebruikt door 64-bits BI-platformprocessen.
- `<FIRST_ENV_VAR32>`=De waarde die moet worden gebruikt voor 32-bits processen.
- `<SECOND_ENV_VAR>`=De waarde die moet worden gebruikt voor 64-bits processen.
- `<SECOND_ENV_VAR32>`=De waarde die moet worden gebruikt voor 32-bits processen.
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

Als u bijvoorbeeld het BI-platform hebt geïnstalleerd op zowel een AIX-computer als op 32-bits en 64-bits Oracle-clients en u moet de variabele LIBPATH instellen, moet u de volgende variabelen instellen:

- ORACLE_HOME=`<hoofdmap van de 64-bits versie van de Oracleclient>`
- ORACLE_HOME32=`<hoofdmap van de 32-bits versie>`
- LIBPATH=`<bibliotheekpad van de 64-bits versie>`
- LIBPATH32=`<bibliotheekpad van de 32-bits versie>`
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Opmerking**
>
> Gebruik BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH niet om de 32-bits en 64-bits paden in Linux en Solaris te scheiden. Voeg 32-bits en 64-bits paden in plaats daarvan toe aan LD_LIBRARY_PATH.

11.16 Tijdelijke aanduidingen voor servers en knooppunten beheren

11.16.1 Tijdelijke plaatsaanduidingen van servers weergeven

Klik in het beheergebied *Servers* van de CMC met de rechtermuisknop op een server en selecteer *Tijdelijke plaatsaanduidingen*.
In het dialoogvenster *Tijdelijke plaatsaanduidingen* wordt een lijst met tijdelijke plaatsaanduidingen weergegeven voor alle servers in hetzelfde cluster als de geselecteerde server. Als u de waarde voor een tijdelijke plaatsaanduiding wilt wijzigen, past u de tijdelijke plaatsaanduiding voor het knooppunt aan.

Verwante informatie

Tijdelijke plaatsaanduidingen voor server en knooppunt [pagina 1211]

11.16.2 De tijdelijke plaatsaanduidingen voor een knooppunt bekijken en bewerken

1. In het beheergebied *Servers* van de Central Management Console klikt u met de rechtermuisknop op het knooppunt waarvoor u de tijdelijke plaatsaanduidingen wilt wijzigen en selecteert u *Tijdelijke plaatsaanduidingen*.
2. Als u de instellingen voor tijdelijke aanduidingen wilt bewerken, brengt u de gewenste wijzigingen aan en klikt u op *Opslaan* om verder te gaan.

> ⚠ Let op
>
> Tijdelijke aanduidingen die niet voor bewerking zijn bedoeld, mogen op geen enkele manier worden gewijzigd. De systeembeheerder moet ervoor zorgen dat alleen de juiste persoon uit de beheerdersgroep (die bedoeld zijn voor het knooppuntbeheer) over de bewerkingsrechten voor het knooppunt beschikt. Alle andere gebruikers, inclusief andere leden van de beheerdersgroep, moeten worden beperkt tot het weergeven/beheren van de knooppuntobjecten door de juiste beveiligingsrechten toe te passen. Als een van de tijdelijke aanduidingen per ongeluk is beschadigd en CMS niet wordt weergegeven, raadpleegt u deze SAP Note: 3269127.

> ⓘ Opmerking
>
> Zie SAP Knowledge Base Article 3278916 voor informatie over hoe het wijzigen van plaatsaanduidingen kan worden voorkomen om verstoring van het BI-landschap door kwaadwillenden te voorkomen.

Verwante informatie

Tijdelijke plaatsaanduidingen voor server en knooppunt [pagina 1211]

12 CMS-databases (Central Management Server) beheren

12.1 CMS-systeemdatabaseverbindingen beheren

Wanneer de CMS-systeemdatabase niet beschikbaar is, bijvoorbeeld na een hardware- of softwarestoring, of een netwerkprobleem, krijgt de CMS de status "Wachten op bronnen". Als de implementatie van het BI-platform meerdere CMS'en heeft, worden verdere aanvragen van andere servers doorgestuurd naar een CMS in het cluster die een actieve verbinding met de systeemdatabase heeft. Wanneer een CMS de status "Wachten op bronnen" heeft, worden reeds bestaande aanvragen die geen databasetoegang vereisen gewoon verwerkt; aanvragen waarvoor wel toegang tot de CMS-database nodig is, mislukken echter.

Standaard probeert een CMS met de status "Wachten op bronnen" periodiek het aantal verbindingen dat is opgegeven in de eigenschap "Aantal gevraagde systeemdatabaseverbindingen" te herstellen. Zodra ten minste één databaseverbinding tot stand is gebracht, synchroniseert de CMS alle noodzakelijke gegevens, gaat de CMS over naar de status "Actief" en wordt de normale uitvoering hervat.

In bepaalde gevallen wilt u mogelijk voorkomen dat de CMS de verbinding met de database automatisch herstelt. Het kan bijvoorbeeld zijn dat u de integriteit van de database wilt controleren voordat databaseverbindingen worden hersteld. Schakel in dat geval op de pagina *Eigenschappen* van de CMS-server het selectievakje *Automatisch opnieuw verbinding maken met systeemdatabase* uit.

Verwante informatie

De eigenschappen van een server wijzigen [pagina 454]

12.1.1 SQL Anywhere selecteren als CMS-database

Als u SQL Anywhere als CMS-database wilt gebruiken, volgt u de onderstaande stappen:

1. Stop alle knooppunten in het systeem.
2. Voer de toepasselijke toepassing uit:
   - Voer onder UNIX het volgende uit: `/cmsdbsetup.sh.`
   - Start in Windows de CCM (Central Configuration Manager).
3. Kopieer uw gegevens uit de CMS-standaarddatabase en kies SQL Anywhere als de doeldatabase. Raadpleeg voor meer informatie de verwante koppeling "Gegevens kopiëren tussen CMS-systeemdatabases".
4. Bij implementaties met meerdere knooppunten moet u de CMS-gegevensbron op elk knooppunt (behalve het knooppunt waarop u de database kopieert) bijwerken naar de nieuwe SQL Anywhere-database.

Raadpleeg voor meer informatie de verwante koppeling “Een nieuwe of bestaande CMS-database selecteren”.

5. Zorg ervoor dat de implementatie naar behoren werkt (u kunt bijvoorbeeld aanmelden bij de CMC en een rapport weergeven).

Verwante informatie

Gegevens kopiëren tussen CMS-systeemdatabases [pagina 506]
Een nieuwe of bestaande CMS-database selecteren [pagina 501]

12.1.2 SAP HANA kiezen als CMS-database

Als u SAP HANA als CMS-database wilt gebruiken, volgt u de onderstaande stappen.

1. Installeer het BI-platform met de standaard CMS-database.
2. Installeer de SAP HANA-client.
3. Stel een verbinding met SAP HANA in.
   - Op Unix controleert u de omgevingsvariabele `ODBCINI`. Als de variabele bestaat en naar een bestaand `odbc.ini`-bestand wijst, voegt u de volgende regels aan dat bestand toe:

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>
     [NewDB]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` is de SAP HANA-versie, bijvoorbeeld “NewDB 1.0”, `<HANA Server IP address>` is het IP-adres van de SAP HANA-server, en `<HANA server port #>` is het poortnummer van de SAP HANA-server.
     Als de `ODBCINI`-omgevingsvariabele niet bestaat, maakt u een `odbc.ini`-bestand in de map `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/`, voegt u bovenstaande regels toe aan het bestand en stelt u de `ODBCINI`-omgevingsvariabele als volgt in:

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

     Zorg dat de ODBCINI-omgevingsvariabele is ingesteld in het gebruikersprofiel dat de BI-servers start.
   - Onder Windows moet u een ODBC-verbinding met SAP HANA instellen.

     > **Opmerking**
     > Voor ODBC-verbindingswijzigingen moet u de 64-bits versie van de ODBC-gegevensbronbeheer uitvoeren: *Start* > *Configuratiescherm* > *Beheerprogramma's* > *Gegevensbronnen (ODBC)*.

4. Zorg ervoor dat het mogelijk is verbinding te maken met de SAP HANA-server.

- Onder Unix kunt u de verbinding met de SAP HANA-server testen door de volgende opdracht uit te voeren. De variabelen in het onderstaande voorbeeld verwijzen naar de SAP HANA-installatie:

```
<INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
<NONADMINUSER> <NONADMINPASSWORD>
```

- Onder Windows kunt u ODBC-gegevensbronbeheer gebruiken om de ODBC-verbinding met SAP HANA te testen.

5. Zorg dat in Unix de `LD_LIBRARY_PATH`- of `LIBPATH`-omgevingsvariabele het pad naar `libodbcHDB.so` bevatten. Zie 2792543, 1886746 en 2721890 voor meer informatie.
6. Installeer het product door de wizard te volgen en selecteer SAP HANA als de CMS-/controledatabase.
7. Zorg ervoor dat de implementatie naar behoren werkt (u kunt bijvoorbeeld aanmelden bij de CMC en een rapport weergeven).

> **Opmerking**
>
> Deze procedure is niet van toepassing als u een database van een bestaande database naar een SAP HANA-database verplaatst. Gebruik in dat geval de procedure voor het kopiëren van een gegevensbron. Zie Gegevens kopiëren tussen CMS-systeemdatabases [pagina 506] voor meer informatie.

Verwante informatie

Gegevens kopiëren tussen CMS-systeemdatabases [pagina 506]
Een nieuwe of bestaande CMS-database selecteren [pagina 501]

12.2 Een nieuwe of bestaande CMS-database selecteren

U kunt de CCM of `cmsdbsetup.sh` gebruiken om een nieuwe of bestaande CMS-systeemdatabase voor een knooppunt op te geven. In het algemeen hoeft u de volgende stappen in slechts enkele gevallen uit te voeren:

- Als u het wachtwoord voor de huidige CMS-systeemdatabase hebt gewijzigd, kunt u met deze stappen de verbinding met de huidige database verbreken en vervolgens een nieuwe verbinding tot stand brengen. Als u daarom wordt gevraagd, kunt u het nieuwe wachtwoord voor de CMS opgeven.
- Als u een lege database voor het BI-platform wilt selecteren en initialiseren, kunt u met deze stappen die nieuwe gegevensbron selecteren.
- Als u een CMS-systeemdatabase hebt hersteld met een back-up (met uw standaardprogramma's en -procedures voor databasebeheer) waardoor de oorspronkelijke databaseverbinding ongeldig is geworden, moet u opnieuw verbinding maken tussen de CMS en de herstelde database. (Dit kan bijvoorbeeld het geval zijn als u de oorspronkelijke CMS-database hebt hersteld naar een onlangs geïnstalleerde databaseserver.)

> **Opmerking**
>
> Als u IBM DB2 als uw CMS-database gebruikt en een upgrade uitvoert van een versie vóór 9.5 Fix Pack 5 naar versie 9.5 Fix Pack 5 of nieuwer (voor de 9.5-reeks), of als u een upgrade uitvoert van een versie vóór

9.7 Fix Pack 1 naar versie 9.7 Fix Pack 1 of nieuwer (voor de 9.7-reeks), wordt het CMS-databaseschema wanneer het BI-platformknooppunt of de CMS de volgende keer opnieuw wordt gestart, automatisch bijgewerkt door de CMS om ondersteuning voor het HADR-compatibele schema te bieden.

Dit kan een langdurig proces zijn, waarbij het BI-platformsysteem niet gebruikt kan worden. Onderbreek het updateproces niet om te voorkomen dat u de CMS-database beschadigt. Het is uiterst raadzaam een back-up van uw CMS-database te maken voordat u deze bewerking uitvoert. Probeer IBM HADR ook niet te gebruiken met een IBM DB2 CMS-database met een oudere versie dan 9.5 Fix Pack 5 (voor de 9.5-reeks) of 9.7 Fix Pack 1 (voor de 9.7-reeks).

ⓘ Opmerking

Configureer niet een installatie van het BI-platform om een CMS-systeemdatabase te gebruiken die tot een ander cluster behoort, tenzij u een werkstroom voor een systeemkopie uitvoert.

Het systeem kan beschadigd raken als de versies en patchniveaus van de BI-platforminstallaties en CMS-databases afwijken, of als installatiepaden afwijken, of als geïnstalleerde onderdelen verschillen, enzovoort.

U voorkomt beschadiging wanneer u BI-inhoud niet van het ene systeem naar het andere migreert door de BI-platformimplementatie te laten wijzen naar een CMS-database van een ander BI-platformsysteem, met name een systeem met een andere versie en patchniveau.

ⓘ Opmerking

Business Intelligence-platform ondersteunt SSL-communicatie tussen de CMS en databases zoals de CMS-database en controledatabase. Voor SSL-communicatie:

- Gebruik SQL Anywhere-, SQL Server- en SAP HANA-database als CMS- of controledatabase om veilig met CMS te communiceren.
- U moet SSL inschakelen in de respectieve databaseservers. Raadpleeg de documentatie voor uw database.
- U moet een ODBC-verbinding maken en het DB-servercertificaat doorgeven via deze ODBC-verbinding.
- U moet dezelfde ODBC-verbinding gebruiken voor het maken van verbinding met de CMS-database en de controledatabase.

12.2.1 Een nieuwe of bestaande CMS-database selecteren onder Windows

1. Gebruik de CCM om de SIA (Server Intelligence Agent) te stoppen.
2. Selecteer de SIA en klik op de knop *CMS-gegevensbron opgeven*.
3. Selecteer *Instellingen van de gegevensbron bijwerken* en klik op *OK*.
4. Selecteer een databasestuurprogramma en klik op *OK*.
5. Deze stappen zijn afhankelijk van het type verbinding dat u hebt geselecteerd:
   - Als u ODBC hebt geselecteerd, wordt het dialoogvenster “Gegevensbron selecteren” van Windows weergegeven. Selecteer de ODBC-gegevensbron die u als de CMS-database wilt gebruiken en klik vervolgens op *OK*. (Klik op *Nieuw* om een nieuwe DSN-naam te configureren.) Als u daarom wordt gevraagd, geeft u uw databasereferenties op en klikt u op *OK*.

- Als u een eigen stuurprogramma hebt geselecteerd, wordt u gevraagd de servernaam, de aanmeldings-id en het wachtwoord voor de database op te geven. Voer deze gegevens in en klik op *OK*.

6. Geef de clustersleutel op.
7. Start de Server Intelligence Agent opnieuw.

12.2.2 Een nieuwe of bestaande CMS-database selecteren in UNIX

Gebruik het script `cmsdbsetup.sh`. Zie het onderwerp "Unix-scripts" in het hoofdstuk Beheer van opdrachtregels in de *Beheerdershandleiding voor BI-platform* voor meer informatie.

1. Voer het script `cmsdbsetup.sh` uit (dit bevindt zich standaard in `<INSTALLATIEMAP>/sap_bobj/`).
2. Selecteer de bijwerkactie (optie 6).
3. Geef het databasetype van de nieuwe CMS-database op wanneer u erom wordt gevraagd.
4. Geef de databasegegevens op (bijvoorbeeld: hostnaam, gebruikersnaam, wachtwoord en clustersleutel). Wanneer de CMS-database naar de nieuwe locatie verwijst, wordt er een bericht weergegeven.
5. Als u wordt gevraagd de SIA (Server Intelligence Agent) opnieuw te maken, geeft u het beheerderswachtwoord op en de poort die u voor de CMS wilt gebruiken.

> ⓘ Opmerking
>
> U wordt alleen om deze gegevens gevraagd wanneer u naar een lege CMS-database verwijst.

Verwante informatie

Unix-scripts [pagina 1094]

12.3 De CMS-systeemdatabase opnieuw maken

In deze procedure wordt uitgelegd hoe u de huidige CMS-systeemdatabase opnieuw maakt (initialiseert). Met deze procedure verwijdert u alle gegevens die al in de database aanwezig zijn. Deze procedure kan bijvoorbeeld handig zijn, als u het BI-platform hebt geïnstalleerd in een ontwikkelomgeving voor het ontwerpen en testen van uw eigen, aangepaste webtoepassingen. Telkens wanneer u alle gegevens uit het systeem wilt verwijderen, kunt u de CMS-systeemdatabase in uw ontwikkelomgeving opnieuw initialiseren.

> ⚠ Let op
>
> Wanneer u de stappen implementeert die in deze werkstroom worden beschreven, verwijdert u alle gegevens uit de CMS-database plus objecten, zoals rapporten en gebruikers. Voer deze stappen niet uit in een productie-implementatie.

Het is belangrijk dat u een back-up maakt van alle serverconfiguratie-instellingen voordat u de CMS-systeemdatabase opnieuw initialiseert. Wanneer u de database opnieuw maakt, worden de instellingen van uw serverconfiguratie verwijderd en moet u dus een back-up hebben om deze gegevens te kunnen herstellen.

Wanneer u de systeemdatabase opnieuw maakt, blijven uw bestaande licentiesleutels behouden in de database. Als u echter licentiesleutels opnieuw moet invoeren, moet u zich met de standaard Administrator-account aanmelden bij de CMS. Ga naar het beheergebied Verificatie en voer uw gegevens in op het tabblad Licentiesleutels.

> **Opmerking**
>
> Als u de CMS-systeemdatabase opnieuw initialiseert, worden alle gegevens in de huidige CMS-systeemdatabase vernietigd. Maak daarom eventueel een back-up van de huidige database voordat u met de procedure begint. Neem zo nodig contact op met uw databasebeheerder.

Verwante informatie

Back-up maken van serverinstellingen [pagina 557]

12.3.1 De CMS-systeemdatabase opnieuw maken onder Windows

1. Gebruik de CCM om de SIA (Server Intelligence Agent) te stoppen.

   > **Opmerking**
   >
   > Voor deze procedure kunt u de CCM niet uitvoeren op een externe computer. De CCM moet worden uitgevoerd op een computer met minimaal één geldig knooppunt. Bovendien moeten de binaire bestanden op deze computer worden geïnstalleerd.

2. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*.
3. Ga in het dialoogvenster *Eigenschappen* naar het tabblad *Configuratie* en klik op *Opgeven*.
4. Klik in het dialoogvenster *Instellingen van CMS-database* op *De huidige gegevensbron opnieuw maken*.

   > **Opmerking**
   >
   > Servers en objecten op de computer waarop u de CCM hebt uitgevoerd in stap 1, worden ook opnieuw gemaakt. Niet alle objecten worden echter opnieuw gemaakt, alleen de standaardsleutelobjecten. Voorbeelrapporten worden bijvoorbeeld niet opnieuw gemaakt.

5. Klik op *OK* en klik op *Ja* als u om een bevestiging wordt gevraagd.
6. Geef het wachtwoord voor de CMS-systeemdatabase op en klik op *OK*.

   > **Opmerking**
   >
   > Zorg dat u een nieuw beheerderswachtwoord instelt. De beheerdersaccount heeft standaard geen wachtwoord.

U ontvangt bericht wanneer de instelling van de CMS-systeemdatabase is voltooid.

7. Klik op *OK*.

   De CCM wordt opnieuw weergegeven.

8. Start de SIA (Server Intelligence Agent) opnieuw en schakel services in.

   Tegelijk met de Server Intelligence Agent wordt ook de CMS gestart. De CMS schrijft vereiste systeemgegevens naar de eerder leeggemaakte gegevensbron geschreven.

9. Als er meerdere computers in de implementatie voorkomen, moet u de knooppunten op de andere computers opnieuw maken.

12.3.2 De CMS-systeemdatabase opnieuw maken in UNIX

Gebruik het script `cmsdbsetup.sh`. Zie het onderwerp "Unix-scripts" in het hoofdstuk Beheer van opdrachtregels in de *Beheerdershandleiding voor BI-platform* voor meer informatie.

1. Voer `cmsdbsetup.sh` uit (bevindt zich standaard in `<INSTALLATIEMAP>/sap_bobj/`).
2. Kies 'opnieuw initialiseren' (optie 5) en bevestig uw keuze.
   Het script `cmsdbsetup.sh` wordt gestart en de CMS-systeemdatabase wordt gemaakt.
3. Geef het wachtwoord voor de CMS-systeemdatabase op.
4. Wanneer de database is gemaakt, sluit u het script `cmsdbsetup.sh` af.
5. Geef de databasegegevens op (bijvoorbeeld: hostnaam, gebruikersnaam en wachtwoord).
   Wanneer de CMS-database naar de nieuwe locatie verwijst, wordt er een bericht weergegeven.
6. Als u wordt gevraagd de SIA (Server Intelligence Agent) opnieuw te maken, geeft u het beheerderswachtwoord op en de poort die u voor de CMS wilt gebruiken.

   > ⓘ Opmerking
   >
   > U wordt alleen om deze gegevens gevraagd wanneer u naar een lege CMS-database verwijst.

7. Gebruik in de map `<INSTALLATIEMAP>/sap_bobj/` de volgende opdracht om het knooppunt te starten.

   ```
   ccm.sh -start <knooppuntnaam>
   ```

8. Gebruik de volgende opdracht om de services te activeren:

   ```
   ccm.sh -enable all -cms <CMSNAME:POORT> -username administrator -password
   <wachtwoord>
   ```

   > ⓘ Opmerking
   >
   > Aangezien u de CMS-database opnieuw hebt gemaakt, is het beheerderswachtwoord leeg.

Verwante informatie

Unix-scripts [pagina 1094]

12.4 Gegevens kopiëren tussen CMS-systeemdatabases

U kunt de CCM (Central Configuration Manager) of `cmsdbsetup.sh` gebruiken om systeemgegevens te kopiëren van de ene databaseserver naar de andere. Als u bijvoorbeeld de database door een andere database wilt vervangen omdat u een upgrade uitvoert voor de database of overstapt van het ene databasetype naar het andere, kunt u de inhoud van de bestaande database naar een nieuwe database kopiëren voordat u de bestaande database uit bedrijf neemt.

De doeldatabase wordt geïnitialiseerd voordat de nieuwe gegevens worden gekopieerd, zodat alle bestaande inhoud van de doeldatabase permanent wordt verwijderd (alle BI-platformtabellen worden definitief verwijderd en vervolgens opnieuw gemaakt). Nadat de gegevens zijn gekopieerd, wordt de doeldatabase de huidige database voor de CMS.

> ⚠ Let op
>
> Probeer geen CMS-database van een ander BI-platformcluster te gebruiken. Voordat u deze workflow start moet u ervoor zorgen dat de CMS-brondatabase werd gebruikt met deze BI-platformcluster en niet met een andere BI-platformcluster.

> ⚠ Let op
>
> Probeer geen update uit te voeren via een kopieworkflow van de CMS-database. De workflow van de CMS-databasekopie is ontworpen om een CMS-database van de ene databaseserver naar een andere databaseserver te verplaatsen. De workflow is niet ontworpen om voor de CMS-database een upgrade uit te voeren. Voordat u met deze workflow start moet u er altijd voor zorgen dat de CMS-brondatabase werd gebruikt met deze BI-platformcluster en dat deze dezelfde versie en patchniveaus heeft als de huidige installatie van het BI-platform.

12.4.1 Kopiëren van CMS-systeemdatabase voorbereiden

Voordat u een CMS-systeemdatabase kopieert, zet u de bron- en doelomgeving offline door alle servers uit te schakelen en vervolgens te stoppen. Maak een back-up van beide CMS-databases en maak een back-up van de hoofdmappen die door alle Input en Output File Repository Servers worden gebruikt. Neem zo nodig contact op met uw database- of netwerkbeheerder.

Zorg ervoor dat u een databasegebruikersaccount hebt waarmee u alle gegevens in de brondatabase kunt lezen en een databasegebruikersaccount waarmee u alle gegevens in de doeldatabase kunt maken, verwijderen of bijwerken. Zorg er bovendien voor dat u via uw databaseclientsoftware of via ODBC verbinding kunt maken met beide databases vanaf de CMS-computer waarop u de database vervangt.

Als u een CMS-database van de huidige locatie naar een andere databaseserver kopieert, is uw huidige CMS-database de bronomgeving. De inhoud van de database wordt naar de doeldatabase gekopieerd, die vervolgens als de actieve database voor de huidige CMS wordt ingesteld. Deze procedure moet u volgen als u de standaard CMS-database van de bestaande standaarddatabase wilt verplaatsen naar een speciale databaseserver, zoals Microsoft SQL Server, Informix, Oracle, DB2 of Sybase. Meld u met een beheerdersaccount aan bij de computer waarop de CMS wordt uitgevoerd waarvan u de database wilt verplaatsen.

> **Opmerking**
>
> Als u gegevens van de ene naar de andere database kopieert, wordt de doeldatabase geïnitialiseerd voordat de nieuwe gegevens worden gekopieerd. Dit houdt in dat als uw doeldatabase geen systeemtabellen van BI-platform bevat, deze tabellen worden gemaakt. Als de doeldatabase wel de systeemtabellen van het BI-platform bevat, worden de tabellen permanent verwijderd, worden nieuwe systeemtabellen gemaakt en worden de gegevens van de brondatabase naar de nieuwe tabellen gekopieerd. Andere tabellen in de database ondervinden hiervan geen invloed.

> **Opmerking**
>
> Als u een CMS-systeemdatabase kopieert naar een MaxDB-doeldatabase in Windows, moet u ervoor zorgen dat het pad naar de MaxDB-client is toegevoegd aan de omgevingsvariabele `<PATH>`. Bijvoorbeeld `;C:\Program Files\sdb\MAXDB1\pgm`.

12.4.2 Een CMS-systeemdatabase kopiëren in Windows

Voordat u de inhoud van de CMS-database kopieert, moet u controleren of u zich kunt aanmelden bij de doeldatabase met een account die bevoegd is voor het toevoegen en neerzetten van tabellen, en voor het toevoegen, verwijderen en bijwerken van gegevens in deze tabellen.

1. Zet de SIA (Server Intelligence Agent) stop vanuit de CCM (Central Configuration Manager).
2. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*.
3. Klik op het tabblad *Configuratie* en klik vervolgens op *Opgeven*.
4. Kies *Kopiëren* en klik op *OK*.
5. Selecteer het databasetype voor de bron-CMS en geef daarna de bijbehorende databasegegevens op (met inbegrip van hostnaam, gebruikersnaam en wachtwoord).
6. Selecteer het databasetype voor de doel-CMS en geef daarna de bijbehorende databasegegevens op (met inbegrip van hostnaam, gebruikersnaam en wachtwoord).
7. Klik op *OK* als de CMS-database is gekopieerd.

12.4.3 Gegevens kopiëren vanuit een CMS-systeemdatabase onder UNIX

Voordat u de inhoud van de CMS-database kopieert, moet u controleren of u zich kunt aanmelden bij de doeldatabase met een account die bevoegd is voor het toevoegen en neerzetten van tabellen, en voor het toevoegen, verwijderen en bijwerken van gegevens in deze tabellen.

> **Opmerking**
>
> Onder UNIX kunt u niet direct migreren van een bronomgeving waarin een ODBC-verbinding naar de CMS-database wordt gebruikt. Als uw CMS-brondatabase gebruikmaakt van ODBC, moet u dat systeem eerst bijwerken naar een ondersteund eigen stuurprogramma.

1. Stop de CMS door de volgende opdracht te typen:

   ```
   ./ccm.sh -stop <knooppuntnaam>
   ```

2. Voer `cmsdbsetup.sh` uit (bevindt zich standaard in `<INSTALLATIEMAP>/sap_bobj/`).
3. Kies de optie “kopiëren” (optie 4) en bevestig uw keuze.
4. Selecteer het databasetype voor de CMS-database die als bron fungeert en geef de bijbehorende database-informatie op (met inbegrip van hostnaam, gebruikersnaam en wachtwoord).
5. Selecteer het databasetype voor de CMS-database die als doel fungeert en geef de bijbehorende database-informatie op (met inbegrip van hostnaam, gebruikersnaam en wachtwoord).
   De CMS-database wordt naar de doeldatabase gekopieerd. Zodra het kopiëren is voltooid, krijgt u daarvan melding.

12.5 Databasestuurprogramma Central Management Server

U kunt nu toegang krijgen tot CMS-gegevensopslagdatabase van BI-platform voor rapportageanalyse met gebruik van bestaande platformfuncties (verbindingsserver, semantische laag, rapportageclients). Met SAP BusinessObjects Data Access Driver kunt u een universe gebruiken om query's uit te voeren op de CMS-database. Zie http://scn.sap.com/docs/DOC-74580 voor meer informatie.

13 Containerservers voor webtoepassingen (WACS) beheren

13.1 WACS

13.1.1 Containerserver voor webtoepassingen (WACS)

Containerservers voor webtoepassingen bieden een platform voor hosting van webtoepassingen van SAP BusinessObjects Business Intelligence-platform. U kunt bijvoorbeeld een CMC (Central Management Console) hosten op een WACS.

Met WACS wordt systeembeheer eenvoudiger omdat diverse procedures die eerst vereist waren voor de configuratie van toepassingsservers en de implementatie van webtoepassingen niet meer nodig zijn. Bovendien is er een vereenvoudigde, consistente, administratieve interface beschikbaar.

Webtoepassingen worden automatisch geïmplementeerd op WACS. Containerservers voor webtoepassingen bieden geen ondersteuning voor handmatige of WDeploy-implementatie van het BI-platform of externe webtoepassingen.

13.1.1.1 Heb ik de WACS nodig?

Als u geen Java-toepassingsserver wilt gebruiken om uw SAP BusinessObjects-webtoepassingen te hosten, kunt u ze op WACS hosten.

Als u een ondersteunde Java-toepassingsserver wilt gebruiken voor de implementatie van webtoepassingen van het BI-platform of als u het BI-platform installeert op een UNIX-systeem, hoeft u WACS niet te installeren en te gebruiken.

13.1.1.2 Wat zijn de voordelen van werken met een WACS?

Het gebruik van een WACS voor het hosten van de CMC biedt een aantal voordelen:

- U kunt de WACS zeer eenvoudig installeren, onderhouden en configureren.
- Alle gehoste toepassingen worden vooraf op de WACS geïmplementeerd, zodat er geen extra handmatige stappen nodig zijn.
- WACS wordt ondersteund door SAP.
- Met de WACS zijn serverbeheer en onderhoudstaken voor Java-toepassingen niet nodig.
- De Containerserver voor webtoepassingen bevat een beheerinterface die consistent is met andere BI-platformservers.

13.1.1.3 Algemene taken

Taak	Beschrijving	Onderwerp
Hoe verbeter ik de prestaties van webtoepassingen of webservices die op WACS worden gehost?	U kunt de prestaties van de webtoepassingen of webservices verbeteren door WACS op meerdere computers te installeren.	• Extra containerserver voor webtoepassingen aan uw implementatie toevoegen of daaruit verwijderen [pagina 512] • Een containerserver voor webtoepassingen klonen [pagina 514]
Hoe verbeter ik de beschikbaarheid van mijn weblaag?	U kunt extra containerservers voor webtoepassingen maken in uw implementatie. In het geval van een hardware- of softwarefout op een server kan een andere server de afhandeling van aanvragen overnemen.	Extra containerserver voor webtoepassingen aan uw implementatie toevoegen of daaruit verwijderen [pagina 512]
Hoe maak ik een omgeving waarin ik een niet goed geconfigureerde CMC eenvoudig kan herstellen?	Maak een tweede containerserver voor webtoepassingen, stop deze server en gebruik de server voor het maken van een configuratiesjabloon. Wanneer op de eerste containerserver voor webtoepassingen fouten ontstaan, kunt u de tweede containerserver voor webtoepassingen gebruiken totdat de eerste is hersteld of u kunt de configuratiesjabloon toepassen op de eerste server.	Extra containerserver voor webtoepassingen aan uw implementatie toevoegen of daaruit verwijderen [pagina 512]
Ho kan ik de communicatie tussen clients en containerservers voor webtoepassingen beter beveiligen?	Configureer HTTPS op de containerservers voor webtoepassingen.	• HTTPS/SSL configureren [pagina 517] • Containerserver voor webtoepassingen gebruiken met firewalls [pagina 543]
Hoe kan ik de communicatie tussen de containerservers voor webtoepassingen en de andere BI-platformservers in mijn implementatie beter beveiligen?	Configureer SSL-communicatie tussen WACS en andere BI-platformservers in uw implementatie.	• Back-endservers configureren voor SSL [pagina 181] • Containerserver voor webtoepassingen gebruiken met firewalls [pagina 543]
Kan ik containerservers voor webtoepassingen gebruiken met HTTPS en een omgekeerde proxy?	U kunt containerservers voor webtoepassingen gebruiken met HTTPS en een omgekeerde proxy als u twee containerservers voor webtoepassingen maakt en beide servers configureert met HTTPS. De eerste containerserver voor webtoepassingen gebruikt u voor communicatie binnen het interne netwerk, de tweede server voor	Containerserver voor webtoepassingen instellen voor ondersteuning van HTTPS met omgekeerde proxy [pagina 543]

Taak	Beschrijving	Onderwerp
	communicatie met een extern netwerk via een omgekeerde proxy.	
Hoe kan ik een containerserver voor webtoepassingen inpassen in mijn IT-omgeving?	Containerservers voor webtoepassingen kunnen in een IT-omgeving worden geïmplementeerd met bestaande webservers, load balancer voor hardware, omgekeerde proxy's en firewalls.	• Containerservers voor webtoepassingen gebruiken met andere webservers [pagina 541] • Containerservers voor webtoepassingen gebruiken met een load balancer [pagina 542] • Containerservers voor webtoepassingen gebruiken met een omgekeerde proxy [pagina 542] • Containerserver voor webtoepassingen gebruiken met firewalls [pagina 543]
Kan ik containerserver voor webtoepassingen gebruiken in een implementatie met een load balancer?	U kunt een containerserver voor webtoepassingen gebruiken in een implementatie met een load balancer voor hardware. U kunt de containerserver voor webtoepassingen zelf niet als een load balancer gebruiken.	Containerservers voor webtoepassingen gebruiken met een load balancer [pagina 542]
Kan ik de containerserver voor webtoepassingen gebruiken in een implementatie met een omgekeerde proxy?	U kunt een containerserver voor webtoepassingen gebruiken in een implementatie met een omgekeerde proxy. U kunt de containerserver voor webtoepassingen zelf niet als een omgekeerde proxy gebruiken.	Containerservers voor webtoepassingen gebruiken met een omgekeerde proxy [pagina 542]
Hoe kan ik problemen met mijn containerservers voor webtoepassingen oplossen?	Raadpleeg de logboekbestanden en de systeemgegevens voor mogelijke oorzaken van de slechte prestaties van uw containerservers voor webtoepassingen.	• Tracering op WACS configureren [pagina 545] • Servergegevens weergeven [pagina 545]
Ik krijg geen pagina's te zien op een bepaalde poort. Wat is er mis?	Er is een aantal redenen te noemen waarom u geen verbinding kunt maken met uw containerservers voor webtoepassingen. Controleer of: • De HTTP-, HTTP via proxy- en HTTPS-poorten die u hebt opgegeven voor de containerservers voor webtoepassingen misschien door andere toepassingen worden gebruikt. • De containerserver voor webtoepassingen genoeg	• Conflicten met HTTP-poorten oplossen [pagina 546] • Geheugeninstellingen wijzigen [pagina 547] • Het aantal gelijktijdige aanvragen wijzigen [pagina 548] • Standaardwaarden herstellen [pagina 548]

Taak	Beschrijving	Onderwerp
	geheugen toegewezen heeft gekregen. • Het aantal gelijktijdige aanvragen dat is toegestaan op de containerserver voor webtoepassingen voldoende is. • Herstel indien nodig de standaardwaarden voor de containerserver voor webtoepassingen.	
Hoe configureer ik de eigenschappen van webtoepassingen die op WACS worden gehost?	De procedure voor het configureren van de eigenschappen voor webtoepassingen hangt af van de specifieke eigenschap en webtoepassing. Zie de sectie "Eigenschappen van webtoepassing configureren" van dit hoofdstuk voor meer informatie.	Eigenschappen van webtoepassing configureren [pagina 544]
Waar vind ik een lijst met eigenschappen voor de containerserver voor webtoepassingen?	De bijlage "Servereigenschappen" in deze handleiding bevat een overzicht met WACS-eigenschappen.	Eigenschappen van kernservices [pagina 1159]

13.1.2 Extra containerserver voor webtoepassingen aan uw implementatie toevoegen of daaruit verwijderen

Het toevoegen van een extra containerserver voor webtoepassingen aan uw implementatie biedt een aantal voordelen:

- Sneller herstel van verkeerd geconfigureerde server.
- Betere beschikbaarheid van servers.
- Betere taakverdeling.
- Betere algehele prestaties.

U kunt op drie manieren extra containerservers voor webtoepassingen aan uw implementatie toevoegen:

- Een containerserver voor webtoepassingen installeren op een computer.
- Een nieuwe containerserver voor webtoepassingen maken.
- Een containerserver voor webtoepassingen klonen.

> ⓘ Opmerking
>
> U kunt het beste één containerserver voor webtoepassingen tegelijk op dezelfde computer uitvoeren vanwege het hoge bronnengebruik. U kunt wel meerdere containerservers voor webtoepassingen op dezelfde computer installeren en slechts één daarvan uitvoeren, zodat u snel de configuratie kunt herstellen in het geval van een verkeerd geconfigureerde containerserver voor webtoepassingen.

13.1.2.1 Containerservers voor webtoepassingen installeren

Wanneer u de containerservers voor webtoepassingen op verschillende computers installeert, zorgt u voor betere prestaties, betere taakverdeling en betere serverbeschikbaarheid in uw implementatie. Als uw implementatie twee of meer WACS op afzonderlijke computers bevat, wordt de beschikbaarheid van webtoepassingen en -services niet beïnvloed door hardware- of softwarefouten op een bepaalde computer omdat de andere WACS de services kan blijven leveren.

Voor de installatie van een containerserver voor webtoepassingen gebruikt u het installatieprogramma van het BI-platform. U kunt een containerserver voor webtoepassingen op twee manieren installeren:

- Bij een volledige installatie kiest u in het scherm *Java-webtoepassingsserver selecteren* de optie *Containerserver voor webtoepassingen installeren en webtoepassingen automatisch implementeren*. Als u een Java-toepassingsserver selecteert bij een nieuwe installatie, wordt geen containerserver voor webtoepassingen geïnstalleerd.
- Als u een aangepaste/uitgebreide installatie uitvoert, kunt u de WACS installeren door in het scherm *Functies selecteren* de optie *Servers* > *Platformservices* uit te vouwen en *Containerserver voor webtoepassingen* te selecteren.

Wanneer u containerservers voor webtoepassingen installeert, maakt het installatieprogramma automatisch een server met de naam `<KNOOPPUNT>.WebApplicationContainerServer`, waarbij `<KNOOPPUNT>` de naam van uw knooppunt is. BI-platformwebtoepassingen en -services worden dan op die server geïmplementeerd. Voor de installatie of configuratie van de CMC hoeft handmatig niets te worden ingesteld. Het systeem is klaar voor gebruik.

Tijdens de installatie van containerservers voor webtoepassingen wordt u gevraagd een HTTP-poortnummer voor de containerserver voor webtoepassingen op te geven. Geef een poortnummer op dat nog niet wordt gebruikt. Het standaardpoortnummer is 6405. Als u gebruikers wilt toestaan om van buiten een firewall verbinding te maken met de containerservers voor webtoepassingen, moet u controleren of de HTTP-poort van de server in de firewall is geopend.

> **Opmerking**
>
> De webtoepassingen waarvan de WACS de host is, worden automatisch geïmplementeerd wanneer u de WACS installeert of wanneer u updates of hotfixes toepast op de WACS of webtoepassingen waarvan de WACS de host is. De implementatie van de webtoepassingen duurt enkele minuten. De WACS heeft de status “Bezig met initialiseren” totdat de implementatie van de webtoepassing is voltooid. Gebruikers kunnen webtoepassingen waarvan de WACS de host is pas openen als de webtoepassingen volledig zijn geïmplementeerd. Stop de server niet totdat de initiële implementatie is voltooid. U kunt de serverstatus van de WACS weergeven via CCM (Central Configuration Manager).
>
> Deze vertraging treedt alleen op wanneer u de WACS de eerste keer start nadat de WACS is geïnstalleerd of hierop updates zijn toegepast. Deze vertraging treedt niet meer op wanneer u de WACS hierna opnieuw opstart.
>
> Webtoepassingen kunnen niet handmatig worden geïmplementeerd op een WACS-server. U kunt Wdeploy niet gebruiken om webtoepassingen te implementeren op de WACS.

13.1.2.2 Een nieuwe containerserver voor webtoepassingen toevoegen

> **Opmerking**
>
> U kunt het beste één containerserver voor webtoepassingen tegelijk op dezelfde computer uitvoeren vanwege het hoge bronnengebruik. U kunt wel meerdere containerservers voor webtoepassingen op dezelfde computer installeren en slechts één daarvan uitvoeren, zodat u snel de configuratie kunt herstellen in het geval van een verkeerd geconfigureerde containerserver voor webtoepassingen.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik op *Beheren* > *Nieuw* > *Nieuwe Server*.
   Het scherm *Nieuwe server maken* wordt weergegeven.
3. Kies *Kernservices* in de lijst *Servicecategorie*.
4. Selecteer in de lijst *Service selecteren* de services die u door de WACS wilt laten hosten, en klik op *Volgende*.
   - Als u wilt dat de WACS als host fungeert voor webtoepassingen zoals de CMC, BI-startpunt of OpenDocument, selecteert u *BOE-webtoepassingsservice*.
   - Als u wilt dat de WACS als host fungeert voor webservices zoals Live Office of Query als een webservice (QaaWS), selecteert u *Webservices-SDK en QaaWS-service*.
   - Als u wilt dat de WACS als host fungeert voor Business Process BI-webservices, selecteert u *Business Process BI-webservice*.
5. Selecteer in het volgende venster *Nieuwe server maken* een van de extra services die de WACS moet hosten en klik op *Volgende*.
6. Selecteer in het volgende scherm *Server maken* het knooppunt waaraan u de server wilt toevoegen, typ een servernaam en beschrijving voor de server, en klik op *Maken*.

   > **Opmerking**
   >
   > In de lijst *Knooppunt* worden alleen de knooppunten weergeven waarop een containerserver voor webtoepassingen is geïnstalleerd.

7. Dubbelklik in het scherm *Servers* op de gemaakte containerserver voor webtoepassingen.
   Het scherm *Eigenschappen* wordt weergegeven.
8. Als u niet wilt dat de WACS automatisch wordt gestart als het systeem opnieuw wordt opgestart, zorg dan dat in het venster *Algemene instellingen* het selectievakje *Deze server automatisch starten wanneer Server Intelligence Agent wordt gestart* is uitgeschakeld.
9. Klik op *Opslaan en sluiten*.

Er wordt een nieuwe containerserver voor webtoepassingen gemaakt. Op deze server worden de standaardinstellingen en -eigenschappen toegepast.

13.1.2.3 Een containerserver voor webtoepassingen klonen

Behalve een nieuwe containerserver voor webtoepassingen aan uw implementatie toevoegen, kunt u ook een containerserver voor webtoepassingen klonen, ofwel naar dezelfde of naar een andere computer. Wanneer u

een nieuwe containerserver voor webtoepassingen toevoegt, wordt een server met de standaardinstellingen gemaakt. Wanneer u echter een bestaande containerserver voor webtoepassingen kloont, worden de instellingen van de bronserver toegepast op de nieuwe containerserver voor webtoepassingen.

Servers kunnen alleen worden gekloond naar computers waarop reeds een containerserver voor webtoepassingen is geïnstalleerd.

> **Opmerking**
>
> U kunt het beste één containerserver voor webtoepassingen tegelijk op dezelfde computer uitvoeren vanwege het hoge bronnengebruik. U kunt wel meerdere containerservers voor webtoepassingen op dezelfde computer installeren en slechts één daarvan uitvoeren, zodat u snel de configuratie kunt herstellen in het geval van een verkeerd geconfigureerde containerserver voor webtoepassingen.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Selecteer de containerserver voor webtoepassingen die u wilt klonen, klik met de rechtermuisknop en selecteer *Server klonen*.

   In het scherm *Server klonen* wordt een lijst weergegeven met knooppunten in uw implementatie waarnaar u de containerserver voor webtoepassingen kunt klonen. De lijst *Klonen naar knooppunt* bevat alleen de knooppunten waarop reeds een containerserver voor webtoepassingen is geïnstalleerd.
3. Typ in het scherm *Server klonen* een nieuwe servernaam, selecteer het knooppunt waarnaar u de server wilt klonen en klik op *OK*.

Er wordt een nieuwe containerserver voor webtoepassingen gemaakt. De nieuwe server bevat dezelfde services als de server waarvan de kloon is gemaakt. De nieuwe server en de services daarop hebben dezelfde instellingen als de server waarvan de kloon is gemaakt, met uitzondering van de servernaam.

> **Opmerking**
>
> Als u een containerserver voor webtoepassingen naar dezelfde computer hebt gekloond, kunnen poortconflicten ontstaan met de containerserver voor webtoepassingen die voor het klonen is gebruikt. Wijzig in dat geval de poortnummers op de nieuwe, gekloonde containerserver voor webtoepassingen.

Verwante informatie

Conflicten met HTTP-poorten oplossen [pagina 546]

13.1.2.4 Containerservers voor webtoepassingen uit uw implementatie verwijderen

U kunt een containerserver voor webtoepassingen alleen verwijderen als op die server niet de huidige CMC-service wordt uitgevoerd. Als u een containerserver voor webtoepassingen uit uw implementatie wilt verwijderen, moet u zich aanmelden bij een CMC vanaf een andere containerserver voor webtoepassingen of een Java-toepassingsserver. U kunt een containerserver voor webtoepassingen niet verwijderen als daarop de huidige CMC-service wordt uitgevoerd.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Stop de containerserver voor webtoepassingen die u wilt verwijderen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server stoppen*.
3. Klik met de rechtermuisknop op de server en selecteer *Verwijderen*.
4. Klik op *OK* om het verwijderen te bevestigen.

13.1.3 Services op een WACS toevoegen of verwijderen

13.1.3.1 Een webtoepassing of webservice toevoegen aan een WACS

Wilt u extra BI-platformwebtoepassingen of -webservices aan een WACS toevoegen, dan moet u de WACS stoppen. Daarom moet u in de implementatie minimaal één extra CMC hosten op een WACS die een BOE-webtoepassingsservice aanbiedt terwijl u een service op de andere WACS stopt en toevoegt.

Als u een service aan een WACS toevoegt, wordt de service automatisch op de WACS geïmplementeerd wanneer u de server opnieuw start.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de WACS waarop u de service wilt toevoegen en kijk in de eigenschappen van de server of de service daar niet al is geïnstalleerd.
3. Klik op *Annuleren* om terug te gaan naar het scherm *Servers*.
4. Stop de server door met de rechtermuisknop op de server te klikken en *Server stoppen* te selecteren.

   Als u de containerserver voor webtoepassingen stopt waarop op dat moment de CMC-service wordt uitgevoerd, verschijnt een waarschuwingsbericht. Ga alleen verder als u ten minste één extra actieve BOE-webtoepassingsservice op een andere WACS in uw implementatie hebt. Als dit het geval is, klikt u op *OK*, meldt u zich aan bij een andere WACS en start u deze procedure vanaf het begin.
5. Klik met de rechtermuisknop op de server en klik op *Services selecteren*.
   Het scherm *Services selecteren* wordt weergegeven.
6. Selecteer de service die u aan de server wilt toevoegen, voeg de service aan de server toe door op > en op *OK* te klikken.
7. Start de WACS door met de rechtermuisknop op de server te klikken en *Server starten* te selecteren.

De service wordt aan de WACS toegevoegd. Op de service worden de standaardinstellingen en -eigenschappen toegepast.

13.1.3.2 Een webtoepassing of webservice verwijderen uit een WACS

U moet zich bij een CMC op een andere WACS of op een Java-toepassingsserver aanmelden om een webtoepassing of -service pas van een WACS te verwijderen. U kunt de WACS niet stoppen als daarop de huidige CMC wordt uitgevoerd.

U kunt niet de laatste service op een containerserver voor webtoepassingen verwijderen. Wanneer u dus een webservice verwijdert van een containerserver voor webtoepassingen, moet u altijd eerst controleren of er nog minstens een andere service op de server wordt uitgevoerd.

Als u de laatste service wilt verwijderen van een WACS, verwijdert u de WACS zelf.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de WACS waarvan u de service wilt verwijderen en kijk in de eigenschappen van de server of de webservice daar niet al is geïnstalleerd.
3. Klik op *Annuleren* om terug te gaan naar het scherm *Servers*.
4. Stop de WACS door met de rechtermuisknop op de server te klikken en *Server stoppen* te selecteren.

   Als u de containerserver voor webtoepassingen stopt waarop op dat moment de CMC-service wordt uitgevoerd, verschijnt een waarschuwingsbericht. Ga alleen verder als u ten minste één extra actieve BOE-webtoepassingsservice op een andere WACS in uw implementatie hebt. Als dit het geval is, klikt u op *OK*, meldt u zich aan bij een andere WACS en start u deze procedure vanaf het begin.
5. Klik met de rechtermuisknop op de containerserver voor webtoepassingen en klik op *Services selecteren*. Het scherm *Services selecteren* wordt weergegeven.
6. Selecteer de service die u wilt verwijderen, klik op < en klik vervolgens op *OK*.
7. Start de WACS door met de rechtermuisknop op de server te klikken en *Server starten* te selecteren.

De service wordt van de WACS verwijderd.

13.1.4 HTTPS/SSL configureren

U kunt het SSL- (Secure Sockets Layer) en het HTTP-protocol gebruiken voor alle netwerkcommunicatie tussen clients en containerservers voor webtoepassingen in uw implementatie van het BI-platform. Het SSL/HTTPS-protocol zorgt voor de versleuteling van het netwerkverkeer en een betere beveiliging.

Er zijn twee SSL-typen:

- SSL zoals gebruikt tussen BI-platformservers, waaronder WACS en andere BI-platformservers in uw implementatie. Dit is ook bekend als CORBA SSL. Zie de sectie “Communicatie tussen SAP BI-platformonderdelen begrijpen” van het hoofdstuk “Werken met firewalls” van de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over het gebruik van SSL tussen de BI-platformservers in uw implementatie.
- HTTP via SSL, dat wordt gebruikt tussen containerservers voor webtoepassingen en clients (zoals browsers) die met deze containerservers voor webtoepassingen communiceren.

> ⓘ Opmerking
>
> Als u de WACS implementeert in een implementatie met een proxy of reverse proxy en de netwerkcommunicatie in de implementatie wilt beveiligen met SSL, moet u twee WACS-servers maken. Zie *Containerservers voor webtoepassingen gebruiken met een omgekeerde proxy* voor meer informatie.

Voer de volgende stappen uit om HTTPS/SSL op een WACS te configureren:

- Een PKCS12-certificaatarchief of JKS-keystorebestand maken of verkrijgen waarin uw certificaten en privésleutels zijn opgenomen. U kunt Microsoft IIS (Internet Information Service) en MMC (Microsoft Management Console) gebruiken om een PCKS12-bestand te maken, of de opdracht openssl of het hulpprogramma Java-keytool gebruiken om een keystore-bestand te maken.

- Als u wilt dat alleen bepaalde clients verbinding maken met een containerserver voor webtoepassingen, maakt u een certificaatvertrouwenslijst.
- Wanneer u een certificaatarchief hebt en, indien nodig ook een certificaatvertrouwenslijst, kopieert u de bestanden naar de computer met de containerserver voor webtoepassingen.
- Configureer HTTPS op de containerserver voor webtoepassingen.

Verwante informatie

Communicatie tussen BI-platformonderdelen begrijpen [pagina 191]
Containerservers voor webtoepassingen gebruiken met een omgekeerde proxy [pagina 542]

13.1.4.1 Een PKCS12-certificaatarchief maken

U kunt op verschillende manieren een PKCS12-certificaatarchief of Java-keystorebestand maken, en daarvoor verschillende hulpprogramma's gebruiken. Welke manier u gebruikt, is afhankelijk van de beschikbaarheid van en uw bekendheid met de hulpprogramma's.

Het volgende voorbeeld laat zien hoe u een PKCS12-bestand maakt met Microsoft IIS (Internet Information Services) en de MMC (Microsoft Management Console) voor Windows 2008.

1. Meld u als beheerder aan bij een computer waarop een containerserver voor webtoepassingen wordt uitgevoerd.
2. Vraag vanuit IIS een certificaat aan bij de certificeringsinstantie. Zie de Help voor IIS voor meer informatie hierover.
3. Start de MMC door eerst te klikken op *Start* > *Uitvoeren*. Typ vervolgens `mmc.exe` en klik op *OK*.
4. Voeg als volgt de module Certificaten toe aan de MMC:
   a. Klik in het menu *Bestand* op *Module toevoegen/verwijderen*.
      Het venster *Modules toevoegen of verwijderen* wordt nu weergegeven.
   b. Selecteer in de lijst *Beschikbare modules* de optie *Certificaten* en klik op *Toevoegen*.
   c. Selecteer *Computeraccount* en klik op *Volgende*.
   d. Selecteer *Lokale computer* en klik op *Voltooien*.
   e. Klik op *OK*.

   De module Certificaten wordt toegevoegd aan de MMC.
5. Vouw in de MMC *Certificaten* uit en selecteer het gewenste certificaat.
6. Klik in het menu *Actie* op *Alle taken* > *Exporteren*.
   De *wizard Certificaat exporteren* wordt gestart.
7. Klik op *Volgende*.
8. Selecteer *Ja, de persoonlijke sleutel exporteren* en klik op *Volgende*.
9. Selecteer *Personal Information Exchange - PKCS #12 (*.pfx)* en klik op *Volgende*.
10. Typ het wachtwoord dat u voor het maken van het certificaat hebt gebruikt en klik op *Volgende*. Typ dit wachtwoord in het vak *Wachtwoord persoonlijke sleutel* wanneer u HTTPS configureert voor de containerserver voor webtoepassingen.

Er wordt een PKCS12-certificaatarchief gemaakt.

13.1.4.2 Een certificaatvertrouwenslijst maken

1. Meld u als beheerder aan bij een computer waarop een containerserver voor webtoepassingen wordt uitgevoerd.
2. Start de MMC (Microsoft Management Console).
3. Voeg de module Internet Information Services toe:
   a. Selecteer in het menu *Bestand* de optie *Module toevoegen/verwijderen*.
   b. Selecteer in de lijst *Beschikbare modules* de optie *Internet Information Services (IIS) Manager* en klik op *Toevoegen*.
   c. Klik op *OK*.
   De module IIS wordt toegevoegd aan de MMC.
4. Volg de stappen die hier worden beschreven om een certificaatvertrouwenslijst te maken: http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard .

13.1.4.3 HTTPS/SSL configureren

Voordat u HTTPS/SSL op uw containerserver voor webtoepassingen kunt configureren, moet u controleren of u al een PCKS12-bestand of een JKS-keystorebestand hebt gemaakt, en dit bestand hebt gekopieerd naar de computer waarop de containerserver voor webtoepassingen is geïnstalleerd.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de containerserver voor webtoepassingen waarvoor u HTTPS wilt inschakelen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel in het gedeelte *HTTPS configureren* het selectievakje *HTTPS inschakelen* in.
4. Typ in het vak *Binden aan hostnaam of IP-adres* het IP-adres waarvoor de certificaten zijn uitgegeven en waaraan u de containerserver voor webtoepassingen wilt binden.
   De HTTPS-services worden geleverd via een IP-adres dat u opgeeft.
5. Geef in het vak *HTTPS-poort* een poortnummer op voor de containerserver voor webtoepassingen waarop de HTTPS-services kunnen worden geleverd. Controleer of deze poort vrij is. Als u gebruikers wilt toestaan om van buiten een firewall verbinding te maken met de containerservers voor webtoepassingen, moet u controleren of deze poort is geopend in de firewall.
6. Als u SSL configureert met een omgekeerde proxy, geeft u de hostnaam en poort van de proxyserver op in de vakken *Proxy-hostnaam* en *Proxy-poort*.
7. Selecteer een protocol in de lijst *Protocol*. De beschikbare opties zijn:
   - *SSL*
     SSL (Secure Sockets Layer) is een protocol voor codering van het netwerkverkeer.
   - *TLS*
     TLS (Transport Layer Security) is een recenter en uitgebreider protocol. De verschillen tussen SSL en TLS zijn klein, maar TLS beschikt over een sterker coderingsalgoritme.

8. Typ het bestandstype voor het certificaat in het vak *Type certificaatarchief*. De beschikbare opties zijn:
   - *PKCS12*
     Selecteer PKCS12 als u liever werkt met Microsoft-hulpprogramma's.
   - *JKS*
     Selecteer JKS als u liever werkt met Java-hulpprogramma's.
9. Geef in het vak *Locatie certificaatarchief* het pad op waarnaar u het certificaatarchief of Java-keystorebestand hebt gekopieerd of verplaatst.
10. Typ het wachtwoord in het vak *Wachtwoord persoonlijke sleutel*.

    PKCS12-certificaatarchieven en JKS-keystorebestanden hebben persoonlijke sleutels die zijn beveiligd met een wachtwoord om toegang door onbevoegden te voorkomen. U moet een wachtwoord opgeven voor toegang tot de persoonlijke sleutels zodat de containerserver voor webtoepassingen toegang tot de persoonlijke sleutels krijgt.
11. Het wordt aanbevolen om een certificaatarchief of keystorebestand te gebruiken waarin ofwel een enkel certificaat is opgeslagen, of waarin het desbetreffende certificaat als eerste is vermeld. Als u een certificaatarchief of keystorebestand gebruikt dat meer dan één certificaat bevat, moet u in het vak *Certificaatalias* de alias voor het certificaat opgeven.
12. Als u wilt dat de containerserver voor webtoepassingen alleen HTTPS-aanvragen van bepaalde clients accepteert, moet u clientverificatie inschakelen.

    Met clientverificatie worden geen gebruikers geverifieerd. De verificatie zorgt ervoor dat op containerserver voor webtoepassingen alleen HTTPS-aanvragen van bepaalde clients worden verwerkt.
    a. Schakel het selectievakje *Clientverificatie inschakelen* in.
    b. Typ in het vak *Locatie certificaatvertrouwenslijst* de locatie van het PCKS12-bestand of JKS-keystorebestand dat de vertrouwde lijst bevat.

> **Opmerking**
>
> Het type certificaatvertrouwenslijst moet hetzelfde zijn als het type certificaatarchief.

> **Opmerking**
>
> Raadpleeg Voor RESTful-webservices [pagina 405] voor meer informatie over het vastleggen van trusted verificatie met X.509-certificaten.

> **Opmerking**
>
> U kunt het certificaat van een ABAP-systeem naar het Bi-platform importeren door de volgende opdracht uit te voeren: `keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` . Raadpleeg de onderstaande tabel om de opdracht te begrijpen:
>
> | Opdracht | Beschrijving |
> | --- | --- |
> | -alias | Aliasnaam |
> | -bestand | Bestandspad van certificaat ABAP-systeem |

Opdracht	Beschrijving
-keystore	Bestandspad van de trusted keystore.

c. Typ in het vak *Wachtwoord voor toegang tot privésleutel certificaatvertrouwenslijst* het wachtwoord voor toegang tot de persoonlijke sleutels in het bestand met de certificaatvertrouwenslijst.

> **Opmerking**
>
> Als u clientverificatie inschakelt en de gebruiker van een browser- of webservice niet is geverifieerd, wordt de HTTPS-verbinding geweigerd.

13. Klik op *Opslaan en sluiten*.
14. Open het scherm *Gegevens* en controleer of de HTTPS-connector in de lijst *Actieve connectors van containerserver voor webtoepassingen* staat. Als HTTPS niet in deze lijst staat, controleert u of de HTTPS-connector juist is geconfigureerd.

13.1.5 Ondersteunde verificatiemethoden

De WACS ondersteunt de volgende verificatiemethoden:

- Enterprise
- LDAP
- AD Kerberos

De WACS ondersteunt de volgende verificatiemethoden niet:

- NT
- AD NTLM
- LDAP met eenmalige aanmelding

13.1.6 AD Kerberos configureren voor de WACS

Als u AD Kerberos-verificatie wilt configureren voor de WACS, moet u eerst de ondersteuning van AD instellen op de computer. U moet de volgende stappen uitvoeren.

- De Windows AD-beveiligingsinvoegtoepassing inschakelen.
- Gebruikers en groepen toewijzen.
- Een serviceaccount instellen.
- Beperkte overdracht instellen.
- Kerberos-verificatie inschakelen in de Windows AD-invoegtoepassing voor de WACS.
- Configuratiebestanden maken.

Wanneer u de computer waarop de WACS wordt gehost, hebt ingesteld voor gebruik van AD Kerberos-verificatie, moet u extra configuratiestappen uitvoeren via de CMC (Central Management Console).

Als u via AD Kerberos eenmalige aanmelding configureert voor Web Services SDK en QaaWS, moet u ook de WACS en de computer waarop de WACS wordt gehost, configureren.

Verwante informatie

Windows Active Directory-beveiligingsinvoegtoepassing [pagina 294]
Windows AD-gebruikers en -groepen toewijzen [pagina 295]
Een serviceaccount aanmaken voor AD-verificatie met Kerberos [pagina 293]
De SIA uitvoeren onder de BI-platformserviceaccount [pagina 302]
Kerberos-verificatie inschakelen in de Windows AD-invoegtoepassing voor de WACS [pagina 522]
Configuratiebestanden maken [pagina 523]
De WACS configureren voor AD Kerberos [pagina 526]
Eenmalige AD Kerberos-aanmelding configureren [pagina 529]

13.1.6.1 Kerberos-verificatie inschakelen in de Windows AD-invoegtoepassing voor de WACS

Voor ondersteuning van Kerberos moet u de Windows Active Directory-beveiligingsinvoegtoepassing in de CMC configureren voor Kerberos-verificatie. Dit houdt het volgende in:

- Controleren of Windows Active Directory-verificatie is ingeschakeld.
- De beheerdersaccount voor Active Directory invoeren.

  > **Opmerking**
  >
  > voor deze account is alleen leestoegang tot Active Directory vereist. Er zijn dus geen andere rechten nodig.

- Kerberos-verificatie en desgewenst eenmalige aanmelding inschakelen.
- De SPN (Service Principal Name) invoeren voor de serviceaccount.

13.1.6.1.1 Vereisten

Voordat u de Windows Active Directory-beveiligingsinvoegtoepassing voor Kerberos configureert, moet u de volgende taken uitvoeren:

- Een serviceaccount aanmaken voor AD-verificatie met Kerberos [pagina 293]
- De SIA uitvoeren onder de BI-platformserviceaccount [pagina 302]
- Windows AD-gebruikers en -groepen toewijzen [pagina 295]

13.1.6.1.2 De Windows Active Directory-beveiligingsinvoegtoepassing voor Kerberos configureren

1. Ga naar het beheergebied *Verificatie* van de CMC.
2. Dubbelklik op *Windows AD*.
3. Zorg dat het selectievakje *Windows Active Directory (AD) inschakelen* is ingeschakeld.
4. Selecteer *Kerberos-verificatie gebruiken* in het gebied *Verificatieopties*.
5. Als u eenmalige aanmelding bij een database wilt configureren, schakelt u het selectievakje *Beveiligingscontext in cache (vereist voor SSO naar database)* in.
6. Voer in het veld *Naam van service-principal* de account en het domein in van de serviceaccount of de SPN-toewijzing.

   Gebruik de volgende notatie, waarbij `<svcacct>` de naam is van de serviceaccount of SPN die u eerder hebt gemaakt en `<DNS.COM>` de volledige naam van het domein in hoofdletters. De serviceaccount is bijvoorbeeld svcacct@DNS.COM en de SPN BOBJCentralMS/een_naam@DOMEIN.COM.

   > ⓘ Opmerking
   >
   > - Als u wilt toestaan dat gebruikers van andere domeinen dan het standaarddomein zich kunnen aanmelden, geeft u de SPN op die u eerder hebt toegewezen.
   > - De serviceaccount is hoofdlettergevoelig. Het gebruik van hoofdletters en kleine letters in de account moet exact overeenkomen met de gegevens in het Active Directory-domein.
   > - Dit moet de account zijn waarmee u de BI-platformservers uitvoert of de SPN die is toegewezen aan deze account.

7. Als u eenmalige aanmelding wilt configureren, schakelt u *Eenmalige aanmelding inschakelen voor geselecteerde verificatiemodus* in.

   > ⓘ Opmerking
   >
   > Als u eenmalige aanmelding hebt ingeschakeld, moet de WACS worden geconfigureerd.

Verwante informatie

Eenmalige AD Kerberos-aanmelding configureren [pagina 529]

13.1.6.2 Configuratiebestanden maken

Bij de algemene procedure voor de configuratie van Kerberos op de toepassingsserver moet u de volgende stappen uitvoeren:

- Het Kerberos-configuratiebestand maken.
- Het JAAS-aanmeldingsconfiguratiebestand maken.

> **Opmerking**
>
> - Het standaard Active Directory-domein moet worden opgegeven in hoofdletters en de DNS-notatie.
> - Het is niet meer nodig om MIT Kerberos voor Windows te downloaden en te installeren. Ook hebt u geen KEY-bestand meer nodig voor uw serviceaccount.

13.1.6.2.1 Het Kerberos-configuratiebestand maken

Voer de volgende stappen uit om het Kerberos-configuratiebestand te maken.

1. Maak het bestand `krb5.ini` als dit nog niet bestaat en sla het op in `C:\Windows` voor Windows.

   > **Opmerking**
   >
   > U kunt dit bestand opslaan op een andere locatie. Als u dit doet, moet u deze locatie echter opgeven in het veld *Locatie van Krb5.ini-bestand* op de pagina *Eigenschappen* voor de WACS-server in de CMC.

2. Voeg de volgende vereiste informatie toe aan het Kerberos-configuratiebestand:

```
[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 =
}
```

   > **Opmerking**
   >
   > `DNS.COM` is de DNS-naam van uw domein dat in hoofdletters in FQDN-notatie moet worden ingevoerd.

   > **Opmerking**
   >
   > `kdc` is de hostnaam van de domeincontroller.

> **Opmerking**
>
> U kunt meerdere domeinvermeldingen toevoegen aan de sectie [realms] als de gebruikers zich aanmelden vanaf verschillende domeinen. Zie Voorbeelden van het bestand Krb5.ini [pagina 525] of voor een voorbeeld van dit bestand met meerdere domeinvermeldingen.

> **Opmerking**
>
> In een configuratie met meerdere domeinen kan onder `[libdefaults]` de waarde `default_realm` elk gewenst domein zijn. U kunt het beste het domein gebruiken met het grootste aantal gebruikers dat de verificatie uitvoert met de AD-account.

13.1.6.2.2 Het configuratiebestand voor de JAAS-aanmelding maken

1. Maak een bestand met de naam `bscLogin.conf` als dit nog niet bestaat en sla het op de standaardlocatie `C:\Windows` op.

   > **Opmerking**
   >
   > U kunt dit bestand opslaan op een andere locatie. Als u dit doet, moet u deze locatie echter opgeven in het veld *Locatie van bscLogin.conf-bestand* op de pagina *Eigenschappen* voor de WACS-server in de CMC.

2. Voeg de volgende code toe aan het JAAS-configuratiebestand `bscLogin.conf`:

   ```
   com.businessobjects.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required;
   };
   ```

3. Sla het bestand op en sluit het.

13.1.6.2.3 Voorbeelden van het bestand Krb5.ini

Voorbeeld van het bestand Krb5.ini met meerdere domeinen

Hierna ziet u een voorbeeldbestand met meerdere domeinen:

```
[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
        }
```

Voorbeeldbestand Krb5.ini met één domein

Hieronder volgt een voorbeeld van het bestand Krb5.ini met één domein.

```
[libdefaults]
        default_realm = ABCD.MFROOT.ORG
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        ABCD.MFROOT.ORG = {
            kdc = ABCDIR20.ABCD.MFROOT.ORG
            kdc = ABCDIR21.ABCD.MFROOT.ORG
            kdc = ABCDIR22.ABCD.MFROOT.ORG
            kdc = ABCDIR23.ABCD.MFROOT.ORG
            default_domain = ABCD.MFROOT.ORG
        }
```

13.1.6.3 De WACS configureren voor AD Kerberos

Wanneer u de computer hebt geconfigureerd waarop de WACS voor de AD Kerberos-verificatie wordt gehost, moet u de WACS zelf configureren via de CMC (Central Management Console).

13.1.6.3.1 WACS configureren voor AD Kerberos

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de WACS waarvoor u AD wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.

3. Geef in het veld *Locatie van Krb5.ini-bestand* het pad op naar het configuratiebestand `krb5.ini`.
4. Geef in het veld *Locatie van bscLogin.conf-bestand* het pad op naar het configuratiebestand `bscLogin.conf`.
5. Klik op *Opslaan en sluiten*.
6. Start de containerserver voor webtoepassingen opnieuw.

13.1.6.4 Problemen met Kerberos oplossen

Deze stappen kunnen u helpen bij het oplossen van problemen met de configuratie van Kerberos:

- De logboekfunctie inschakelen
- De Kerberos-configuratie testen

13.1.6.4.1 De Kerberos-logboekfunctie inschakelen

1. Start de CCM (Central Configuration Manager) en klik op *Servers beheren*.
2. Geef de aanmeldingsreferenties op.
3. Stop de containerserver voor webtoepassingen in het scherm *Servers beheren*.
4. Klik op *Weblaagconfiguratie*.

   > **Opmerking**
   >
   > Het pictogram *Configuratie van weblaag* is alleen beschikbaar als u een containerserver voor webtoepassingen selecteert die is gestopt.

   Het scherm *Configuratie weblaag* verschijnt.
5. Kopieer onder *Opdrachtregelparameters* de volgende tekst aan het einde van de parameters:

   ```
   “-Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.Kerberos.debug=true”
   ```
6. Klik op *OK*.
7. Start de containerserver voor webtoepassingen in het scherm *Servers beheren*.

13.1.6.4.2 De Kerberos-configuratie testen

Voer de volgende opdracht uit om de Kerberos-configuratie te testen, waarbij `servact` de naam is van de serviceaccount en het domein van de CMS, en `wachtwoord` het wachtwoord van de serviceaccount.

```
<INSTALLDIR>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Bijvoorbeeld:

```
 C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM
Password
```

Als het probleem zich blijft voordoen, controleert u of u voor het domein en de SPN (Service Principal Name) exact dezelfde hoofdletters en kleine letters hebt opgegeven als in Active Directory.

13.1.6.4.3 De toegewezen AD-gebruiker kan zich niet aanmelden bij het BI-platform op de WACS

De volgende twee problemen kunnen optreden, ondanks het feit dat de gebruikers zijn toegewezen aan het BI-platform.

13.1.6.4.3.1 Aanmeldingsfout vanwege verschillende UPN- en SAM-namen in AD

De Active Directory-id van een gebruiker is toegewezen aan het BI-platform. Desondanks kan de gebruiker zich niet aanmelden bij CMC met AD-verificatie en Kerberos met de volgende notatie: `DOMAIN\ABC123`

Dit probleem kan zich voordoen als de gebruiker in Active Directory is ingesteld met een UPN- en SAM-naam die niet gelijk aan elkaar zijn (bijvoorbeeld een andere combinatie van hoofdletters en kleine letters of anderszins). Hier volgen twee voorbeelden die een probleem kunnen opleveren:

- De UPN is abc123@bedrijf.com, maar de SAM-naam is DOMEIN\ABC123.
- De UPN is jsmit@bedrijf, maar de SAM-naam is DOMEIN\jansmit.

U kunt dit probleem op twee manieren oplossen:

- Laat gebruikers zich aanmelden met UPN-naam in plaats van de SAM-naam.
- Zorg ervoor dat de SAM-accountnaam en de UPN-naam hetzelfde zijn.

13.1.6.4.3.2 Fout vóór de verificatie

Een gebruiker die zich eerder wel kon aanmelden, kan zich nu niet meer aanmelden. De volgende fout wordt weergegeven: Accountgegevens worden niet herkend. In de WACS-logboeken wordt de volgende fout aangegeven: `Voorverificatiegegevens zijn ongeldig (24)`.

Dit kan optreden wanneer de Kerberos-gebruiker geen wijziging heeft aangebracht in UPN in AD. Dit houdt mogelijk in dat de Kerberos-gebruikersdatabase en de AD-gegevens niet zijn gesynchroniseerd.

Stel het wachtwoord van de gebruiker opnieuw in AD in om dit probleem op te lossen. Hierdoor worden de wijzigingen correct doorgevoerd.

13.1.7 Eenmalige AD Kerberos-aanmelding configureren

Als u eenmalige aanmelding van AD Kerberos wilt configureren voor BI-startpunt of de webservices SDK en QaaWS, moet u ervoor zorgen dat u zowel de WACS als de computer waarop WACS wordt gehost, hebt geconfigureerd voor AD Kerberos-verificatie.

Als u WACS wilt configureren voor eenmalige aanmelding van AD Kerberos, moet u eerst de computer configureren waarop WACS gehost wordt, en vervolgens de WACS zelf configureren.

> ⓘ Opmerking
>
> Als u eenmalige aanmelding wilt gebruiken in een omgeving met een omgekeerde proxy, moet u de informatie over beveiliging van deze handleiding lezen.

Verwante informatie

Overzicht van beveiliging [pagina 151]
AD Kerberos configureren voor de WACS [pagina 521]
Uw computer configureren voor eenmalige aanmelding van AD Kerberos [pagina 529]
WACS configureren voor eenmalige aanmelding van AD Kerberos [pagina 530]

13.1.7.1 Uw computer configureren voor eenmalige aanmelding van AD Kerberos

Als u eenmalige aanmelding van AD Kerberos wilt configureren voor Webservices SDK en QaaWS moet u eerst de computer configureren waarop de Containerservers voor webtoepassingen wordt geconfigureerd:

- Beperkte machtiging voor Vintela SSO configureren [pagina 316]
- De serviceaccount instellen voor Vintela SSO [pagina 313]
- Meerdere SPN's installeren [pagina 529]
- De groottebeperking van de koptekst van de WACS verhogen [pagina 530]

In de volgende secties wordt beschreven hoe u deze stappen kunt uitvoeren.

13.1.7.1.1 Meerdere SPN's installeren

Gebruik van meerdere SPN's wordt niet ondersteund.

13.1.7.1.2 De groottebeperking van de koptekst van de WACS verhogen

In Active Directory wordt een Kerberos-token gemaakt die wordt gebruikt in het verificatieproces. Deze token wordt in de HTTP-koptekst opgeslagen. Uw WACS heeft een standaardgrootte voor de HTTP-koptekst, die voor de meeste gebruikers groot genoeg is. Deze koptekstgrootte kan worden aangepast.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de WACS waarvoor u de HTTP-koptekstgrootte wilt aanpassen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Onder de sectie *HTTP-configuratie*, *Configuratie van HTTP via proxy* of *HTTPS-configuratie* geeft u een waarde op in het veld *Maximale HTTP-koptekstgrootte (bytes)*.
4. Klik op *Opslaan en sluiten*.
5. Start de servers opnieuw.

13.1.7.2 WACS configureren voor eenmalige aanmelding van AD Kerberos

U kunt een containerserver voor webtoepassingen configureren om eenmalige aanmelding van AD Kerberos te gebruiken. Eenmalige aanmelding van AD Kerberos wordt ondersteund. AD NTLM wordt niet ondersteund.

Voordat u WACS configureert, moet u de eenmalige aanmelding van AD Kerberos configureren voor de computer waarop de WACS wordt gehost.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de containerserver voor webtoepassingen die u wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.
3. *Eenmalige aanmelding van Kerberos Active Directory* selecteren.
4. Geef waarden op voor standaard AD-domein, Naam van service-principal en Keytab-bestandseigenschappen en klik op *Opslaan en sluiten*.
5. Start de containerserver voor webtoepassingen opnieuw.

Eenmalige aanmelding van Active Directory is klaar voor gebruik.

13.1.7.3 Kerberos en eenmalige aanmelding bij database configureren

Eenmalige aanmelding bij de database wordt ondersteund voor implementaties die aan alle volgende vereisten voldoen:

- De implementatie van het BI-platform vindt plaats op WACS.
- WACS is geconfigureerd met AD met Kerberos
- De database waarvoor eenmalige aanmelding is vereist, is een ondersteunde versie van SQL Server of Oracle.

- Aan de groepen of gebruikers die toegang tot de database moeten hebben, moeten machtigingen zijn toegewezen in SQL Server of Oracle.
- Het selectievakje Beveiligingscontext in cache (dat vereist is voor eenmalige aanmelding bij de database) op de pagina voor AD-verificatie van de CMC is ingeschakeld.

De laatste stap is het aanpassen van het bestand `krb5.ini` zodat eenmalige aanmelding bij de database wordt ondersteund.

> **Opmerking**
>
> Deze instructies dienen als uitleg van de configuratie van eenmalige aanmelding bij de database. Als u end-to-end eenmalige aanmelding bij de database wilt configureren, moet u ook de configuratiestappen die vereist zijn voor eenmalige Vintela-aanmelding. Zie Eenmalige AD Kerberos-aanmelding configureren [pagina 529] voor meer informatie

13.1.7.3.1 Eenmalige aanmelding bij de database configureren

1. Open het bestand `krb5.ini` dat wordt gebruikt voor de implementatie van het BI-platform.

   De standaardlocatie van dit bestand is de map C:\Windows op de webtoepassingsserver.
2. Ga naar de sectie `[libdefaults]` van het bestand.
3. Voer de volgende tekenreeks in vóór het begin van de sectie `[realms]` van het bestand:

   ```
   forwardable = true
   ```
4. Sla het bestand op en sluit het.
5. Uw WACS opnieuw starten

13.1.8 RESTful-webservices configureren

Met de Business Intelligence-platform RESTful-webservices SDK hebt u toegang tot BI-platform via het HTTP-protocol. Hiermee kunnen gebruikers door de gegevensopslagruimte van BI-platform navigeren en objecten plannen met elke programmeertaal die HTTP-aanvragen ondersteunt. RESTful-webservices zijn geïnstalleerd als onderdeel van WACS.

In deze sectie wordt uitgelegd hoe u RESTful-webservices kunt beheren. Zie de *Ontwikkelaarshandleiding voor Business Intelligence-platform RESTful-webservice* voor meer informatie over RESTful-webservices.

13.1.8.1 Toepassingen

13.1.8.1.1 De basis-URL voor RESTful-webservices configureren

Als uw implementatie van BI-platform een proxyserver gebruikt of meer dan één exemplaar van de WACS (Web Application Container Server) bevat, moet u mogelijk de basis-URL configureren voor gebruik met

RESTful-webservices. Voordat u de basis-URL configureert, moet u de servernaam en het poortnummer weten die reageren op aanvragen van RESTful-webservices.

De basis-URL wordt gebruikt als deel van elke aanvraag van RESTful-webservices. Ontwikkelaars zoeken de basis-URL via een programma en gebruiken deze om aanvragen van RESTful-webservices naar de juiste server en poort te leiden. De basis-URL wordt ook gebruikt in antwoorden van RESTful-webservices om hyperlinks naar andere RESTful-bronnen te definiëren.

> **Opmerking**
>
> In standaardinstallaties van het BI-platform wordt de basis-URL gedefinieerd als `http://<servername>:6405/biprws`. Vervang `<servername>` door de naam van de server die RESTful-webservices host.

1. Meld u bij de CMC (Central Management Console) aan als beheerder.
2. Klik in de CMC op *Toepassingen*.
   Een lijst met toepassingen wordt weergegeven.
3. Klik met de rechtermuisknop op *RESTful Web Service* > *Eigenschappen*.
   De pagina *Eigenschappen: RESTful-webservice* wordt weergegeven. Het selectievakje *Pad relatieve URL gebruiken* is aan de pagina toegevoegd zodat u de RESTful-webservice via de URL in uw browser kunt starten. Zie SAP Note 3048101 voor meer informatie.
4. In het tekstvak *URL voor toegang* typt u de naam van de basis-URL voor RESTful-webservices.
   Typ bijvoorbeeld `http://<servername>:<portnumber>/biprws`. Vervang `<servername>` en `<portnumber>` door de naam van de server en de poort die reageren op aanvragen van RESTful-webservices.

   > **Let op**
   >
   > - **Tomcat-server, WACS-server, JBoss, SAP NetWeaver en WebSphere-server worden ondersteund** voor API's van RESTful-webservices.
   > - De *URL voor toegang* geeft de WACS-URL **standaard** weer. Als u de API's van RESTful-webservices op de Tomcat-webserver wilt gebruiken, moet u de vereiste waarden van `<server>` en `<port>` dienovereenkomstig aanpassen.

5. Klik op *Opslaan en sluiten*.

   > **Opmerking**
   >
   > Als u *Pad relatieve URL gebruiken* inschakelt, wordt de relatieve URL van de browser gebruikt.

13.1.8.2 WACS-eigenschappen

13.1.8.2.1 De opdrachtregelparameters Methods en Headers configureren

Als beheerder kunt u beperken welke methoden en kopteksten kunnen worden gebruikt door RESTful-webservices, door de toepasselijke opties toe te voegen aan *Opdrachtregelparameters* in de eigenschappen

van uw Containerservice voor webtoepassingen. Wanneer u de parameters wijzigt, moet de Containerservice voor webtoepassingen mogelijk opnieuw worden gestart.

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld `MySIA.WebApplicationContainerServer`, en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.
4. Voer in het gebied *Opdrachtregelparameters* de methoden en kopteksten in die worden toegestaan.

   Elke optiegroep wordt omgeven door dubbele aanhalingstekens. Gebruik andere methoden dan `GET`, `HEAD` en `POST`. Gebruik komma's om de optiewaarden te scheiden, zoals `PUT` en `DELETE` die in het volgende voorbeeld worden weergegeven.

   ```
   "-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
   "-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
   Authenticate"
   ```

   > **Opmerking**
   >
   > De standaardwaarde die alle methoden en kopteksten toestaat, is * (asterisk). U kunt ook de opdrachtregelparameters weglaten om hetzelfde effect te bereiken.

5. Klik op *Opslaan en sluiten*.
6. Start de service opnieuw door met de rechtermuisknop op de naam van de Containerserver voor webtoepassingen te klikken, bijvoorbeeld `MySIA.WebApplicationContainerServer`, en klik op *Server opnieuw starten*.

13.1.8.2.2 Configuratie van systeemeigenschappen

13.1.8.2.2.1 Stapelen van foutberichten inschakelen

Als beheerder kunt u de foutberichten configureren die worden geretourneerd door de RESTful-webservices om te worden opgenomen in de stapel met fouten. De stapel met fouten biedt extra foutopsporingsinformatie die kan worden gebruikt om te ontdekken waar fouten zijn opgetreden.

> **Opmerking**
>
> Het is raadzaam het stapelen van fouten niet in te schakelen in productiescenario's, omdat er informatie over het BI-platform kan worden gegeven die u niet aan eindgebruikers wilt laten zien. Schakel het stapelen van fouten in productiescenario's in voor foutopsporing, en schakel het weer uit als het niet meer nodig is.

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld op `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.
4. Selecteer in het gedeelte *RESTful-.webservice Stapel met fouten weergeven*.

5. Klik op *Opslaan en sluiten*.

Informatie van de stapel met fouten wordt opgenomen in foutberichten van RESTful-webservices.

13.1.8.2.2.2 Het standaardaantal items instellen dat op elke pagina wordt weergegeven

Wanneer een antwoord van de RESTful-webservice een feed met een groot aantal items bevat, kan het antwoord in pagina's worden gedeeld. U kunt het standaardaantal items configureren dat op elke pagina wordt weergegeven. Wanneer ontwikkelaars aanvragen voor de RESTful-webservice maken, kunnen ze het aantal items opgeven dat moet worden weergegeven op elke pagina. Als ze deze waarde echter niet opgeven, wordt de standaardpaginagrootte gebruikt.

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld op `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.
4. In het gedeelte *RESTful-webservice* typt u de standaardpaginagrootte in het tekstgedeelte *Standaardaantal objecten op één pagina*.
5. Klik op *Opslaan en sluiten*.

13.1.8.2.2.3 De time-outwaarde van een aanmeldingstoken instellen

Aanmeldingstokens verlopen nadat ze een tijdlang niet zijn gebruikt. U kunt instellen hoelang een ongebruikt aanmeldingstoken geldig blijft.

> **Opmerking**
>
> De time-outwaarde van het aanmeldingstoken is standaard een uur.

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld op `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.
4. Typ in het gedeelte *RESTful-webservice* in het tekstgedeelte *Time-out van Enterprise-sessietoken (minuten)* het aantal minuten dat een aanmeldingstoken geldig moet blijven.
5. Klik op *Opslaan en sluiten*.

13.1.8.2.2.4 Instellingen van sessiepool configureren

U kunt de serverprestaties verbeteren door een sessiepool te gebruiken. De sessiepool plaatst actieve sessies van de RESTful-webservice in cache zodat ze opnieuw kunnen worden gebruikt wanneer een gebruiker een andere aanvraag verstuurt waarvoor hetzelfde aanmeldingstoken wordt gebruikt in de HTTP-aanvraagheader. De grootte van de sessiepool definieert het aantal sessies in cache dat tegelijk moet worden opgeslagen, en de time-outwaarde van de sessie bepaalt hoelang een sessie in cache wordt geplaatst.

U kunt de grootte van de sessiepool en de time-outwaarde van de sessie instellen:

1. Meld u bij de CMC (Central Management Console) aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld op `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.
4. Typ het maximumaantal sessies dat in cache moet worden geplaatst in het tekstvak *Poolgrootte* van het gedeelte *RESTful-webservice*.
5. Typ de time-outwaarde van de sessiepool in het tekstvak *Time-out van sessiepool (minuten)* van het gedeelte *RESTful-webservice*.
6. Klik op *Opslaan en sluiten*.
7. Klik met de rechtermuisknop op de WACS-server, bijvoorbeeld `MySIA.WebApplicationContainerServer`, en klik vervolgens op *Server opnieuw starten*.

13.1.8.2.2.5 HTTP Basic-verificatie inschakelen

Met HTTP Basic-verificatie kunnen gebruikers aanvragen voor de RESTful-webservice maken zonder een aanmeldingstoken op te geven. Als HTTP Basic-verificatie is ingeschakeld, worden gebruikers gevraagd hun gebruikersnaam en wachtwoord op te geven bij de eerste keer dat ze een aanvraag voor de RESTful-webservice maken.

> **Opmerking**
>
> Gebruikersnamen en wachtwoorden worden niet veilig verzonden met HTTP Basic-verificatie, tenzij deze samen met HTTPS wordt gebruikt.

Wanneer u HTTP Basic-verificatie inschakelt, stelt u het standaardverificatietype voor HTTP Basic op SAP, Enterprise, LDAP of WinAD in. Gebruikers kunnen het standaardverificatietype voor HTTP Basic overschrijven wanneer ze zich aanmelden.

Voor het aanmelden bij het BI-platform met HTTP Basic-verificatie wordt een licentie gebruikt. Als de sessiepool die in cache is geplaatst, wordt gebruikt, gebruikt de aanvraag de licentie die is gekoppeld aan de sessie in cache. Als de sessiepool die in cache is geplaatst, niet wordt gebruikt, wordt een licentie gebruikt terwijl de aanvraag in behandeling is en wordt deze vrijgegeven als de aanvraag voltooid is.

1. Meld u bij de CMC (Central Management Console) aan als beheerder.
2. Klik op *Server* > *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld op `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.

Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.

4. Selecteer in het gedeelte *RESTful-webservice HTTP Basic-verificatie inschakelen*.
5. (Optioneel) Selecteer in de lijst *Standaardverificatieschema voor HTTP Basic* het standaardverificatietype voor HTTP Basic.
6. Klik op *Opslaan en sluiten*.

Wanneer eindgebruikers zich aanmelden via HTTP Basic-verificatie, kunnen ze het verificatietype opgeven dat moet worden gebruikt. In een webbrowser typt de gebruiker `<verificatietype>\<gebruikersnaam>` in de gebruikersnaamprompt, en `<wachtwoord>` in de wachtwoordprompt.

Gebruikers moeten het attribuut `Verificatie` toevoegen aan de HTTP-aanvraagheader en de waarde instellen op `Basic <verificatietype>\<gebruikersnaam>:<wachtwoord>` om zich aan te melden met HTTP Basic-verificatie via een programma.

Vervang `<verificatietype>` door het verificatietype, `<gebruikersnaam>` door de gebruikersnaam en `<wachtwoord>` door het wachtwoord. Het verificatietype, de gebruikersnaam en het wachtwoord moeten base64-gecodeerd zijn zoals gedefinieerd door RFC 2617. Gebruikersnamen die het teken `:` bevatten, kunnen niet worden gebruikt met HTTP Basic-verificatie.

Verwante informatie

Instellingen van sessiepool configureren [pagina 535]

13.1.8.2.3 Cross-Origin Resource Sharing

13.1.8.2.3.1 Cross-Origin Resource Sharing configureren

Met de instelling *Configuratie Cross-Origin Resource Sharing* (CORS) kunt u een lijst met domeinnamen toevoegen, zodat gebruikers gegevens van meerdere bronnen op JavaScript-webpagina's kunnen ophalen. Dit is nodig om het beveiligingsbeleid te vermijden dat JavaScript- en Ajax-talen gebruiken om interdomeintoegang te voorkomen. Teneinde beveiligingsinbreuk te voorkomen, worden alleen websites die mogen worden opgeroepen, toegevoegd aan *Oorsprong toestaan* in de servereigenschappen van de Containerserver voor webtoepassingen in CMC.

De instelling *Maximumleeftijd (minuten)* is ook beschikbaar om de cacheverlooptijd aan te passen. Hiermee wordt ingesteld hoe lang browser HTTP-verzoeken kunnen bewaren.

> **Opmerking**
>
> Standaard wordt toegang tot alle domeinen met een * (asterisk) toegestaan.

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Server* > *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld `MySIA.WebApplicationContainerServer` en klik vervolgens op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.

4. Ga in het gebied *RESTful-webservice* naar het tekstvakje *Configuratie Cross-Origin Resource Sharing* naast *Oorsprong toestaan* en vervang het sterretje (*) door uw lijst met domeinnamen, die worden gescheiden door komma's. Bijvoorbeeld `http://origin1.server:8080, http://origin2.server:8080`
5. Voer in het tekstvakje *Maximumleeftijd (minuten)* in hoe lang browsers HTTP-verzoeken in cache mogen plaatsen.
6. Klik op *Opslaan en sluiten*.

13.1.8.2.4 Verificatie

13.1.8.2.4.1 web.xml configureren om eenmalige aanmelding van WinAD in te schakelen

Als u de RESTful-webservices wilt configureren om de eenmalige aanmelding van WinAD (Windows Active Directory) te herkennen, moet u het configuratiebestand `web.xml` bewerken, dat zich op de BI-platformserver bevindt. Voor meer informatie raadpleegt u de sectie "Using the SDK > Authentication > To get a logon token using an Active Directory Single Sign-On (AD SSO) account" in de *Business Intelligence Platform RESTful Web Service Developer Guide*.

Als de BI-platformserver de aanmeldingsreferenties voor eenmalige aanmelding van WinAD op een clientcomputer moet herkennen, moet u de sectie `Kerberos Proxy Filter` van het bestand `web.xml` als programmacode behandelen en waarden voor `idm.realm`, `idm.princ` en `idm.keytab` bijwerken die de gebruikte actieve mapomgeving reflecteren.

1. Zoek de `web.xml`-configuratie op `<boe-hoofdmap>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. Het volgende bestandspad is een voorbeeld.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\java\
pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. In het bestand `web.xml` behandelt u de se tie Kerberos Proxy Filter als programmacode door een code sluiten `-->` voor de code `<filter>` toe te voegen, en de code voor het sluiten `-->` te verwijderen.

```
  <!-- Kerberos Proxy Filter
    - Uncomment this filter and the corresponding filter-mapping to enable
Kerberos SSO
    - for Windows AD (secWinAD) authentication.
    - The following options must be specified (the rest are optional):
    -   idm.realm
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->
  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>
  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>
```

```
</web-app>
```

3. Werk de `<param-value>` voor elke instelling van `idm.realm`, `idm.princ` en `idm.keytab` bij met de waarden die in uw actieve mapomgeving zijn gebruikt.

```
    <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>
```

> **Opmerking**
>
> De waarde van `idm.keytab` verwijst naar een bestandspad op de BI-platformserver. Waarden voor `idm.realm` en `idm.prince` kunnen worden weergegeven vanuit de Central Management Console. Dubbelklik op het tabblad *Verificatie* in de CMC op *Windows AD*. De waarde voor `idm.realm` wordt ingesteld met de parameter *Standaard AD-domein* onder *Overzicht van AD-configuratie*. De waarde voor `idm.prince` wordt ingesteld met de parameter *Naam van service-principal* onder *Verificatieopties*.

4. Start de Containerservice voor webtoepassingen opnieuw op zodat de wijzigingen in `web.xml` worden herkend.
5. Gebruik een clientcomputer om te verifiëren dat een AD SSO-aanmeldingstoken kan worden opgehaald via de API van de RESTful-webservices, bijvoorbeeld `http://<boe_host>:6405/biprws/logon/adsso`.
6. Test de token met een `GET`-query met `X-SAP-LogonToken` in de koptekst en via de API van `/infostore`.

13.1.8.2.4.2 Vertrouwde verificatie inschakelen en configureren

Vertrouwde verificatie wordt geactiveerd en geconfigureerd via de CMC (Central Management Console) in gebieden zoals *Verificatie > Enterprise*, waar het is ingeschakeld. Er wordt een bestand met een gedeeld geheim is gegenereerd, *Gebruikers en groepen > Gebruikerslijst*, waar een account wordt gemaakt voor een vertrouwde gebruiker in het volgende pad *Servers > Lijst met servers > WACS > Eigenschappen*. Hier is de optie *Methode wordt opgehaald* geselecteerd voor API-aanmeldingstokenverzoeken `/logon/trusted`.

> **Opmerking**
>
> Om beveiligingsredenen mag vertrouwde verificatie niet worden ingeschakeld zonder HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie hierover.

1. Meld u bij de Central Management Console aan als beheerder.
2. Ga naar *Verificatie* > *Enterprise* en klik op *Vertrouwde verificatie is ingeschakeld*.
3. Klik op *Nieuw gedeeld geheim* en klik op *Gedeeld geheim downloaden*.
4. Klik op *Opslaan* en plaats het bestand `TrustedPrincipal.conf` op de standaardlocatie, namelijk `<EnterpriseDir>\<platform>`.
   Hieronder ziet u een voorbeeldlocatie:

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

   > **Opmerking**
   >
   > U kunt de standaardlocatie van het bestand `TrustedPrincipal.conf` met het gedeelde geheim wijzigen door een opdrachtregelvermelding toe te voegen in de CMC op *Servers > Lijst met servers > WACS > Eigenschappen > Opdrachtregelparameters* en de Containerservice voor webtoepassingen opnieuw te starten. Een opdrachtregelvermelding met `-Dbobj.trustedauth.home=` en de map `SharedSecrets` die in de hoofdmap van het station `C:\` van de BI-platformserver wordt geplaatst, ziet er als volgt uit:
   >
   > ```
   > "-Dbobj.trustedauth.home=C:\SharedSecrets"
   > ```

   > **Opmerking**
   >
   > U kunt de optie *Geldigheidsperiode van gedeeld geheim (dagen)* op de standaardwaarde nul (0) laten staan, zodat de geldigheidsperiode niet verstrijkt. De optie *Time-out van vertrouwde aanmeldingsaanvraag na N milliseconde(n) (0 betekent geen limiet)* kan op de standaardwaarde nul (0) blijven staan, zodat er geen tijdlimiet voor vertrouwde-aanmeldingsverzoeken is.

5. Klik op *Bijwerken* om de wijziging op te slaan.
6. Voeg een nieuwe gebruiker en een nieuw wachtwoord toe, bijvoorbeeld `bob` en `Passw0rd`, in *Gebruikers en groepen* > *Gebruikerslijst* via *Beheren > Nieuw > Nieuwe gebruiker*. Hef de selectie van *Gebruiker moet wachtwoord bij volgende aanmelding wijzigen* op en klik op *Maken en sluiten*.

> **Opmerking**
>
> U kunt ook een nieuwe gebruiker maken door op het pictogram *Nieuwe gebruiker maken* te klikken, of door met de rechtermuisknop te klikken op een open gebied van het venster waarin gebruikersnamen worden weergegeven en *Nieuw* > *Nieuwe gebruiker* te selecteren.

7. Ga naar *Servers* > *Kernservices* > *WACS* > *Eigenschappen*, schuif omlaag naar de sectie *Configuratie vertrouwde verificatie* en gebruik het menu *Methode wordt opgehaald* om *HTTP_HEADER*, *QUERY_STRING* of *COOKIE* te selecteren.

> **Opmerking**
>
> U kunt eventueel de *Parameter gebruikersnaam* wijzigen van het standaardlabel `X-SAP-TRUSTED-USER` in een ander duidelijk label (bijvoorbeeld `UserName`, `bankteller` of `nurse`) dat ontwikkelaars van RESTful-webservices moeten gebruiken.

8. Start de service opnieuw door met de rechtermuisknop op de naam van de Containerserver voor webtoepassingen te klikken, bijvoorbeeld `MySIA.WebApplicationContainerServer`. Klik vervolgens op *Server opnieuw starten*.

> **Opmerking**
>
> Als u de optie later onder *Methode wordt opgehaald* wijzigt zoals u kunt zien in stap 7, hoeft u de Containerserver voor webtoepassingen niet opnieuw op te starten.

9. Controleer of u een aanmeldingstoken kunt ophalen door de API `.../biprsw/logon/trusted/` te gebruiken en een `GET`-aanvraag te verzenden met het standaardkoptekstlabel `X-SAP-TRUSTED-USER` met de gebruikersnaam die in stap 6 is gemaakt.

13.1.8.2.4.3 De opdrachtregelparameter configureren om het configuratiebestand `TrustedPrincipal.conf` met het gedeelde geheim te configureren

RESTful-webservices hebben een opdrachtregelparameter om een andere locatie te kiezen voor het bestand `TrustedPrincipal.conf` voor vertrouwde verificatie.

Het bestand `TrustedPrincipal.conf` bevat een gedeelde geheime sleutel die wordt gegenereerd via de CMC: klik op *Verificatie* en klik vervolgens op *Enterprise*. Selecteer *Vertrouwde verificatie is ingeschakeld* en klik vervolgens op de knop *Nieuw gedeeld geheim*. Klik op *Gedeeld geheim downloaden* en sla het bestand op de standaardlocatie op.

Werk de opdrachtregel van de Containerserver voor webtoepassingen bij met een aangepast pad voor het bestand `TrustedPrincipal.conf`:

1. Meld u bij de Central Management Console aan als beheerder.
2. Klik op *Servers* en vervolgens op *Lijst met servers*.
3. Klik met de rechtermuisknop op uw Containerserver voor webtoepassingen, bijvoorbeeld `MySIA.WebApplicationContainerServer`, en klik op *Eigenschappen*.
   Het tabblad *Eigenschappen* voor de WACS-server wordt weergegeven.

4. Voer in het gebied *Opdrachtregelparameters* het pad in naar de map dat het bestand `TrustedPrincipal.conf` bevat.

   De tekenreeks wordt omsloten door dubbele aanhalingstekens, zoals u kunt zien in het volgende voorbeeld.

   ```
   "-Dbobj.trustedauth.home=C:\SharedSecrets"
   ```

   > **Opmerking**
   >
   > De standaardlocatie van het bestand `TrustedPrincipal.conf` is `<Enterprise_map>\<platform>`. Hieronder ziet u een voorbeeldlocatie:
   >
   > ```
   > C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise
   > XI 4.0\win64_x64
   > "
   > ```

5. Klik op *Opslaan en sluiten*.
6. Start de service opnieuw door met de rechtermuisknop op de naam van de Containerserver voor webtoepassingen te klikken, bijvoorbeeld `MySIA.WebApplicationContainerServer`, en klik op *Server opnieuw starten*.

13.1.9 Containerservers voor webtoepassingen en uw IT-omgeving

In deze sectie vindt u informatie over het configureren van een containerserver voor webtoepassingen in een complexe omgeving.

13.1.9.1 Containerservers voor webtoepassingen gebruiken met andere webservers

Een geïnstalleerde containerserver voor webtoepassingen werkt als een toepassingsserver en een webserver, zonder dat daarvoor extra configuratie nodig is. U kunt ondersteunde webservers, zoals IIS (Internet Information Services) en Apache, instellen voor het doorsturen van URL-adressen naar de containerserver voor webtoepassingen.

> **Opmerking**
>
> Het doorsturen van aanvragen vanuit IIS met behulp van een ISAPI-filter naar de containerserver voor webtoepassingen wordt niet ondersteund.

Op een containerserver voor webtoepassingen wordt niet het scenario ondersteund waarin de statische inhoud op een webserver staat en de dynamische inhoud op de containerserver voor webtoepassingen. De statische en dynamische inhoud moeten beide op de containerserver voor webtoepassingen staan.

13.1.9.2 Containerservers voor webtoepassingen gebruiken met een load balancer

Als u containerservers voor webtoepassingen wilt gebruiken in een implementatie met een load balancer voor hardware, moet u de load balancer configureren voor gebruik van IP-routing of actieve cookies. In dat geval worden, zodra een gebruikerssessie op een containerserver voor webtoepassingen is gestart, alle volgende aanvragen van dezelfde gebruiker naar dezelfde containerserver voor webtoepassingen gestuurd.

De containerserver voor webtoepassingen wordt niet ondersteund met load balancers voor hardware waarop passieve cookies worden gebruikt.

Als de load balancer voor hardware SSL-gecodeerde HTTPS-aanvragen naar uw containerserver voor webtoepassingen verzendt, moet u HTTPS configureren op de containerserver voor webtoepassingen, en SSL-certificaten installeren op elke containerserver voor webtoepassingen.

Als de load balancer voor hardware HTTPS-verkeer decodeert en de gedecodeerde HTTP-aanvragen doorstuurt naar uw containerserver voor webtoepassingen, is geen extra configuratie van de containerserver voor webtoepassingen vereist.

Verwante informatie

HTTPS/SSL configureren [pagina 517]

13.1.9.3 Containerservers voor webtoepassingen gebruiken met een omgekeerde proxy

U kunt containerservers voor webtoepassingen gebruiken in een omgeving met een proxyserver of omgekeerde proxyserver. U kunt niet de containerserver voor webtoepassingen zelf als proxyserver gebruiken.

13.1.9.3.1 Containerserver voor webtoepassingen instellen voor ondersteuning van HTTP met omgekeerde proxy

Als u de containerserver voor webtoepassingen wilt gebruiken in een implementatie met een omgekeerde proxy, stelt u de server zodanig in dat de HTTP-poort wordt gebruikt voor communicatie binnen een firewall (bijvoorbeeld in een beveiligd netwerk), en de HTTP via proxy-poort voor communicatie van buiten de firewall (bijvoorbeeld vanaf het internet).

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de containerserver voor webtoepassingen die u wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.
3. In het gedeelte *HTTP via proxy configureren* doet u het volgende:

a. Schakel het selectievakje *HTTP via proxy inschakelen* in.
b. Geef de HTTP-poort van de containerserver voor webtoepassingen op die voor de communicatie via proxy wordt gebruikt.
c. Geef de proxy-hostnaam en proxy-poort van de proxy op.

4. Klik op *Opslaan en sluiten*.

13.1.9.3.2 Containerserver voor webtoepassingen instellen voor ondersteuning van HTTPS met omgekeerde proxy

U kunt bepaalde load balancers en omgekeerde proxy's instellen voor decodering van HTTPS-verkeer en het doorsturen van dit gedecodeerde verkeer naar uw toepassingsservers. In dat geval configureert u de containerserver voor webtoepassingen voor gebruik van HTTP of HTTP via proxy.

Als uw load balancer of omgekeerde proxy het HTTPS-verkeer doorstuurt en u HTTPS met een omgekeerde proxy wilt configureren, maakt u twee containerservers voor webtoepassingen. Configureer de eerste containerserver voor webtoepassingen voor extern verkeer via de omgekerde proxy en configureer de tweede server voor communicatie met clients in uw interne netwerk via HTTPS.

13.1.9.4 Containerserver voor webtoepassingen gebruiken met firewalls

Implementatie van containerservers voor webtoepassingen in een IT-omgeving met firewalls wordt ondersteund.

Een containerserver voor webtoepassingen wordt standaard gebonden aan alle IP-adressen op de computer waarop de server is geïnstalleerd. Als u een firewall wilt gebruiken tussen uw clients en uw containerserver voor webtoepassingen, moet u de containerserver voor webtoepassingen dwingen te binden aan een bepaald IP-adres voor HTTP of HTTP via proxy. Schakel hiertoe het selectievakje *Binden aan alle IP-adressen* uit en typ een IP-adres of hostnaam waarmee de containerserver voor webtoepassingen kan binden.

Als u een firewall wilt gebruiken tussen een WACS-server en de andere servers van BI-platform in uw implementatie, raadpleegt u de sectie “Communicatie tussen BI-platformonderdelen ” van de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform*.

Verwante informatie

Communicatie tussen BI-platformonderdelen begrijpen [pagina 191]

13.1.9.5 WACS configureren op een multihomed-computer

Een multihomed-computer is een computer met meerdere netwerkadressen. Een exemplaar van een containerserver voor webtoepassingen bindt de HTTP-poort standaard aan alle IP-adressen. Als u een containerserver voor webtoepassingen wilt binden aan een specifieke netwerkinterfacekaart, bijvoorbeeld wanneer u de HTTP-poort van de server wilt binden aan een netwerkinterfacekaart en de aanvraagpoort wilt binden aan een andere netwerkinterfacekaart:

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de containerserver voor webtoepassingen die u wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel in de sectie *Configuratie van HTTP via proxy* van het deelvenster *Containerservice voor webtoepassingen* het selectievakje *Aan alle IP-adressen binden* uit en typ een IP-adres waarmee de containerserver voor webtoepassingen kan binden.
4. Schakel in de sectie *HTTP-configuratie* het selectievakje *Aan alle IP-adressen binden* uit en typ een IP-adres of hostnaam waarmee de containerserver voor webtoepassingen kan binden.
5. Schakel onder *Algemene instellingen* het selectievakje *Automatisch toewijzen* uit en geef de hostnaam of het IP-adres op van de netwerkinterfacekaart die wordt gebruikt voor de communicatie tussen de containerservers voor webtoepassingen en de andere BI-platformservers in uw implementatie.
6. Klik op *Opslaan en sluiten*.
7. Start de containerserver voor webtoepassingen opnieuw.

13.1.10 Eigenschappen van webtoepassing configureren

De eigenschappen van webtoepassingen die op een WACS worden gehost kunnen op de volgende manieren worden geconfigureerd:

- Eigenschappen die vaak worden gewijzigd worden aangeduid als configureerbare service-eigenschappen voor de WACS. Als u deze eigenschappen wilt bewerken, opent u de pagina *Eigenschappen* van de WACS in de CMC (Central Management Console, wijzigt u de waarde voor de desbetreffende eigenschap en klikt u op *Opslaan*.
- Als u de sessietime-outs voor webtoepassingen die op WACS worden gehost wilt wijzigen, bepaalt u eerst of de webtoepassing over eigenschappen beschikt die in de CMC kunnen worden geconfigureerd.
  Indien de webtoepassing over eigenschappen beschikt die in de CMC kunnen worden gewijzigd, wijzigt u het bestand `web_xml.ino` voor de webtoepassing. Het bestand is `<Webtoepassingsnaam>_web_xml.ino`, waarbij `<Webtoepassingsnaam>` voor de naam van de webtoepassing staat. Dit kan worden gevonden in de map `<Enterprisemap>/java/pjs/services/<Webtoepassingsnaam>`.
  Indien de webtoepassing niet over eigenschappen beschikt die in de CMC kunnen worden gewijzigd, wijzigt u het bestand `web.xml` voor de webtoepassing. Dit bestand kan worden gevonden in de `<Enterprisemap>/warfile/webapps/<Webtoepassingsnaam>`, waarbij `<Webtoepassingsnaam>` de naam is van de webtoepassing.
- Als u andere eigenschappen wilt wijzigen dan de sessietime-out of de eigenschappen die worden aangeduid in het venster *Eigenschappen* voor de WACS in de CMC, wijzigt u het bestand `.properties` voor de webtoepassing. Raadpleeg de sectie “Toepassingen beheren via BOE.war-eigenschappen” van de *Beheerdershandleiding voor SAP BI-platform*.

> **Opmerking**
>
> Breng geen wijzigingen aan in de bestanden `web.xml`, `web_xml.ino` of `.properties` in de map `<Enterprisemap>/java/pjs/container/work/<ServerFriendly_naam>`, omdat uw wijzigingen telkens zullen worden overschreven als de WACS wordt gestart of opnieuw gestart.

> **Opmerking**
>
> Na het wijzigen van de eigenschappen voor een WACS moet u deze altijd opnieuw opstarten.

Verwante informatie

De eigenschappen van een server wijzigen [pagina 454]
Het BOE.war-bestand [pagina 754]

13.1.11 Problemen oplossen

13.1.11.1 Tracering op WACS configureren

Raadpleeg Tracering voor onderdelen registreren [pagina 1069] om tracering op WACS te configureren

13.1.11.2 Servergegevens weergeven

U kunt de servergegevens van een WACS weergeven in de CMC (Central Management Console).

1. Ga naar het beheergebied *Servers* van de CMC.
2. Klik met de rechtermuisknop op de containerserver voor webtoepassingen en klik op *Gegevens*.

Verwante informatie

Gegevens van containerserver voor webtoepassingen [pagina 1205]

13.1.11.3 De status van een containerserver voor webtoepassingen weergeven

Als u de status van een containerserver voor webtoepassingen wilt weergeven, gaat u naar het beheergebied *Servers* van de CMC. De *Serverlijst* bevat de kolom *Status* met de status van elke server in de lijst.

Voor containerservers voor webtoepassingen is er de status “Wordt uitgevoerd met fouten”. Deze status betekent dat de containerserver voor webtoepassingen actief is, maar een of meer van de volgende fouten heeft:

- Een HTTP-, HTTP via proxy- of HTTPS-connector is niet goed geconfigureerd.
- Een service die actief is op een containerserver voor webtoepassingen, zoals de traceerlogboekservice, wordt niet goed uitgevoerd.
- Een webtoepassing is niet geïmplementeerd op een containerserver voor webtoepassingen.

Op de pagina *Eigenschappen* van de containerserver voor webtoepassingen kunt u zien welke services zijn mislukt.

13.1.11.4 Poortconflicten oplossen

Als u geen pagina's kunt weergeven wanneer u via een bepaalde poort toegang tot de CMC probeert te krijgen, moet u controleren of de HTTP-, HTTP via proxy- of HTTPS-poort die u voor de containerserver voor webtoepassingen hebt opgegeven niet is overgenomen door een andere toepassing.

Er zijn twee manieren waarop u kunt bepalen of er poortconflicten zijn met uw containerserver voor webtoepassingen. Als u meer dan één containerserver voor webtoepassingen in uw implementatie hebt, meldt u zich aan bij de CMC en controleert u de lijst met actieve serverconnectors en serveropstartfouten. Als de HTTP-, HTTP via proxy- of HTTPS-connectors niet in de lijst met actieve serverconnectors staan, kunnen deze connectors niet worden gestart vanwege een poortconflict.

Als in uw implementatie slechts één containerserver voor webtoepassingen is geïnstalleerd, of als u niet via een containerserver voor webtoepassingen toegang krijgt tot de CMC, moet u met behulp van een programma als Netstat bepalen of de serverpoort door een andere toepassing wordt gebruikt.

13.1.11.4.1 Conflicten met HTTP-poorten oplossen

1. Start de CCM (Central Configuration Manager) en klik op het pictogram *Servers beheren*.
2. Geef de aanmeldingsreferenties op.
3. Stop de containerserver voor webtoepassingen in het scherm *Servers beheren*.
4. Klik op het pictogram *Configuratie van weblaag*.

   > **Opmerking**
   >
   > Het pictogram *Configuratie van weblaag* is alleen beschikbaar als u een containerserver voor webtoepassingen selecteert die is gestopt.

   Het scherm *Configuratie weblaag* verschijnt.
5. Typ in het vak *HTTP Port* een vrije HTTP-poort die kan worden gebruikt door de containerserver voor webtoepassingen en klik op *OK*.
6. Start de containerserver voor webtoepassingen in het scherm *Servers beheren*.

13.1.11.4.2 Conflicten met HTTP via proxy- of HTTPS-poorten oplossen

Als u geen toegang kunt krijgen tot een containerserver voor webtoepassingen via de HTTP via proxy- of HTTPS-poort, maar wel verbinding kunt maken met de CMC (Central Management Console) via de HTTP-poort, kunt u de poortnummers in de CMC wijzigen.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Stop de containerserver voor webtoepassingen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server stoppen*.
3. Dubbelklik op de containerserver voor webtoepassingen die u wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.
4. Geef een nieuwe HTTP-poort op in het gedeelte *HTTP via proxy configureren*.
5. Als u de HTTPS-poort wilt wijzigen, typt u in het gedeelte *HTTPS configureren* een nieuwe waarde in het vak *HTTPS-poort*.
6. Klik op *Opslaan en sluiten*.
7. Start de containerserver voor webtoepassingen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server starten*.

13.1.11.5 Geheugeninstellingen wijzigen

Als u de serverprestaties van een containerserver voor webtoepassingen wilt verbeteren, kunt u in de CCM (Central Configuration Manager) de hoeveelheid geheugen wijzigen dat aan de server is toegewezen.

1. Start de CCM en klik op het pictogram *Servers beheren*.
2. Geef de aanmeldingsreferenties voor de CMC (Central Management Console) op.
3. Stop de containerserver voor webtoepassingen in het scherm *Servers beheren*.
4. Klik op het pictogram *Configuratie van weblaag*.

   > **Opmerking**
   >
   > Het pictogram *Configuratie van weblaag* is alleen beschikbaar als u een containerserver voor webtoepassingen selecteert die is gestopt.

   Het scherm *Configuratie weblaag* verschijnt.
5. Geef onder *Opdrachtregelparameters* een nieuwe waarde voor het geheugen op door de opdrachtregel te bewerken:
   a. Ga naar de parameter `-Xmx`. Meestal is voor deze parameter een waarde opgegeven.
      Bijvoorbeeld "-Xmx1g". Hiermee wordt 1 GB geheugen aan de server toegewezen.
   b. Geef een andere waarde op voor de parameter.
      - Typ een "m" als u een waarde in MB wilt opgeven. Met de parameter "**`-Xmx640m`**" bijvoorbeeld wijst u 640 MB geheugen toe aan de containerserver voor webtoepassingen.
      - Typ een "g" als u een waarde in GB wilt opgeven. Met de parameter "**`-Xmx2g`**" bijvoorbeeld wijst u 2 GB geheugen toe aan de containerserver voor webtoepassingen.

c. Klik op *OK*.

6. Start de containerserver voor webtoepassingen in het scherm *Servers beheren*.

13.1.11.6 Het aantal gelijktijdige aanvragen wijzigen

Het aantal gelijktijdige HTTP-aanvragen dat wordt geconfigureerd voor verwerking op de containerserver voor webtoepassingen, is standaard 150. Voor de meeste implementaties is dit een werkbaar aantal. Als u de prestaties van de containerserver voor webtoepassingen wilt verbeteren, kunt u het maximum aantal gelijktijdige HTTP-aanvragen verhogen. Hoewel een groter aantal gelijktijdige aanvragen de prestaties kan verhogen, kan een te hoge waarde de prestaties weer nadelig beïnvloeden. De ideale instelling is afhankelijk van uw hardware, software en IT-vereisten.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Stop de containerserver voor webtoepassingen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server stoppen*.
3. Dubbelklik op de containerserver voor webtoepassingen die u wilt configureren.
   Het scherm *Eigenschappen* wordt weergegeven.
4. Typ onder *Instellingen voor gelijktijdigheid (per connector)* in het veld *Maximumaantal gelijktijdige aanvragen* het gewenste aantal gelijktijdige aanvragen en klik op *Opslaan en sluiten*.
5. Start de containerserver voor webtoepassingen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server starten*.

13.1.11.7 Standaardwaarden herstellen

Als de configuratie van een containerserver voor webtoepassingen mislukt, kunt u de standaardwaarden in de CCM (Central Configuration Manager) herstellen.

1. Start de CCM en klik op het pictogram *Servers beheren*.
2. Geef de aanmeldingsreferenties op.
3. Stop de containerserver voor webtoepassingen in het scherm *Servers beheren*.
4. Klik op het pictogram *Configuratie van weblaag*.

   > **Opmerking**
   >
   > Het pictogram *Configuratie van weblaag* is alleen beschikbaar als u een containerserver voor webtoepassingen selecteert die is gestopt.

   Het scherm *Configuratie weblaag* verschijnt.
5. Klik op *Standaardwaarden herstellen*.
6. Geef indien nodig een vrije HTTP-poort op en klik op *OK*.
7. Start de containerserver voor webtoepassingen in het scherm *Servers beheren*.

13.1.11.8 Voorkomen dat gebruikers verbinding maken met containerservers voor webtoepassingen via HTTP

Soms wilt u alleen gebruikers van de lokale computer toegang geven tot een containerserver voor webtoepassingen via HTTP of HTTPS. Hoewel u de HTTP-poort niet kunt sluiten, kunt u wel uw containerserver voor webtoepassingen zodanig configureren dat daarop alleen HTTP-aanvragen worden geaccepteerd van clients die op dezelfde computer zijn geïnstalleerd als de containerserver voor webtoepassingen. Op deze manier kunt u onderhouds- of configuratietaken uitvoeren op een containerserver voor webtoepassingen via een browser op dezelfde computer als waarop de containerserver voor webtoepassingen is geïnstalleerd, terwijl u voorkomt dat andere gebruikers toegang hebben tot de server.

1. Ga naar het beheergebied *Servers* van de CMC.
2. Dubbelklik op de containerserver voor webtoepassingen die u wilt wijzigen.
   Het scherm *Eigenschappen* wordt weergegeven.
3. Schakel in de sectie *Containerservice voor webtoepassingen* het selectievakje *Aan alle IP-adressen* uit.
4. Typ in het veld *Aan hostnaam of IP-adres binden* het nummer **`127.0.0.1`** en klik op *Opslaan en sluiten*.
5. Start de containerserver voor webtoepassingen door met de rechtermuisknop op de server te klikken en vervolgens te klikken op *Server starten*.
   De containerserver voor webtoepassingen die zo is ingesteld, accepteert alleen verbindingen vanaf de lokale computer.

13.1.12 Eigenschappen van containerserver voor webtoepassingen

Zie de sectie “Instellingen kernserver” in de bijlage “Servereigenschappen” voor een compleet overzicht van de algemene, HTTP-, HTTP via Proxy- en HTTPS-configuratie-eigenschappen die voor WACS kunnen worden geconfigureerd.

Verwante informatie

Eigenschappen van kernservices [pagina 1159]

14 Back-ups van uw systeem maken en het systeem herstellen

14.1 Overzicht van back-up en herstel

In dit hoofdstuk wordt uitgelegd hoe u een back-up maakt van het BI-platform en hoe u het systeem herstelt na een hardware- of softwarefout of gegevensverlies. Om een herstel- en back-upplan uit te voeren hebt u ondersteuning nodig van een ervaren SAP BusinessObjects-professional, systeembeheerder en databasebeheerder.

Verwante informatie

Een back-up maken van het volledige systeem [pagina 554]
Een back-up maken van BI-inhoud [pagina 560]
Back-ups maken van serverinstellingen in de CCM in Windows [pagina 558]
Een back-up maken van serverinstellingen op een Unix-systeem [pagina 558]
Overzicht van systeemkopieën [pagina 575]

14.2 Terminologie

Begrip	Definitie
Gegevensherhaling	Bij gegevensherhaling worden een of meer kopieën van uw gegevens gemaakt. De kopieën worden in real time bijgewerkt, bijvoorbeeld bij het gebruik van schijfkopieën. Replicatie biedt realtime-gegevensbeveiliging tegen fysieke gegevensschade, maar omdat de stations voortdurend worden bijgewerkt, kunt u uw systeem niet naar een eerdere staat herstellen als gegevens beschadigd raken of per ongeluk worden verwijderd.
Versiebeheer	Bij versiebeheer worden er meerdere versies gemaakt van een of meer specifieke bestanden op uw systeem. In dit geval kunt u uw systeem wel laten terugkeren naar een eerdere staat. Alle gegevensversies worden doorgaans op hetzelfde hostsysteem opgeslagen. Als dit systeem wordt aangetast of beschadigd, loopt u het risico dat u zowel de huidige versie als de oudere versies kwijtraakt. Functies voor het ongedaan maken van verwijderingen bewaren kopieën van 'verwijderde' bestanden zodat deze later hersteld kunnen worden, maar ook deze worden vaak op hetzelfde hostsysteem als de originele gegevens opgeslagen. Er wordt geen bescherming geboden tegen fysieke gegevensschade (zoals schijffouten).

Begrip	Definitie
Bare-metalsysteemback-up	Een bare-metalback-up van een systeem is een back-up van het volledige bestandssysteem, inclusief het besturingssysteem. Een bare-metalback-up van een systeem is bedoeld om een systeemback-up te herstellen naar hardware die geen software of besturingssysteem bevat. Voor bare-metalsysteemback-ups wordt bij een fout het volledige bestandssysteem (inclusief het besturingssysteem) hersteld naar identieke hardware, of, als uw herstelprogramma's hardwareonafhankelijk herstel ondersteunen, naar andere hardware.
Bare-metalsysteemback-up vs. toepassingsback-up	Een bare-metalback-up van een systeem maakt een kopie van het volledige bestandssysteem, inclusief het besturingssysteem. Zo kunt u terugkeren naar een eerdere versie van het gehele systeem. Bij een toepassingsback-up wordt een back-up gemaakt van bestanden van afzonderlijke toepassingen. Het BI-platform ondersteunt bare-metalback-ups van het systeem maar niet toepassingsback-ups. Voor bare-metalsysteemback-ups wordt bij een fout het volledige bestandssysteem (inclusief het besturingssysteem) hersteld naar identieke hardware, of, als uw herstelprogramma's hardwareonafhankelijk herstel ondersteunen, naar andere hardware. Een back-up van een volledig BI-platformsysteem wordt een back-upset genoemd.
Back-upset	Een back-upset bestaat uit de volgende afzonderlijke back-ups, die tegelijk gemaakt zijn: • Een back-up van de CMS-systeemdatabase • Een bare-metalback-up van het volledige bestandssysteem, waaronder het besturingssysteem, van alle computers in de BI-platformimplementatie • Een back-up van de invoer-FRS- en uitvoer-FRS-bestandsopslag (indien niet opgenomen in het BI-platformbestandssysteem) • Een back-up van de weblaagonderdelen (indien niet opgenomen als deel van het BI-platformbestandssysteem) • Een back-up van de controledatabase
Statische vs. dynamische back-up	Een statische back-up wordt uitgevoerd terwijl het systeem is stopgezet en niet beschikbaar is voor gebruikers. Tijdens een dynamische back-up is het systeem actief en beschikbaar voor gebruikers, waardoor gegevens kunnen veranderen terwijl de back-up wordt uitgevoerd. Bij het uitvoeren van een dynamische back-up moet u de back-upstappen in de juiste volgorde uitvoeren, wat bij een statische back-up niet nodig is. Het BI-platform ondersteunt zowel statische als dynamische back-ups. Dynamische back-ups worden soms “onlineback-ups” genoemd.

14.3 Cases gebruiken voor back-up en herstel

In de volgende tabel worden de doelen beschreven die u wilt verwezenlijken met de resources waarover u mogelijk beschikt, en wordt de meest toepasselijke back-upoplossing geboden.

Doelstelling	Vereiste resources	Oplossing
Doel: een systeem herstellen 1. Mijn BI-platformsysteem is beschadigd. Ik moet het systeem dus herstellen naar de staat voordat de laatste back-up is uitgevoerd. 2. Een computer die als host van het BI-platform fungeert, is beschadigd. Ik moet de computer vervangen door een nieuwe computer.	• Een doelsysteem met identieke hardware op het bronsysteem AND • Back-ups van het bronsysteem	Gebruik de werkstroom voor systeemback-up en herstel die in deze handleiding wordt beschreven. Zie de procedure Een back-up maken van het volledige systeem [pagina 554]. Maak het doelsysteem op basis van de back-ups van het bronsysteem.
Doel: objecten herstellen Ik wil een document of ander object herstellen dat per ongeluk is verwijderd.	• Back-ups van de databases en bestanden op het bronsysteem AND • Uitgebreide systeeminformatie in Exporteren vanaf een bronsysteem [pagina 579]	Maak met behulp van back-ups een kopie van het systeem op een andere computer en volg hierbij de werkstroom Systeemkopie in het hoofdstuk "Uw BI-platformimplementatie kopiëren". Gebruik vervolgens de hulpprogramma's voor Promotiebeheer om de objecten die per ongeluk van dat nieuwe systeem zijn verwijderd, te promoten. Zie de werkstroom Systeemkopie vanaf Voorbereiding op het kopiëren van uw systeem [pagina 576], en voer de instructies in de rest van dat hoofdstuk uit. **Opmerking** U kunt uw doelsysteem maken op een computer met een bestaande BI-platformimplementatie met dezelfde versie, hetzelfde ondersteuningspakket en hetzelfde patchniveau, of op een "schone" computer waarop BI-platform niet is geïnstalleerd.
Doel: objecten herstellen 2 Ik wil een document of ander object herstellen dat per ongeluk is verwijderd.	Een systeem waarop versiebeheer voor Promotiebeheer wordt gebruikt	Gebruik de toepassing Promotiebeheer om een eerdere versie van het document te herstellen. Zie het verwante onderwerp over Promotiebeheer voor meer informatie.

Opmerking

Een back-up van het systeem maken voor en na een software-upgrade:

CMS is gekoppeld aan de 'versie' van een product. U kunt het SAP BusinessObjects Business Intelligence-platformsysteem niet gebruiken met CMS en FRS van een andere versie. U moet altijd een back-up maken van zowel CMS als FRS-bestandsopslag, voor en na elke software-upgrade. Als u met 'herstellen' een

software-upgrade terugzet, moet u ervoor zorgen dat CMS, FRS en de software alle tot dezelfde versie behoren.

Verwante informatie

Back-ups [pagina 553]
Voorbereiding op het kopiëren van uw systeem [pagina 576]
Overzicht [pagina 587]

14.4 Back-ups

Een herstel- en back-upplan bestaat uit de voorzorgsmaatregelen die getroffen moeten worden in geval van een systeemfout door een natuurramp of onverwachte fout. Het plan beoogt de impact van de ramp op dagelijkse bewerkingen te beperken zodat u kritieke functies kunt behouden of snel kunt hervatten.

U beschikt over drie opties wanneer u een back-up van uw BI-platform maakt:

- U kunt een back-up van het volledige systeem maken, zodat u het volledige systeem kunt herstellen. Het is in dit geval niet mogelijk alleen een deel van het systeem te herstellen. Als u het BI-platform opnieuw wilt bouwen en niet wilt herstellen via een back-up, raadpleegt u het verwante onderwerp over systeemkopieën.
- U kunt een back-up van de serverinstellingen maken, zodat u alleen de serverinstellingen kunt herstellen zonder andere objecten te herstellen. Hiermee blijft de huidige staat van de BI-inhoud op uw systeem behouden.
- U kunt een back-up van BI-inhoud maken, bijvoorbeeld documenten. U kunt dan delen van BI-inhoud selecteren om te herstellen zonder alle objecten te moeten herstellen.

Zie de verwante onderwerpen voor informatie over alle drie back-uptypen.

→ Tip

Voer geregeld back-ups uit om gegevensverlies te voorkomen.

→ Tip

U kunt een back-up maken van een BI-platformsysteem en dit vervolgens herstellen naar dezelfde of een andere hostcomputer om een kopie van het systeem te maken.

Verwante informatie

Een back-up maken van het volledige systeem [pagina 554]
Back-up maken van serverinstellingen [pagina 557]
Een back-up maken van BI-inhoud [pagina 560]

Overzicht van systeemkopieën [pagina 575]

14.4.1 Een back-up maken van het volledige systeem

Maak een back-up van het volledige BI-platformsysteem door een statische of dynamische back-up uit te voeren, waarmee een back-upset wordt gemaakt. Als u meerdere back-upsets van verschillende tijdstippen bewaart, beschikt u over meer mogelijkheden wanneer u het systeem herstelt. Maak zo vaak een back-up van uw systeem als uw bedrijfsbehoeften vereisen.

U kunt uw BI-platformsysteem stoppen en een statische back-up maken, of u kunt een dynamische back-up uitvoeren. Bij een dynamische back-up blijft het systeem actief en tijdens het back-upproces beschikbaar voor gebruikers. Het voordeel hiervan is geen downtime van uw systeem.

> **Opmerking**
>
> Het is raadzaam het transactielogboek naar een ander systeem te schrijven dan het serversysteem van de hoofddatabase, geregeld een back-up te maken van dit transactielogboek en het bij de andere bestanden van de back-upset te bewaren.

> **Opmerking**
>
> Als u een back-up maakt van controlegegevens, moet u het transactielogboek van de database voor de controledatabase opnemen bij de bestandsset van uw back-up. U hoeft de tijdelijke bestanden van de controle niet bij de back-up op te nemen.

14.4.1.1 Dynamische back-ups

Met de functie voor dynamische back-ups kunt u een back-up maken van uw BI-platformsysteem terwijl andere gebruikers het systeem kunnen blijven gebruiken. Als uw bedrijfsactiviteiten niet moeten worden onderbroken wanneer een systeemback-up wordt gemaakt, schakelt u dynamische back-ups in en configureert u deze in de Central Management Console.

Met de instelling *Maximumduur van dynamische back-up* geeft u de verwachte maximumduur van de back-up op (vanaf het moment dat de CMS-back-up begint tot het moment dat de FRS-back-up eindigt). Als de opgegeven duur te kort is, kunnen er bestanden worden verwijderd voordat de back-up de kans heeft gekregen om ze te kopiëren. Het is dus veiliger om de benodigde tijd hoger in te schatten. U moet dit bezwaar afwegen tegen het gebruik van systeembronnen, omdat een hoge waarde uw FRS-bestandsopslag enigszins kan vergroten.

> **Opmerking**
>
> - Dynamische back-up voert geen werkelijke back-up uit, maar vertraagt slechts het verwijderen van bestanden. Als bestanden worden bewerkt of geactualiseerd, worden meerdere kopieën bewaard. Dit betekent dat de CMS en de FRS altijd de correcte relaties behouden, zodat een back-up van beide servers apart van elkeaar op verschillende momenten mogelijk is. Dit gebeurt echter binnen het venster van de dynamische back-up.

- Als u het systeem herstelt, heeft u veel extra bestanden in de FRS die moeten worden verwijderd door het diagnostisch hulpprogramma voor gegevensopslagruimte.
- Voer de back-up van CMS altijd uit vóórdat u een back-up van de FRS-bestandsopslag uitvoert.

Dynamische back-up is geactiveerd zolang het selectievakje *Dynamische back-up inschakelen* is ingeschakeld in de CMC; de instelling *Maximumduur van dynamische back-up* bepaalt niet of dynamische back-up is ingeschakeld of niet.

Het is het gemakkelijkst om uw systeem naar een specifieke back-uptijd te herstellen. Als uw systeemback-ups bijvoorbeeld dagelijks om 3 uur 's nachts worden uitgevoerd, kunt u het systeem gemakkelijk herstellen naar de staat van toen de back-up van het CMS-systeem werd gestart (3 uur 's nachts op de gewenste datum). Als u transactielogboeken hebt ingeschakeld voor de CMS-database of controledatabase, kunt u bij een fout in een CMS-database of controledatabase ook het systeem herstellen naar de staat vlak voor de fout.

Voor een optimale veiligheid moet u de records van transactielogboeken op een andere locatie opslaan dan uw primaire records van databaseback-ups. Hiermee zorgt u dat u de database kunt herstellen naar de staat van de database voordat er een fout optrad.

ⓘ Opmerking

Vanwege een beperking op de grootte van het transactielogboek in oudere versies van IBM DB2, worden dynamische back-ups en taken met betrekking tot het transactielogboek alleen ondersteund als de CMS-systeemdatabase wordt gehost op DB2-databaseserverversie 9.5 Fix Pack 5 of nieuwer (voor de 9.5-reeks) en 9.7 Fix Pack 1 of nieuwer (voor de 9.7-reeks).

ⓘ Opmerking

Het is raadzaam het transactielogboek naar een ander systeem te schrijven dan het serversysteem van de hoofddatabase, geregeld een back-up te maken van dit transactielogboek en het bij andere bestanden van de back-upset te bewaren.

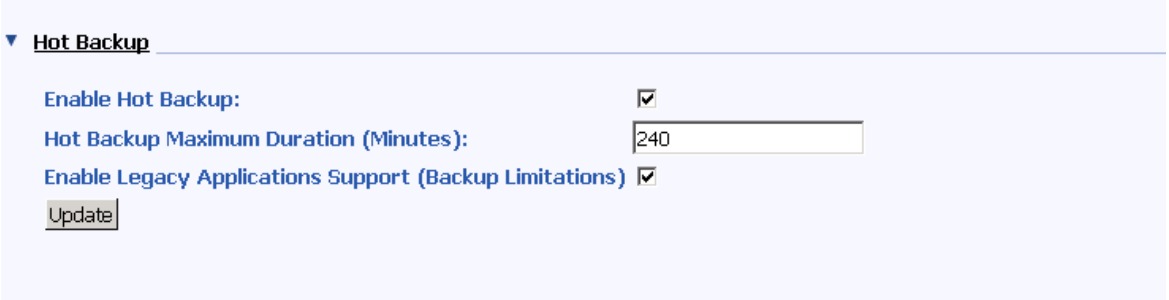
14.4.1.1.1 Dynamische back-up inschakelen

1. Open de CMC (Central Management Console).
2. Ga naar het gebied *Beheren* en open de pagina *Instellingen*.
3. In het gebied *Dynamische back-up* selecteert u *Dynamische back-up inschakelen*.
4. Voer onder *Maximumduur van dynamische back-up (minuten)* het maximumaantal minuten in voor de verwachte duur van de back-up.

   Zorg dat u hierbij de tijd rekent die benodigd is om een back-up te maken van de CMS-database en het bestandssysteem van de hostcomputer met het BI-platform.

   ⓘ Opmerking

   Als de eigenlijke duur van de back-up langer is dan de limiet die u hier hebt ingevoerd, kan dit inconsistenties in de back-upgegevens veroorzaken. Het is dus veiliger om de benodigde tijd hoger in te schatten.
5. Klik op *Bijwerken*.
   Dynamische back-up is ingeschakeld.



Zodra dynamische back-up is ingeschakeld, kunt u back-ups uitvoeren met uw hulpprogramma's voor database- en bestandssysteemback-ups.

14.4.1.2 Een dynamische of statische systeemback-up uitvoeren

Als u een dynamische back-up wilt uitvoeren, raadpleegt u eerst het verwante onderwerp over dynamische back-ups voor vereisten en meer informatie. Als u een statische back-up uitvoert, stopt u alle knooppunten in uw BI-platformimplementatie.

> **⚠ Let op**
>
> Als u een back-up uitvoert zonder dynamische back-up in te schakelen en zonder alle knooppunten te stoppen, kunnen er gegevensinconsistenties optreden tussen de CMS-database en de FRS-bestandsopslag.

> **ⓘ Opmerking**
>
> Voor dynamische back-ups is het belangrijk dat de procedures in de beschreven volgorde worden gestart. Voor statische back-ups kunnen de procedures in willekeurige volgorde worden uitgevoerd. In beide gevallen hoeft u niet te wachten tot elke back-up is voltooid alvorens de volgende stap te starten.

1. Gebruik de hulpprogramma's van uw databaseleverancier om een back-up van de CMS-systeemdatabase (Central Management Server) te maken.

   > **ⓘ Opmerking**
   >
   > Voor dynamische back-ups gebruikt u de hulpprogramma's voor back-up van uw databaseleverancier in de online atomische modus.

2. Gebruik de hulpprogramma's van uw databaseleverancier in de online atomische modus om een back-up te maken van de controledatabase van het BI-platform.
3. Maak een back-up van het volledige bestandssysteem, inclusief het besturingssysteem, van alle computers in de BI-platformimplementatie. Maak voor Unix-computers een back-up van de installatiemap en de hoofdmap van een installatieaccount.
   a. Als de bestandsopslag voor de FRS-invoer en -uitvoer niet is opgenomen in de back-up van het BI-platform (afzonderlijke hostcomputers), maakt u een back-upkopie van beide met uw hulpprogramma's voor bestandsback-up.

b. Als de weblaagonderdelen niet zijn opgenomen in de back-up van het BI-platform (afzonderlijke hostcomputers), maakt u een back-upkopie met uw hulpprogramma's voor bestandsback-up.

Voor dynamische back-ups gebruikt u waar mogelijk hulpprogramma's voor atomische bestandsback-up.

Als u een statische back-up hebt uitgevoerd, wacht u tot alle back-ups zijn voltooid en start u vervolgens de BI-platformknooppunten.

Verwante informatie

Dynamische back-ups [pagina 554]

14.4.2 Back-up maken van serverinstellingen

U moet regelmatig back-ups maken van uw serverinstellingen naar een BIAR-bestand om uw systeem te beschermen tegen onjuist geconfigureerde serverinstellingen. Met back-ups van uw servers kunt u de instellingen herstellen zonder uw CMS-systeemdatabase (Central Management Server), gegevensopslagruimten of Business Intelligence-inhoud te moeten herstellen.

Het is van essentieel belang dat u back-ups maakt van uw serverinstellingen wanneer u de implementatie van uw systeem wijzigt. Dit is onder andere het maken, hernoemen, verplaatsen en verwijderen van knooppunten, en het maken of verwijderen van servers. Het is raadzaam dat u back-ups maakt van uw serverinstellingen voordat u de instellingen wijzigt, en vervolgens nog een keer nadat u tevreden bent met de wijzigingen die u hebt aangebracht.

> **Opmerking**
>
> Het maken van een back-up van de serverinstellingen is geen aanvullende taak bij de back-up van CMS- en FRS-bestandsopslag, d.w.z. wanneer de CMS/FRS wordt hersteld, worden ook de serverinstellingen hersteld. Back-up van serverinstellingen is een kleine subset van een volledige back-up van de CMS-database. Als u de CMS al hebt hersteld, hoeft u de serverinstellingen niet te herstellen.

Gebruik de CCM (Central Configuration Manager) of een script om een back-up van uw serverinstellingen voor het BI-platform naar een BIAR-bestand te maken, en sla het bestand vervolgens op een aparte computer of opslagmedia op.

> **Opmerking**
>
> Als u een back-up maakt van serverinstellingen in een implementatie waarbij SSL is ingeschakeld of deze herstelt, moet u eerst SSL uitschakelen via de CCM en vervolgens weer inschakelen als de back-up of het herstellen is voltooid.

In Windows bevindt het script `BackupCluster.bat` zich in de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In Unix bevindt het script `backupcluster.sh` zich in de map `/<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

14.4.2.1 Back-ups maken van serverinstellingen in de CCM in Windows

Met deze procedure maakt u een back-up van de serverinstellingen voor een hele cluster. Het is niet mogelijk een back-up te maken van de instellingen voor individuele servers.

> **Opmerking**
>
> Als u een tijdelijke CMS gebruikt, moet u de CCM gebruiken op een computer met een lokale binaire CMS-bestanden.

1. Start de CCM en klik op de werkbalk op *Back-up maken van serverconfiguratie*.
   De *Wizard Back-up maken van serverconfiguratie* wordt weergegeven.
2. Klik op *Volgende* om de wizard te starten.
3. Geef aan of u een bestaande CMS wilt gebruiken voor de back-up van uw serverconfiguratie-instellingen of liever een tijdelijke CMS maakt.
   - Selecteer *Bestaande actieve CMS gebruiken* en klik op *Volgende* om een back-up te maken van serverinstellingen van een systeem dat actief is.
   - Selecteer *Een nieuwe tijdelijke CMS starten* en klik op *Volgende* om een back-up te maken van serverinstellingen van een systeem dat niet actief is.
4. Als u een tijdelijke CMS gebruikt, selecteert u een poortnummer waarop de CMS wordt uitgevoerd, en geeft u de databaseverbindingsgegevens op.

   Geef een ander poortnummer op dan de poortnummers die uw bestaande CMS gebruikt om het risico dat gebruikers toegang hebben tot uw systeem terwijl u uw systeem herstelt, te minimaliseren.
5. Voer de clustersleutel in en klik op *Volgende* om verder te gaan.
6. Als u hierom wordt gevraagd, meldt u zich aan bij de CMS door het systeem, de gebruikersnaam en het wachtwoord van een account met beheerdersrechten op te geven, en klikt u op *Volgende* om verder te gaan.
7. Geef de locatie en naam op van een BIAR-bestand waarnaar u een back-up wilt maken van de serverconfiguratie-instellingen, en klik op *Volgende* om verder te gaan.
   De *bevestigingspagina* geeft de gegevens weer die u hebt opgegeven.
8. Controleer of de gegevens die worden weergegeven op de *bevestigingspagina* juist zijn, en klik op *Voltooien* om verder te gaan.
   De CCM maakt een back-up van de serverconfiguratie-instellingen voor de hele cluster naar het BIAR-bestand dat u opgeeft. Details van de back-upprocedure worden naar een logbestand geschreven. De naam en het pad van het logboekbestand worden weergegeven in een dialoogvenster.
9. Als de back-up mislukt, controleert u het logboekbestand om de reden vast te stellen.
10. Klik op *OK* om de wizard af te sluiten.

14.4.2.2 Een back-up maken van serverinstellingen op een Unix-systeem

Gebruik in Unix het script `serverconfig.sh` om een back-up van de serverinstellingen van uw implementatie te maken in een BIAR-bestand.

1. Selecteer optie *5 Back-up maken van serverconfiguratie* en druk op `Enter`.

```
-----------------------------------------------------------

           SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]5
```

2. Geef aan of u een bestaande CMS wilt gebruiken voor de back-up van uw serverconfiguratie-instellingen of liever een tijdelijke CMS maakt.
   - Selecteer *existing* en druk op `Enter` om een back-up te maken van de serverinstellingen van een actief systeem.
   - Selecteer *temporary* en druk op `Enter` om een back-up te maken van de serverinstellingen van een inactief systeem of de serverinstellingen te herstellen.
3. Als u een tijdelijke CMS gebruikt om een back-up te maken van uw serverinstellingen, selecteert u in de volgende vensters een poortnummer waarop de tijdelijke CMS kan worden uitgevoerd, en de verbindingsgegevens voor de CMS-systeemdatabase.

   Geef een ander poortnummer op dan de poortnummers die uw bestaande CMS gebruikt om het risico dat gebruikers toegang hebben tot uw systeem terwijl u uw systeem herstelt, te minimaliseren.
4. Wanneer hierom wordt gevraagd, meld u zich aan bij de CMS door het systeem, de gebruikersnaam en het wachtwoord van een account met beheerdersrechten op te geven en op `Enter` te drukken.
5. Wanneer hierom wordt gevraagd, geeft u de locatie en de naam van een BIAR-bestand op waarin u een back-up van de serverconfiguratie-instellingen wilt opslaan, en drukt u op `Enter`.
   Er wordt een samenvattingspagina weergegeven met de informatie die u hebt opgegeven.
6. Controleer of de weergegeven informatie juist is en druk op `Enter` om door te gaan.
   Met het script `serverconfig.sh` wordt er een back-up gemaakt van de serverconfiguratie-instellingen van het volledige cluster, dat vervolgens wordt opgeslagen in het opgegeven BIAR-bestand. Details van de back-upprocedure worden naar een logbestand geschreven. De naam en het pad van het logboekbestand worden weergegeven.
7. Als de back-up mislukt, controleert u het logboekbestand om de reden vast te stellen.

14.4.2.3 Een back-up maken van serverinstellingen met een script

U kunt een back-up maken van de serverinstellingen in uw implementatie door het script `BackupCluster.bat` uit te voeren in Windows of het script `backupcluster.sh` uit te voeren in Unix.

In Windows bevindt het bestand `BackupCluster.bat` zich in de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In Unix bevindt het script `backupcluster.sh` zich in de map `/<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Verwante informatie

De scripts BackupCluster en RestoreCluster [pagina 571]

14.4.3 Een back-up maken van BI-inhoud

Het wordt aanbevolen dat u de standaardhulpprogramma's voor het maken van database- en bestandsback-ups gebruikt om regelmatig een back-up te maken van:

- De CMS-database.
- De invoer-FRS- en uitvoer-FRS-bestandsopslag.

Met recente back-ups van uw inhoud kunt u uw Business Intelligence herstellen zonder dat u uw volledige systeem of uw serverinstellingen hoeft te herstellen.

Zie Een dynamische of statische systeemback-up uitvoeren [pagina 556] voor meer informatie over het maken van een back-up van uw systeem.

14.5 Uw systeem herstellen

Als uw systeem beschadigd is, kunt u besluiten het hele systeem te herstellen, waarmee het BI-platform ook wordt hersteld. Afhankelijk van de staat van uw systeem is herstel van uw volledige systeem misschien niet nodig. Als het systeem goed werkt maar inhoud verloren is gegaan of is beschadigd, kunt u kiezen om alleen de Business Intelligence-inhoud te herstellen. Als de BI-inhoud geldig is maar uw platformservers een onjuiste configuratie hebben, kunt u alleen de serverinstellingen herstellen.

Deze procedure is van toepassing op herstel van dynamische en statische back-ups.

Verwante informatie

Uw volledige systeem herstellen [pagina 561]
Serverinstellingen herstellen [pagina 568]
BI-inhoud herstellen [pagina 571]

14.5.1 Uw volledige systeem herstellen

Wanneer u het volledige systeem herstelt, wordt ook het BI-platformcluster hersteld. Het is misschien ook mogelijk een gedeeltelijke herstelprocedure uit te voeren, afhankelijk van het systeemonderdeel dat een fout ondervindt.

Als een van de volgende onderdelen is beschadigd of verloren is gegaan, moet u uw volledige systeem herstellen:

- De CMS-database

  > **Opmerking**
  >
  > Als de databaseservice crasht, kunt u de service gewoon opnieuw starten, zonder het volledige systeem te herstellen.

- De FRS-bestandsopslag
- Het bestandssysteem van de computer

> **Opmerking**
>
> Voor herstel van het volledige systeem hoeft het BI-platform niet al op het doelsysteem zijn geïnstalleerd.

Als alleen de controledatabase is beschadigd of verloren is gegaan, kunt u de controledatabase herstellen zonder dat u het volledige systeem hoeft te herstellen.

Als uw weblaaginhoud is beschadigd of verloren is gegaan, kunt u de weblaaginhoud herstellen zonder dat u het volledige systeem hoeft te herstellen.

Verwante informatie

Uw volledige systeem herstellen [pagina 562]
Alleen de controledatabase herstellen [pagina 564]
Weblaaginhoud herstellen [pagina 564]
Alleen de CMS-database herstellen [pagina 564]

14.5.1.1 Uw volledige systeem herstellen

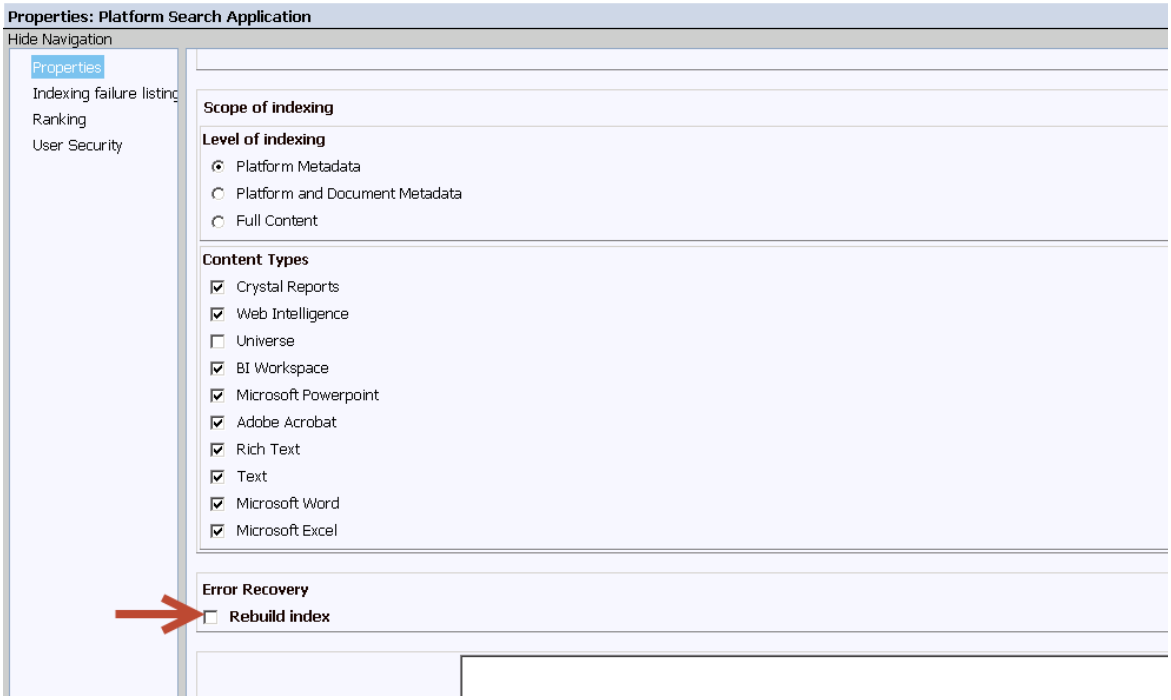
Voordat u uw systeem herstelt, moet u de CCM (Central Configuration Manager) gebruiken om alle knooppunten in uw BI-platformimplementatie te stoppen. Ook moet u besluiten naar welk tijdstip u het systeem wilt herstellen.

> **Opmerking**
>
> Als u mogelijk de huidige status van het systeem wilt herstellen, maakt u een back-up van het systeem voordat u de herstelbewerking uitvoert.

1. Zoek de volgende back-upbestanden:
   - Back-up van CMS-database
   - Back-ups van invoer-FRS- en uitvoer-FRS-bestandsopslag
   - Back-ups van bestandssystemen voor elke hostcomputer in het BI-platformcluster

   > **Opmerking**
   >
   > - Zorg dat u de back-ups valideert en dat alle bovenstaande bestanden uit dezelfde back-upset afkomstig zijn.
   > - Wanneer u een back-up en herstelactie uitvoert, worden de CMS en de FRS als één eenheid behandeld. Als u een van de twee herstelt, moet u de andere tegelijkertijd herstellen.
   > - Als de back-upset als dynamische back-up is verkregen, moet u zorgen dat de tijdstempel van de start van de CMS-databaseback-up eerder is dan de tijdstempel van de bijpassende FRS-filestore, weblaag en het bestandssysteem op de hostcomputer. Al deze bestanden zijn vereist, ook als er slechts één onderdeel een fout ondervindt.

2. Gebruik uw hulpprogramma's voor bestandsherstel om het bestandssysteem van alle hostcomputers in het BI-platformcluster te herstellen.
3. Gebruik uw hulpprogramma's voor bestandsherstel om de Input en Output FRS-bestandsopslag te herstellen.
4. Gebruik uw databasehulpprogramma's om de CMS-database te herstellen.
5. Als u het wachtwoord van de CMS-database hebt gewijzigd sinds de back-up is gemaakt, gebruikt u de CCM om het wachtwoord van de CMS-database op alle knooppunten en hostcomputers met het BI-platform bij te werken.
6. Als u de controlefunctie gebruikt, gebruikt u uw databasehulpprogramma's om de Controledatabase te herstellen.
7. Kies een van de volgende opties om uw zoekindex te herstellen:
   - Als u het herstelscript van de zoekindex wilt uitvoeren, leest u Het herstelscript voor de zoekindex uitvoeren [pagina 566] en volgt u de instructies aldaar. U krijgt dan sneller een volledige index.
   - Als u uw zoekindex sneller opnieuw wilt samenstellen in plaats van het herstelscript te gebruiken, gebruikt u de CCM om de knooppunten van uw BI-platform opnieuw te starten. Dit is een eenvoudigere procedure, maar terwijl de index opnieuw wordt samengesteld, hebt u slechts gedeeltelijke zoektoegang tot de platformgegevens.



8. Start het systeem en maak een aantekening van de tijd voor gebruik tijdens de vervolgstappen.
9. Verifieer dat uw systeem naar verwachting werkt, en voer een gezondheidscontrole uit.

Wanneer het systeem is geverifieerd, voert u de volgende handelingen uit:

- Voer het Repository Diagnostic Tool uit om ongebruikte tijdelijke bestanden te verwijderen en de consistentie van de gegevensopslagruimte te controleren. Raadpleeg de sectie Diagnostisch hulpprogramma voor gegevensopslagruimten van deze handleiding.
- Als u niet het script voor indexherstel hebt gebruikt, stelt u uw platformzoekindex opnieuw samen.
- Publicatietaken die tijdens de back-up van het systeem werden uitgevoerd, worden weergegeven als mislukt. Voer deze exemplaren niet opnieuw uit, maar start nieuwe publicatietaken.
- Als uw controledatabase is hersteld, moet u een SQL-query uitvoeren om gebeurtenissen te verwijderen die vallen tussen het tijdstip van de databasefout en de tijd waarop u de database opnieuw hebt gestart (waarvan u in stap 8 een aantekening hebt gemaakt). Bijvoorbeeld: `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

Verwante informatie

Inhoud indexeren in de CMS-gegevensopslagruimte [pagina 948]

14.5.1.2 Alleen de controledatabase herstellen

Voordat u uw controledatabase herstelt, moet u de CCM (Central Configuration Manager) gebruiken om alle knooppunten in uw BI-platformimplementatie te stoppen. U moet ook kiezen naar welk tijdstip u de database wilt herstellen.

> **Opmerking**
>
> Voer deze taak alleen uit als u zeker weet dat de controledatabase het enige beschadigde onderdeel van het BI-platform is. Als er ook andere onderdelen zijn beschadigd, moet u het volledige systeem herstellen.

Gebruik uw databasehulpprogramma's om de Controledatabase te herstellen.

Verwante informatie

Uw volledige systeem herstellen [pagina 562]

14.5.1.3 Weblaaginhoud herstellen

Voordat u uw weblaaginhoud herstelt, moet u alle knooppunten in uw BI-platformimplementatie stoppen via de CCM (Central Configuration Manager). U moet ook besluiten naar welk tijdstip u de weblaaginhoud wilt herstellen.

Voer een back-up uit als u de huidige staat van het systeem wilt kunnen herstellen.

Als de weblaag is beschadigd, kan deze afzonderlijk worden hersteld.

1. Gebruik hulpprogramma's voor bestandsherstel om de weblaagmappen op de hostcomputer met de weblaag te herstellen.
2. Gebruik de CCM om alle knooppunten voor uw BI-platformimplementatie opnieuw te starten.

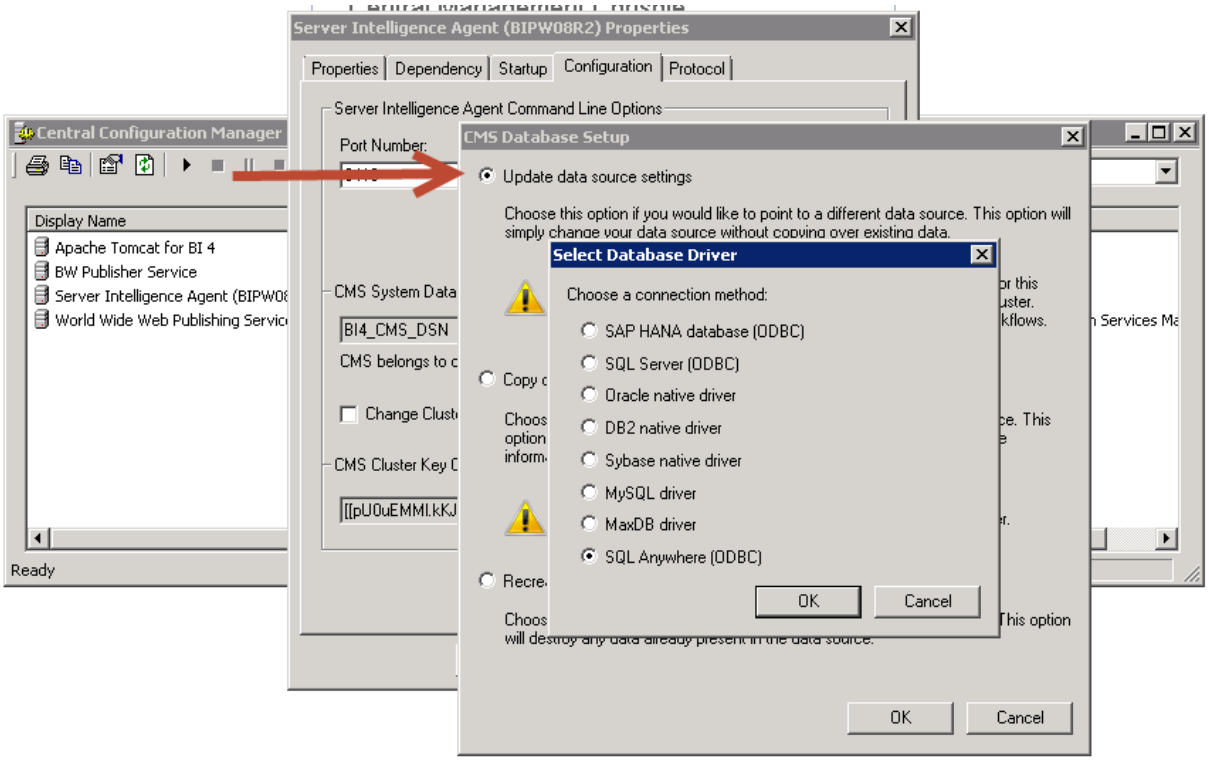
14.5.1.4 Alleen de CMS-database herstellen

> **Opmerking**
>
> Als de databaseservice crasht, kunt u de service gewoon opnieuw starten, zonder het volledige systeem te herstellen. Als de database of andere onderdelen zijn beschadigd, moet u het volledige systeem herstellen.

Herstel of vervang de hostcomputer van de CMS-database. Als u de hostcomputer vervangt, moet u zorgen dat deze dezelfde systeemnaam heeft als de vorige hostcomputer, evenals dezelfde poortinstellingen en databasereferenties.

> **Opmerking**
>
> Als u de computer niet kunt herstellen met dezelfde naam en referenties, moet u de CCM gebruiken om deze databaseverbindingsgegevens voor elk knooppunt in het cluster bij te werken, en deze knooppunten opnieuw starten.

Voor Windows:



Voor Unix: Voer cmsdbsetup.sh uit, voer de knooppuntnaam in wanneer u hierom wordt gevraagd, kies vervolgens optie 6 `update`.

```
-------------------------------------------------------

          SAP BusinessObjects


Current CMS Data Source: BI4_CMS_DSN_1381344842

Current cluster name: LRHEL57x64:6400

Current cluster key: [[pU0uEMMl.kKJPezTK002bw]]


update (Update Data Source Settings)
reinitialize (Recreate the current data surce)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)


[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-------------------------------------------------------

[update]6
```

1. Stop alle BI-platformknooppunten met de CCM.
2. Gebruik uw databasehulpprogramma's om de Controledatabase te herstellen.
3. Gebruik de CCM om de BI-platformknooppunten te starten.

Wanneer u hebt nagegaan dat het systeem goed werkt, voert u de volgende handelingen uit:

- Voer het Repository Diagnostic Tool uit om ongebruikte tijdelijke bestanden te verwijderen en de consistentie van de gegevensopslagruimte te controleren. Raadpleeg de sectie Diagnostisch hulpprogramma voor gegevensopslagruimten van deze handleiding.
- Publicatietaken die tijdens de back-up van het systeem werden uitgevoerd, worden weergegeven als mislukt. Voer deze exemplaren niet opnieuw uit, maar start nieuwe publicatietaken.

Verwante informatie

Inhoud indexeren in de CMS-gegevensopslagruimte [pagina 948]

14.5.1.5 Het zoekindexherstel

De zoekfunctie van Platform onderhoudt een reeks index- en informatiebestanden op uw systeem zodat zoekopdrachten efficiënter kunnen worden uitgevoerd. Als u het systeem moet herstellen, kunnen er inconsistenties in deze informatiebestanden optreden. U kunt deze inconsistenties verhelpen door het indexherstelscript uit te voeren of de index opnieuw samen te stellen.

Het opnieuw samenstellen van de index is een simpele procedure, maar het proces verbruikt de nodige bronnen en kost enige tijd. Bovendien retourneren zoekopdrachten die tijdens het proces worden uitgevoerd alleen resultaten voor geïndexeerde delen van de database. Het herstelscript omvat een meer gecompliceerde procedure, maar zorgt ervoor dat u sneller over een volledig functionerende index beschikt.

Als u een implementatie met meerdere computers herstelt, voert u het script uit op elke computer die de zoekservice host. Gebruik voor de eerste computer in een cluster de optie `-Both` en gebruik voor alle volgende computers in dat cluster de optie `-ContentStore`.

Verwante informatie

Inhoud indexeren in de CMS-gegevensopslagruimte [pagina 948]

14.5.1.5.1 Het herstelscript voor de zoekindex uitvoeren

- Controleer of de CMS wordt uitgevoerd en stop alle Adaptive Processing Servers (APS) die de Zoekservice hebben geïnstalleerd.

> **Opmerking**
>
> U moet deze APS's zo snel mogelijk stoppen nadat het knooppunt is gestart.

- Stel `JAVA_HOME` in op de locatie `sapjvm/bin` in de BI-platforminstallatiemap.
- De gegevensmap voor platform zoeken is toegankelijk vanaf de computer waarop het script wordt uitgevoerd.

1. Open een opdrachtregelvenster (als u Windows gebruikt) op de CMS- of APS-hostcomputer.
2. Ga naar de volgende map `<INSTALLATIEMAP>\SAP BuinsessObjects Enterprise XI 4.0\java\lib\`

   Unix-computers gebruiken het equivalente Unix-bestandspad.
3. Typ `java -jar platformSearchOnlineHotbackupRestore.jar` en druk op *Enter*.
4. Wanneer u daarom gevraagd wordt, voert u de volgende informatie in en drukt u op *Enter*:
   - De installatielocatie van uw BI-platform (bijvoorbeeld `<INSTALLATIEMAP>/SAP businessObjects Enterprise XI 4.0`)
   - Uw CMS-aanmeldingsreferenties, waaronder de CMS-naam, gebruikers-id en wachtwoord, en verificatietype. Verificatietype heeft de volgende opties:
     - `secEnterprise`
     - `secLDAP`
     - `secWinAD`
     - `secSAPR3`
5. Wanneer u wordt gevraagd om het indexhersteltype, typt u een van de volgende opties en drukt u op *Enter*.

Waarde	Beschrijving
`-Both`	Dit moet worden gebruikt voor implementatie van enkele servers, of bij implementatie van meerdere computers, voor de eerste APS-hostcomputer met de zoekservice: Gebruik op een systeem met meerdere zoek-APS's, wanneer het script de eerste keer wordt uitgevoerd, de waarde `-Both` (hiermee wordt de database- en inhoudopslag bijgewerkt). Wanneer het script voor alle andere zoek-APS's wordt uitgevoerd, gebruikt u de waarde `-ContentStore` (hiermee wordt alleen de inhoudsopslag bijgewerkt).
`-ContentStore`	Dit moet worden gebruikt wanneer het script wordt uitgevoerd op APS-hostcomputers waarop de zoekservice is geïnstalleerd, behalve als dit de eerste computer in het cluster is waarop het script wordt uitgevoerd.
`-Exit`	Sluit het script af zonder de index te herstellen.

6. Wanneer het script is uitgevoerd, sluit u het opdrachtregelvenster (voor Windows-computers).

Start alle gestopte APS's.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\java\lib>java  -jar platformsearchOnlineHotbackupRestore.jar
Enter the BOE install location :
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0

Enter the CMS Credentials:
CMS NAME: BIPW08R2
USER NAME: Administrator
PASSWORD:
AUTHENTICATION: secEnterprise
BOE Install Location = C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessOb
jects Enterprise XI 4.0 CMS = BIPW08R2  User = Administrator    Authentication =
 secEnterprise

Please verify if the details given above are correct(y/n)...Press 'e' if you wan
t to exit  :y
 What would you like to restore?
 1. Index ?
 2. Content Store ?
 3. Both Index and Content Store (Choose this option only when index and content
 store are present on one node) ?
 4. Exit ?
3
```

14.5.2 Serverinstellingen herstellen

Als u de serverinstellingen van uw systeem via een BIAR-bestand moet herstellen, kunt u de CCM (Central Configuration Manager) of de RestoreCluster-script gebruiken om de serverinstellingen te herstellen. Het herstellen van serverinhoud via een BIAR-bestand heeft geen invloed op Business Intelligence-inhoud, zoals rapporten, gebruikers en groepen of beveiligingsinstellingen.

> ⓘ Opmerking
>
> Wanneer u serverinstellingen herstelt, wordt alleen het herstel van de instellingen voor een hele cluster ondersteund. Het is niet mogelijk de instellingen te herstellen van slechts enkele servers in de cluster.

> ⓘ Opmerking
>
> Als u een back-up maakt van serverinstellingen in een implementatie waarbij SSL is ingeschakeld of deze herstelt, moet u eerst SSL uitschakelen via de CCM en vervolgens weer inschakelen als de back-up of het herstellen is voltooid.

14.5.2.1 Serverinstellingen herstellen met de CCM in Windows

U kunt de CCM (Central Configuration Manager) gebruiken om serverinstellingen te herstellen. Nadat u serverinstellingen hebt hersteld, moet u op elke computer de knooppunten van uw systeem opnieuw maken in het cluster van uw systeem.

1. Stop alle knooppunten op alle computers in het cluster waarvoor u de serverconfiguratie-instellingen wilt herstellen door Server Intelligence Agent te stoppen voor elk knooppunt.
2. Start de CCM op een computer met een CMS.

3. Klik op de werkbalk op *Serverconfiguratie herstellen*.
   De *wizard Serverconfiguratie herstellen* wordt weergegeven.
4. Klik op *Volgende* om de wizard te starten.
5. Als u hierom wordt gevraagd, geeft u het poortnummer voor de tijdelijke CMS (Central Management Server) op en de gegevens om verbinding te maken met de CMS-systeemdatabase, en klikt u op *Volgende* om verder te gaan.
6. Voer de clustersleutel in en klik op *Volgende* om verder te gaan.
7. Als u hierom wordt gevraagd, meldt u zich aan bij de CMS door de CMS-naam en de gebruikersnaam en het wachtwoord van een account met beheerdersrechten op te geven, en klikt u op *Volgende* om verder te gaan.
8. Geef de locatie en de naam op van het BIAR-bestand dat de serverconfiguratie-instellingen bevat die u wilt herstellen, en klik op *Volgende* om verder te gaan.
   Er verschijnt een overzichtspagina met de inhoud van het BIAR-bestand.
9. Klik op *Volgende* om verder te gaan.
   Er verschijnt een overzichtspagina met de informatie die u hebt opgegeven.
10. Klik op *Voltooien* om verder te gaan.
    Een waarschuwingsbericht geeft aan dat de bestaande serverinstellingen worden overschreven door de waarden in het BIAR-bestand en dat de huidige serverinstellingen verloren gaan als u verdergaat.
11. Klik op *Ja* om de serverconfiguratie-instellingen te herstellen.

    De CCM herstelt de serverconfiguratie-instellingen voor de hele cluster van het BIAR-bestand. Details van de herstelprocedure worden vastgelegd in een logboekbestand. De naam en het pad van het logboekbestand worden weergegeven in een dialoogvenster.
12. Als de herstelbewerking mislukt, controleert u het logboekbestand om de reden vast te stellen.
13. Klik op *OK* om de wizard af te sluiten.

De serverinstellingen van het BIAR-bestand worden hersteld op uw systeem. Knooppunten en servers in het BIAR-bestand die niet op het systeem bestonden voor het herstel worden gemaakt.

> **Opmerking**
>
> Knooppunten en servers die op het systeem aanwezig waren maar niet in het BIAR-bestand staan, worden uit de gegevensopslagruimte verwijderd. De knooppunten en servers worden nog altijd in de CCM weergegeven, maar u kunt de bestanden `dbinfo` en `bootstrap` voor een knooppunt handmatig verwijderen.

U moet de knooppunten van uw systeem opnieuw maken op elke computer in het cluster.

Verwante informatie

Knooppunten gebruiken [pagina 465]

14.5.2.2 De serverinstellingen herstellen op een Unix-systeem

Gebruik op Unix-computers het script `serverconfig.sh` om de serverinstellingen van uw implementatie te herstellen vanuit een BIAR-bestand.

1. Selecteer optie *6 - Serverconfiguratie herstellen* en druk op `Enter`.

```
-----------------------------------------------------------

           SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]6
```

2. Voer een poortnummer in voor de tijdelijke CMS (Central Management Server) en druk op `Enter`.
3. Geef in de volgende vensters de gegevens op van de verbinding met de CMS-systeemdatabase.
4. Wanneer hierom wordt gevraagd, meld u zich aan bij de CMS door het systeem, de gebruikersnaam en het wachtwoord van een account met beheerdersrechten op te geven en op `Enter` te drukken.
5. Wanneer hierom wordt gevraagd, geeft u de locatie en de naam op van een BIAR-bestand vanwaaruit u de serverconfiguratie-instellingen wilt herstellen en drukt u op `Enter`.
   Er wordt een samenvattingsvenster weergegeven met de informatie die u hebt opgegeven.
6. Controleer of de weergegeven informatie juist is en druk op *Enter* om door te gaan.
   Met het script `serverconfig.sh` worden de serverconfiguratie-instellingen hersteld voor het volledige cluster, dat vervolgens wordt opgeslagen in het opgegeven BIAR-bestand. Details van de herstelprocedure worden vastgelegd in een logboekbestand. De naam en het pad van het logboekbestand worden in het venster weergegeven.
7. Als de herstelbewerking mislukt, controleert u het logboekbestand om de reden vast te stellen.

14.5.2.3 Serverinstellingen herstellen met een script

Als u hier de voorkeur aan geeft, kunt u de serverinstellingen van uw implementatie herstellen door het script `RestoreCluster.bat` uit te voeren in Windos, of het script `restorecluster.sh` uit te voeren in Unix.

In Windows bevindt het script `RestoreCluster.bat` zich in de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In Unix bevindt het script `restorecluster.sh` zich in de map `/<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`.

Verwante informatie

De scripts BackupCluster en RestoreCluster [pagina 571]

14.5.3 BI-inhoud herstellen

Als u back-ups van Business Intelligence (BI)-inhoud hebt opgeslagen als LCMBIAR-bestanden, kunt u de toepassing Promotiebeheer gebruiken om BI-inhoud te herstellen zonder dat u het volledige systeem hoeft te herstellen. Raadpleeg het hoofdstuk “Promotiebeheer” voor meer informatie.

14.6 De scripts BackupCluster en RestoreCluster

In de volgende tabel worden de opdrachtregelparameters beschreven die gebruikt worden in combinatie met het script `BackupCluster`.

> ⓘ Opmerking
>
> Dit script maakt alleen een back-up van serverinstellingen voor een cluster. Van andere gegevens moet u een aparte back-up maken.

BackupCluster-parameters

Naam	Beschrijving	Voorbeeld
`-backup`	De naam en het pad van het BIAR-bestand waarin u de back-up van de systeemserverinstellingen wilt opslaan voor herstel.	`-backup "C:\Users\Administrator\Desktop\my.biar"`
`-cms`	De hostnaam van de computer waarop de CMS (Central Management Server) van uw systeem zich bevindt. Als uw CMS niet wordt uitgevoerd op de standaardpoort, 6400, moet u ook het poortnummer opgeven.	`-cms mycms:6400`
`-username`	De gebruikersnaam van een beheerdersaccount.	`-username Administrator`

Naam	Beschrijving	Voorbeeld
`-password`	Het wachtwoord van een beheerdersaccount.	`-password Password1`

In de volgende tabel worden de opdrachtregelparameters beschreven die gebruikt worden in combinatie met het `RestoreCluster`- script.

RestoreCluster-parameters

Naam	Beschrijving	Voorbeeld
`-restore`	De naam en het pad van het BIAR-bestand met de serverconfiguratie-instellingen die u wilt herstellen.	`-restore "C:\Users\Administrator\Desktop\my.biar"`
`-username`	De gebruikersnaam van een beheerdersaccount.	`-username Administrator`
`-password`	Het wachtwoord van een beheerdersaccount.	`-password Password1`
`-displaycontents`	Hiermee wordt een lijst met knooppunten en servers weergegeven die zich in het BIAR-bestand bevinden.	`-displaycontents "C:\Users\Administrator\Desktop\my.biar"`

> **Opmerking**
>
> Voer het script `RestoreCluster` uit met de parameter `-displaycontents` voor weergave van de inhoud van het BIAR-bestand, voordat u de serverinstellingen herstelt.

De volgende parameters zijn vereist als u een back-up maakt van de serverinstellingen van een inactief systeem, of als u serverinstellingen herstelt.

Parameters die gebruikt worden voor een tijdelijke CMS

Naam	Beschrijving	Voorbeeld
`-usetempcms`	Hiermee wordt een tijdelijke CMS gemaakt voor de opgegeven bewerking. Nadat de bewerking is voltooid, wordt de tijdelijke CMS gestopt.	`-usetempcms`
`-cmsport`	Het poortnummer van de tijdelijke CMS.	`-cmsport 6700`

Naam	Beschrijving	Voorbeeld
`-dbdriver`	Het stuurprogramma van de CMS-systeemdatabase. Geldige waarden zijn: • **`db2databasesubsystem`** • **`maxdbdatabasesubsystem`** • **`mysqldatabasesubsystem`** • **`oracledatabasesubsystem`** • **`sqlserverdatabasesubsystem`** • **`sybasedatabasesubsystem`** • **`sqlanywheredatabasesubsystem`** • **`newdbdatabasesubsystem`** ⓘ Opmerking De parameter **`newdbdatabasesubsystem`** is voor gebruik met SAP HANA-databases.	**`-dbdriver sqlserverdatabasesubsystem`**
`-connect`	De verbindingsreeks voor de CMS-systeemdatabase.	**`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"`**
`-dbkey`	De clustersleutel.	**`-dbkey abc1234`**

Voorbeeld

In het volgende voorbeeld wordt getoond hoe u uw back-up kunt maken van uw serverinstellingen en deze kunt opslaan in een BIAR-bestand, met een tijdelijke CMS.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Voorbeeld

In het volgende voorbeeld wordt getoond hoe u de inhoud van een BIAR-bestand kunt weergeven.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Voorbeeld

In het volgende voorbeeld wordt getoond hoe u de instellingen kunt herstellen vanuit een BIAR-bestand. U moet altijd een tijdelijke CMS gebruiken wanneer u serverinstellingen herstelt.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```

15 Uw BI-platformimplementatie kopiëren

15.1 Overzicht van systeemkopieën

In dit hoofdstuk wordt beschreven hoe u een duplicaat van uw BI-platforminstallatie kunt maken voor tests, stand-bygebruik of andere doeleinden.

Zie 1275068 voor meer informatie.

Verwante informatie

Overzicht van back-up en herstel [pagina 550]

15.2 Terminologie

Begrip	Definitie
Bronsysteem	De oorspronkelijke BI-platformimplementatie.
Doelsysteem	De nieuwe implementatie die u wilt maken.
Systeemkopie	Het maken van een duplicaat van een bestaande BI-platformimplementatie.
Homogene systeemkopie	Het maken van een systeemduplicaat waarbij de bron- en doelsystemen hetzelfde type besturingssysteem en database hebben. Het BI-platform ondersteunt alleen homogene systeemkopieën.
Heterogene systeemkopie	Het maken van een systeemduplicaat waarbij bron- en doelsysteem een ander type besturingssysteem en database hebben, maar dezelfde gegevens gebruiken.
Databasekopie	Het maken van een duplicaat van de CMS-systeemdatabase of controledatabase met de hulpprogramma's van de databaseleverancier.

15.3 Use cases voor systeemkopieën

In de volgende tabel worden de doelen beschreven die u wilt verwezenlijken met de resources waarover u mogelijk beschikt, en wordt de meest toepasselijke oplossing geboden.

Doelstelling	Vereiste resources	Oplossing
Doel: identieke kopie Ik wil een gedupliceerd systeem maken voor stand-by- of testdoeleinden met een identieke hardwareconfiguratie en identieke IP-adressen/computernamen.	• Een doelsysteem met identieke hardware op het bronsysteem en • Back-ups van het bronsysteem of toegang tot het bronsysteem om een back-up te maken.	Gebruik de werkstroom voor systeemback-up en -herstel die in deze handleiding wordt beschreven. Zie de procedure Een back-up maken van het volledige systeem [pagina 554]. Maak het doelsysteem op basis van de back-ups van het bronsysteem.
Doel: Kopiëren Ik wil een gedupliceerd systeem maken voor stand-by-, test- of trainingsdoeleinden met andere hardware en IP-adressen/ computernamen dan het bronsysteem.	• Bronsysteem (actief of gestopt) OF back-ups van bronsysteemdatabases en -bestanden en • Uitgebreide systeeminformatie in Exporteren vanaf een bronsysteem [pagina 579]	Zie de werkstroom Systeemkopie vanaf Voorbereiding op het kopiëren van uw systeem [pagina 576], en voer de instructies in de rest van dat hoofdstuk uit. **Opmerking** U kunt uw doelsysteem maken op een computer met een bestaande BI-platformimplementatie met dezelfde versie, hetzelfde ondersteuningspakket en hetzelfde patchniveau, of op een 'schone' computer waarop BI-platform niet is geïnstalleerd.

Verwante informatie

Back-ups [pagina 553]
Voorbereiding op het kopiëren van uw systeem [pagina 576]

15.4 Voorbereiding op het kopiëren van uw systeem

Een systeemkopie hoeft niet uw huidige systeem te weerspiegelen. U kunt een kopie van uw systeem maken en een poosje wachten voordat u de kopie opnieuw op het doelsysteemmaakt, of u kunt een eerdere back-up van het bronsysteem gebruiken als basis voor uw doelsysteem. Dit betekent dat de kopie het systeem vertegenwoordigt op het tijdstip dat de kopie werd gemaakt. Als u bijvoorbeeld een maand wacht, maakt u met de kopie het systeem opnieuw zoals dat een maand eerder bestond.

Na het doornemen van de gebruikscases in de voorgaande sectie en het bepalen welke case het beste aansluit op uw behoeften, moet u een plan voor het maken van de systeemkopie ontwikkelen.

Een plan voor het maken van de systeemkopie ontwikkelen

Wanneer u het kopiëren van een systeem plant, moet u vooraf het volgende vaststellen:

- Wordt het bronsysteem gestopt of blijft het actief terwijl de kopie wordt gemaakt? (U kunt de procedure onder beide omstandigheden uitvoeren.)
  - Als het bronsysteem wordt gestopt, hoeveel uitvaltijd is dan vereist?
  - Plan tijd in om de integriteit van het doelsysteem te testen.
- Welke databasehulpprogramma's u wilt gebruiken voor back-up en herstel van de database.
- Op welke computers het doelsysteem wordt geïmplementeerd en waar elk knooppunt wordt gehost.
- Welke optionele onderdelen u wilt kopiëren.
- Het databasetype dat u wilt gebruiken voor de CMS-doeldatabase, en eventuele andere optionele databases die u zult kopiëren.

U moet ook rekening houden met het volgende:

- Welke BI-platformonderdelen zijn geïnstalleerd op uw bronsysteem. U kunt de functie *Toevoegen/verwijderen* > *Wijzigen* van het installatieprogramma gebruiken om een lijst weer te geven met momenteel geïnstalleerde onderdelen.
- Als het doelsysteem is geïnstalleerd op een andere hardwareset-up dan het bronsysteem, moet u het doelsysteem mogelijk afstemmen voor betere prestaties. Zie de informatie over het verbeteren van systeemprestaties in de *SAP BusinessObjects Business Intelligence sizing companion guide*
- U wilt misschien dat het doelsysteem rapporteert van andere rapportagedatabases dan de bronsysteemdatabases. In dit geval moet u de databaseverbindingsgegevens voor de rapportagedatabases wijzigen. U kunt dit doen door dezelfde DSN-naam te behouden, maar met de DSN op het doelsysteem verwijzen naar een andere database.

Vereiste bronsysteemonderdelen

- CMS-systeemdatabase
- FRS-bestandsopslag
- Configuratiebestanden voor semantische laag.
- Controledatabase (optioneel)
- Database van toezichtfunctie (optioneel)
- Subversiedatabase voor promotiebeheer (optioneel)

15.5 Overwegingen en beperkingen

Bij het maken van een kopie van uw BI-platformimplementatie moet u rekening houden met de volgende overwegingen.

Vlakdiagram	Overweging
SAP Business Warehouse-integraties	Als u het BI-platform en SAP ERP of BW in een geïntegreerde omgeving gebruikt, lees dan de documentatie over SAP-systeemkopieën voordat u uw systeem kopieert. De handleidingen voor systeemkopieën zijn beschikbaar via http://www.sdn.sap.com/irj/sdn/systemcopy (SMP-aanmelding vereist). Kies uw SAP NetWeaver-versie. De relevante handleidingen voor kopieën vindt u in de map met installatiehandleidingen.
Programmaversie	Het bron- en doelsysteem moeten dezelfde versie en hetzelfde ondersteuningspakket en patchniveau hebben.
Inhoud en configuratie-instellingen	U kunt alleen het gehele bronsysteem kopiëren. Het is niet mogelijk om inhoud of systeemconfiguratie-instellingen apart te kopiëren.
Installatiepad	Het installatiepad op de bron- en doellocatie moet identiek zijn: als u bijvoorbeeld het bronsysteem hebt geïnstalleerd op `C:\SAP BusinessObjects Enterprise XI 4.0`, moet u ook het doelsysteem installeren op `C:\SAP BusinessObjects Enterprise XI 4.0`.
Hostbesturingssysteem	De bron- en doelbesturingssystemen moeten ook identiek zijn.
Softwaretype van CMS-database	CMS-bron- en doeldatabases moeten van hetzelfde type zijn. U kunt naar een ander ondersteund databasetype overstappen nadat u het systeem hebt gekopieerd.
Softwaretype van controledatabase	Als u controlegegevens kopieert, moeten de bron- en doeldatabases met controlegegevens van hetzelfde type zijn. Na het maken van de kopie kunt u een nieuwe database van een ander type instellen. **Opmerking** Wanneer u een nieuwe database instelt, worden bestaande gebeurtenissen niet naar die database gekopieerd. Alleen nieuwe gebeurtenissen worden in de nieuwe database vastgelegd.
Weblaagaanpassingen	Bij de kopieerprocedure worden geen weblaagonderdelen van het bronsysteem gekopieerd. Als u de weblaag hebt aangepast (bijvoorbeeld door de `.properties`-bestanden in de map `custom` te wijzigen), moet u deze aanpassingen handmatig in de doelversie aanbrengen.
Onderwerpen die niet in deze instructies worden behandeld	In deze werkstroom wordt niet beschreven hoe u een database exporteert of importeert. Gebruik de hulpprogramma's van uw databaseleverancier om databases te kopiëren en te herstellen.

De volgende gegevens worden gekopieerd tijdens het kopiëren van het systeem:

- De CMS-gegevensopslagdatabase. (bevat rapporten, analyses, mappen, rechten, gebruikers en gebruikersgroepen, serverinstellingen en andere BI-inhoud en systeeminhoud)

- De controledatabase. (bevat controlegebeurtenissen die door BI-platformservers of clienttoepassingen zijn geactiveerd)
- De toezichtsdatabase. (bevat trendinggegevens van waarden, tests en controles)
- De versiebeheerdatabase. (bevat verschillende versies van rapporten, analyses, andere BI-bronnen en versiegegevens)

> **Opmerking**
>
> Zie de sectie Databases [pagina 37] van deze handleiding voor een beschrijving van de databases en de bijbehorende inhoud.

- Configuratiebestanden voor semantische laag.

De weblaagconfiguratie, zoekindex en alle gegevens die hierboven niet specifiek worden genoemd, worden niet gekopieerd.

Overwegingen voor kopieën voor bestandsherstel

Als u een systeem kopieert omdat u een bestand wilt herstellen dat per ongeluk is verwijderd, moet u rekening houden met de volgende aanvullende overwegingen:

Gebruik uw back-up om de stappen in de procedure Importeren naar een doelsysteem [pagina 583] op het productiesysteem uit te voeren.

- Installeer niet alle knooppunten; installeer alleen het eerste knooppunt voor de CMS en de bijbehorende database.
- Installeer niet de controledatabase, de database voor promotiebeheer of de toezichtdatabase.
- Maak niet opnieuw verbinding met de controle- of rapportagedatabases.

Gebruik LCM om het object dat u wilt herstellen van het doelsysteem naar het bronsysteem te verhogen.

15.6 Procedure voor het maken van een systeemkopie

De volgende procedure begeleidt u bij de twee fasen van het kopiëren van uw BI-platformimplementatie.

15.6.1 Exporteren vanaf een bronsysteem

U hebt de volgende informatie over het bronsysteem nodig. Als u deze informatie wilt noteren, kunt u daarvoor het werkblad gebruiken dat u vindt op Werkblad Systeemkopie [pagina 1232].

Eigenschap	Locatie
De CMS-clustersleutel (bewaar deze record op een veilige plaats).	Tijdens de installatie van het BI-platform door de systeembeheerder gemaakt.
De namen van de knooppunten.	Ga naar het tabblad *Servers* van de CMC en vouw *Knooppunten* uit in de linkerboomstructuur.
De computernaam en installatiemap van het BI-platform voor elke computer in de implementatie.	Ga naar het tabblad *Servers* van de CMC, klik met de rechtermuisknop op de CMS en selecteer *Tijdelijke aanduidingen*. Zoek de waarde van de tijdelijke aanduiding `%INSTALLROOTDIR%`.
Het wachtwoord van de BI-platformbeheerder (bewaar deze record op een veilige plaats).	Tijdens de installatie van het BI-platform door de systeembeheerder gecreëerd.
Alle databaseverbindingen die mogelijk door de CMS worden gebruikt en de gebruikersnamen en wachtwoorden voor deze verbindingen. Hiertoe kan ook de controledatabase behoren, als u deze informatie wilt kopiëren. Verzamel deze informatie voor alle computers in het cluster. **Opmerking** Als u de controledatabase kopieert, hebt u ook de namen en referenties voor de verbinding met de controledatabase nodig.	Ga naar het tabblad *Servers* van de CMC, klik met de rechtermuisknop op de CMS en selecteer *Gegevens*. Zoek de volgende gegevens: • *Naam van systeemdatabaseverbinding* • *Servernaam van systeemdatabase* • *Gebruikersnaam voor systeemdatabase* • *Naam gegevensbron* • *Naam verbinding controledatabase* (optioneel) • *Naam gebruiker controledatabase* (optioneel)
De details (clienttypen, versies) van alle andere databaseverbindingen (bijvoorbeeld voor universes en rapporten) van elke computer in het cluster. Noteer ook de gebruikersnamen en wachtwoorden.	Voor Crystal Reports-rapporten die rechtstreeks vanuit databases worden gerapporteerd, kunt u de verbindingsgegevens opvragen met de SAP Crystal Reports 2020- of SAP Crystal Reports voor Enterprise-ontwerpers. Voor informatie over universe-verbindingen kunt u het hulpprogramma voor informatieontwerp (.unx) of het hulpprogramma voor universe-ontwerp (.unv) gebruiken.
De versie, het ondersteuningspakket en het patchniveau van het bronsysteem.	In Windows kunt u deze informatie weergeven in het hulpprogramma *Een programma verwijderen of wijzigen*. In Unix kunt u het hulpprogramma `modifyOrRemoveProducts.sh` in de installatiemap van BI-platform gebruiken.
De locatie van de bestandsopslag voor elke invoer-FRS en uitvoer-FRS in de implementatie.	Ga naar het tabblad *Servers* van de CMC, klik met de rechtermuisknop op de invoer- of uitvoer-FRS en selecteer *Eigenschappen* Zoek de eigenschap *Map voor bestandsopslag*.

Eigenschap	Locatie
	Opmerking Als de waarde met % begint, gaat het om een tijdelijke aanduiding. In dat geval moet u op *Tijdelijke aanduidingen* klikken en een notitie maken van de map die onder de desbetreffende tijdelijke aanduiding wordt weergegeven.
Als u van plan bent Promotiebeheer, de locatie van de Promotiebeheer-databasemap en Subversion-mappen te kopiëren.	De standaardmap voor de Promotiebeheer-database in Windowsinstallaties is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` en in Unix `<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride`. De standaardlocaties voor de Subversion-bestanden in Windows-installaties zijn: • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository` en op Unix: • `<INSTALLDIR>/check_out` (deze map wordt alleen gemaakt nadat u Subversion hebt gebruikt om bestanden uit te checken.) • `$HOME/LCM_Repository`
Als u van plan bent de controledatabase te kopiëren: de controledatabasemap.	Deze waarde is ingesteld in de CMC. Ga naar het beheergebied *Toepassingen* van de CMC, selecteer *Toezichtfunctie* > *Eigenschappen* en zoek *Back-upmap van lopende database*. De standaardmap in Windows-installaties is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` en op Unix `<INSTALLATIEMAP>/sap_bobj/Data/TrendingDB`.
Het pad naar de map van de semantische laag.	Het standaardpad naar deze map in Windows-installaties is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\`.

Nadat u de bovenstaande informatie hebt vastgelegd:

1. Gebruik de hulpprogramma's van uw databaseleverancier om een back-upkopie te maken van de volgende databases:
   - De CMS-systeemdatabase
   - De controledatabase (optioneel)
2. Gebruik de hulpprogramma's voor bestandsback-up om een back-up te maken van de volgende bestandssets:
   - De bestandsopslag voor Input en Output FRS.
   - De trending-database voor controle (optioneel). U maakt hiervoor een back-up van bestanden uit de controlemap zoals vastgelegd op het werkblad. In Windows is dit standaard: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. In Unix: `<INSTALLATIEMAP>/sap_bobj/Data/TrendingDB`.
   - Subversion-database voor Promotiebeheer (optioneel). U maakt hiervoor een back-up van bestanden uit de Subversion-mappen zoals vastgelegd op het werkblad. In Windows is dit standaard:
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`.

     En op Unix:
     - `<INSTALLDIR>/check_out` (deze map wordt alleen gemaakt nadat u Subversion hebt gebruikt om bestanden uit te checken.)
     - `$HOME/LCM_Repository`
   - Configuratiebestanden in de map van de semantische laag: het bestand `cs.cfg` in de map `connectionServer` en alle `.sbo`- en `.prm`-bestanden in alle submappen.

     > **Opmerking**
     >
     > Raadpleeg de sectie Dynamische back-ups [pagina 554] voor beperkingen en een gedetailleerde beschrijving van deze werkstroom.
3. De volgende bestanden kunnen door de gebruiker worden aangepast. Als u bestanden hebt aangepast, maakt u een back-up van de bestanden op het bronsysteem en herstelt u ze later naar dezelfde map op het doelsysteem:
   - `BO_trace.ini` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties` geïnstalleerd op:
     - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
   - WDeploy-configuratiebestanden geïnstalleerd op `[INSTALLATIEMAP]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf`:
     - `config.apache`
     - `config.jboss7`

    - `config.sapappsvr75`
    - `config.tomcat6`
    - `config.tomcat7`
    - `config.weblogic11`
    - `config.websphere7`
    - `config.websphere8`
    - `wdeploy.conf`
4. De volgende weblaagbestanden kunnen door de gebruiker worden aangepast. Als u wijzigingen hebt aangebracht in deze bestanden, maakt u een back-up van deze bestanden op het bronsysteem. Later moet u deze bestanden herstellen of de wijzigingen opnieuw op het doelsysteem toepassen.
   - `BO_trace.ini` geïnstalleerd in:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
   - `clientaccesspolicy.xml` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
   - `clientSDKOptions.xml` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
   - `crossdomain.xml` geïnstalleerd op:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
     - `[INSTALLDIR]tomcat/webapps/ROOT`
   - Alle aangepaste mappen in de map `config/custom` (in de weblaag). Maak een back-up van deze bestanden om de aanpassing naar het doelsysteem over te dragen.
5. Maak een back-up van aangepaste uitbreidingsmodules die u handmatig aan het bronsysteem hebt toegevoegd, bijvoorbeeld uitbreidingsmodules voor publicaties en aangepaste bibliotheken.

Bewaar de bovenstaande informatie bij de kopieën van de database en bestanden. U kunt eventueel een tweede exemplaar bewaren dat u zonodig kunt bijwerken tijdens toekomstige procedures voor het maken van systeemkopieën.

15.6.2 Importeren naar een doelsysteem

In deze procedure wordt ervan uitgegaan dat u back-ups van de implementatiedatabases en systeembestanden van de bron hebt gemaakt die u in het doelsysteem wilt gebruiken. Alle back-upbestanden moeten zich in dezelfde back-upset bevinden. U hebt ook de informatie nodig (bijvoorbeeld clustersleutels en databasereferenties) die wordt beschreven in “Een export vanaf een bronsysteem uitvoeren”.

Als het doelsysteem op een netwerklocatie komt te staan met toegang tot de bronsysteembronnen, moet u zorgen dat het doelsysteem niet probeert toegang tot deze bronnen te krijgen tot het systeem opnieuw is geconfigureerd. U installeert hiervoor een firewall tussen de bronnen van het doelsysteem en van het

bronsysteem, of u schakelt het bronsysteem nog niet in terwijl u het doelsysteem start. Nadat u het doelsysteem voor het eerst hebt opgestart, kunt u de firewall verwijderen of het bronsysteem starten.

Als op het doelsysteem het BI-platform al is geïnstalleerd, moet u controleren of dit dezelfde versie is en de installatie hetzelfde patchniveau heeft als het bronsysteem op het moment dat de kopie werd gemaakt. Controleer ook of het installatiepad gelijk is aan dat van het bronsysteem.

1. Maak op het doelsysteem de databaseverbindingen naar de locaties waarop u de CMS-gegevensopslagruimte, controledatabase en rapportagedatabase wilt plaatsen.

   > **Opmerking**
   >
   > Deze verbindingen kunnen naar verschillende databases verwijzen, maar ze moeten dezelfde verbindingsnaam of DSN hebben en dezelfde referenties gebruiken als op het bronsysteem.

2. Gebruik uw databasehulpprogramma's om de CMS-systeemdatabase en controledatabase (indien vereist) van de back-up van het bronsysteem te herstellen naar de doeldatabase.

   Als de universes of rapporten op het doelssyteem een andere rapportagedatabase moeten gebruiken, wijzigt u de databaseverbinding zodat naar de juiste database wordt verwezen.

   Zie het onderwerp Uw systeem herstellen [pagina 560] voor meer informatie over deze stap.

3. Ga verder met stap 4 als het BI-platform op het doelhostsysteem is geïnstalleerd. Als het BI-platform niet is geïnstalleerd, installeert u het BI-platform op het doelhostsysteem. Houd daarbij rekening met het volgende:
   a. Installeer dezelfde programmaversie en hetzelfde ondersteuningspakket en patchniveau als op het bronsysteem.
   b. Gebruik hetzelfde installatiepad als het bronsysteem.
   c. Selecteer dezelfde onderdelen die op het bronsysteem zijn geïnstalleerd.
   d. Wanneer het installatieprogramma u vraagt de CMS-database (en controledatabase, indien van toepassing) te maken, kiest u de optie *Een bestaande databaseserver gebruiken* en voert u de naam en referenties in van de verbinding die in stap 1 is ingesteld.

      > **Opmerking**
      >
      > U moet de CMS-database niet opnieuw initialiseren.

   e. Wanneer u om de *Naam van knooppunt* wordt gevraagd, gebruikt u dezelfde namen en poortnummers, hetzelfde wachtwoord van de platformbeheerder en dezelfde clustersleutel als op het bronsysteem.

      Zie de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor volledige installatie-instructies. Ga verder met stap 6 als de installatie van het systeem is voltooid.

      > **Opmerking**
      >
      > Als u geen controlegegevens van het bronsysteem kopieert, kunt u een nieuwe controledatabase maken door de controlefunctie tijdens de installatieprocedure te configureren.

   f. Stop alle knooppunten in de CCM.

4. Als het BI-platform al op het doelsysteem is geïnstalleerd, stopt u alle knooppunten in de CCM. Start de CCM op de CCS-hostcomputer van het doelsysteem.
5. Als BI-platform al is geïnstalleerd, voegt u een nieuw knooppunt toe via de optie *Knooppunt opnieuw maken*.
   a. Gebruik de *Naam van knooppunt* en het *SIA-poortnummer van het bronsysteem.*

b. Kies *Een nieuwe tijdelijke CMS starten*.
c. Selecteer een nieuw *CMS-poortnummer* (een willekeurige vrije poort) en *CMS-databasetype* (in overeenstemming met het herstelde databasetype).
d. Geef de gegevens op van de verbinding waarnaar de CMS-database bij stap 1 is hersteld.
e. Geef de clustersleutel van het bronsysteem op.
f. Geef het beheerderswachtwoord van het bronsysteem op.

6. Herstel de bestandsopslag van de invoer- en uitvoer-FRS naar de bestandsopslag van het doelsysteem. Gebruik dezelfde map als op het bronsysteem.
7. Herstel de controledatabasemap (als u controlegegevens wilt kopiëren) naar dezelfde map als op het bronsysteem.
8. Herstel de databasemap Promotiebeheer (als u gegevens Promotiebeheer wilt kopiëren) in dezelfde map als de map die voor het bronsysteem is gebruikt.
9. Herstel de Subversionbestanden (als u gegevens Promotiebeheer wilt kopiëren) in dezelfde map als de map die voor het bronsysteem is gebruikt.
10. Herstel de serverbestanden van de semantische laag/verbindingsconfiguratie naar dezelfde map als op het bronsysteem.
11. Start de hostcomputers van het doelsysteem opnieuw.
12. Als u BI-platform in stap 3 op het doelsysteem hebt geïnstalleerd, moet u de vereiste ondersteuningspakketten of patches toepassen, zodat bron- en doelsysteem overeenkomen.
13. Als het doelsysteem op meerdere hostcomputers wordt uitgevoerd, moet u stap 1 t/m 11 op elke hostcomputer uitvoeren.

    Gebruik de optie Uitgebreide installatie bij het installeren van aanvullende BI-platformknooppunten, en houd er rekening mee dat u dezelfde knooppuntnamen als op het bronsysteem moet gebruiken voor de aanvullende knooppunten op het doelsysteem.
14. Als voor de CMS-database op het doelsysteem een ander databasetype wordt gebruikt dan op het bronsysteem, moet u CCM gebruiken om Gegevens kopiëren tussen CMS-systeemdatabases [pagina 506] uit te voeren, en als doel de database opgeven die u als kopie wilt gebruiken.
15. Herstel bestanden die door de gebruiker kunnen worden aangepast en waarvan u een back-up in stap 3 van de procedure "Exporteren vanaf een bronsysteem" hebt gemaakt.
16. Herstel weblaagbestanden waarvan u een back-up in stap 4 van de procedure "Exporteren vanaf een bronsysteem" hebt gemaakt.

    "Weblaag" verwijst naar het staging-gebied van WDeploy waar u uw aanpassingen kunt uitvoeren, en naar de weblaaginhoud die op de toepassingsserver is geïmplementeerd.

    Wanneer u wijzigingen op het doelsysteem toepast, moet u geen wijzigingen op de toepassingsservermap toepassen. Pas de wijzigingen toe op het WDeploy-staging-gebied en implementeer de weglaag vervolgens opnieuw op de toepassingsserver met behulp van WDeploy.

    Het WDeploy-staging-gebied bevindt zich op deze locatie in Windows: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/warfiles`.
17. Herstel uitbreidingsmodules waarvan u een back-up in stap 5 van de procedure "Exporteren vanaf een bronsysteem" hebt gemaakt.

Nadat de systeemkopie van het BI-platform is uitgevoerd:

1. Bij het installeren van het eerste knooppunt op het doel wordt een tijdelijke CMS gemaakt, die bij het voltooien van de installatie wordt gestopt. Ga in de CMS naar de pagina Servers en verwijder deze CMS.

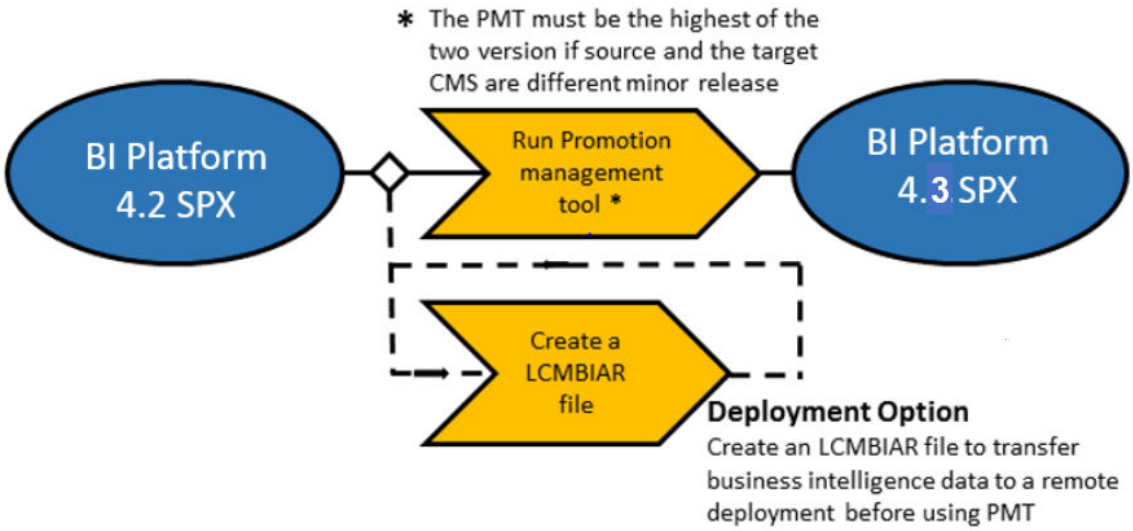
> → Onthouden
>
> Als u het bronsysteem niet verwijdert (of als u het tegelijk met het doelsysteem gebruikt), is het raadzaam de naam van het cluster op het doelsysteem te wijzigen.

2. Gebruik het Diagnostisch hulpprogramma voor gegevensopslagruimte voor de CMS-doeldatabase.
3. Indien van toepassing configureert u Windows AD SSO (Single Sign-On) op het doelsysteem. Zie SSO bij het BI-platform met AD-verificatie [pagina 312].
4. Indien van toepassing configureert u SLD op het doelsysteem. Voor details raadpleegt u SAP Note 1508421: "SAP SLD Data Supplier for Apache Tomcat".
5. Voer een gezondheidscontrole op het doelsysteem uit om de integriteit te controleren.
6. Indexeer de volledige zoekfunctie opnieuw.

16 Promotiebeheer

16.1 Welkom bij promotiebeheer

16.1.1 Overzicht



Met het hulpprogramma voor doorgiftebeheer kunt u:

- BI-bronnen (Business Intelligence) van de ene naar de andere opslagplaats verplaatsen of transporteren.
- Afhankelijkheden van de bronnen beheren.
- De doorgegeven bronnen terugzetten naar het doelsysteem, indien noodzakelijk.

Door het hulpprogramma voor promotiebeheer wordt ook het beheer van verschillende versies van dezelfde BI-bron ondersteund.

Het hulpprogramma Promotiebeheer is met de Central Management Console geïntegreerd. BI-bronnen kunnen uitsluitend van het ene systeem naar het andere worden overgebracht als het bron- en doelsysteem beide dezelfde versie van het BI-platformbevatten.

16.1.2 Functies

Met het hulpprogramma Promotiebeheer kunt u de volgende acties uitvoeren voor InfoObjects in de doelimplementatie.

- Een nieuwe taak aanmaken
- Een bestaande taak kopiëren
- Een taak bewerken
- Een taakverhoging plannen
- De geschiedenis van een taak weergeven
- Exporteren als LCMBIAR
- Importeren van BIAR en LCMBIAR

De werkstroom voor het verhogen bevat de volgende taken:

- *Afhankelijkheden beheren*: met deze functie kunt u de afhankelijkheden van de InfoObjects in de taak die u wilt verhogen, selecteren, filteren en beheren.
- *Planning*: met deze functie kunt u een tijd instellen voor het verhogen van een taak in plaats van een taak meteen te verhogen zodra deze is gemaakt. U kunt aangeven dat de taakverhoging eenmalig of periodiek wordt uitgevoerd.
- *Beveiliging*: met deze functie kunt u InfoObjects verhogen met de bijbehorende beveiligingsrechten en indien noodzakelijk met bijbehorende toepassingsrechten.
- *Verhoging testen*: met deze functie kunt u de verhoging controleren of testen om ervoor te zorgen dat alle voorzorgsmaatregelen zijn genomen voordat de InfoObjects daadwerkelijk worden verhoogd.
- *Terugzetten*: met deze functie kunt u het doelsysteem terugzetten in de vorige status nadat een taak is verhoogd. U kunt een volledige taak of slechts een deel van een taak ongedaan maken.
- *Controle*: de gebeurtenissen die worden gegenereerd door het hulpprogramma Promotiebeheer, worden opgeslagen in de controledatabase. Met deze functie kunt u de gebeurtenissen controleren die worden bijgehouden in de controledatabase.
- *Instellingen voor overschrijven in Promotiebeheer*: met deze functie kunt u de overschrijvingen scannen en verhogen via een taakpromotie.

16.1.3 Toegangsrechten voor toepassingen

In deze sectie worden de toegangsrechten voor het hulpprogramma Promotiebeheer beschreven.

- U kunt toegangsrechten voor het hulpprogramma Promotiebeheer instellen in de CMC.
- U kunt granulaire toepassingsrechten instellen voor verschillende functies in het hulpprogramma Promotiebeheer.

Voer de volgende stappen uit als u specifieke rechten wilt instellen in het hulpprogramma Promotiebeheer:

1. Meld u aan bij de CMC en selecteer *Toepassingen*.
2. Dubbelklik op *Promotiebeheer*.
3. Klik op *Gebruikersbeveiliging* en selecteer een gebruiker. U kunt beveiligingsrechten weergeven voor of toewijzen aan de gebruiker.
4. Voor Promotiebeheer zijn de volgende specifieke rechten beschikbaar:
   - Toegang verlenen voor bewerking van overrides
   - Toegang tot Beveiliging opnemen toestaan
   - Toegang tot beheer toestaan
   - Toegang tot Afhankelijke objecten beheren toestaan

- Taak maken
- Taak verwijderen
- Taak bewerken
- LCMBIAR bewerken
- Exporteren als LCMBIAR
- LCMBIAR importeren
- Taak verhogen
- Taak terugzetten
- BOMM-objecten (BusinessObjects Metadata) weergeven en selecteren
- Business Views weergeven en selecteren
- Agenda's weergeven en selecteren
- Verbindingen weergeven en selecteren
- Profielen weergeven en selecteren
- QaaWS weergeven en selecteren
- Rapportobjecten weergeven en selecteren
- Beveiligingsinstellingen weergeven en selecteren
- Universes weergeven en selecteren

5. Als u rechten aan een geselecteerde gebruiker wilt toewijzen, selecteert u het relevante recht en klikt u op *Beveiliging toewijzen*.

De toegangsrechten voor het hulpprogramma Promotiebeheer worden in de CMC ingesteld.

16.1.4 Ondersteuning voor WinAD in Promotiebeheer

Om het hulpprogramma Promotiebeheer naar behoren te laten functioneren, voegt u het volgende toe aan alle `javaargs`-argumenten voor alle Adaptive Job Servers:

```
Djava.security.auth.login.config=<path>\bsclogin.conf,Djava.security.krb5.conf=<p
ath>\krb5.ini
```

> → Onthouden
>
> Geef het juiste pad naar `bsclogin.conf` en `krb5.ini` op uw implementatie op.

16.2 Aan de slag met het hulpprogramma voor promotiebeheer

16.2.1 Het hulpprogramma voor promotiebeheer openen

U opent het hulpprogramma voor promotiebeheer door *Promotiebeheer* te selecteren op de CMC-startpagina.

Alle gebruikers met weergaverechten voor de map *Promotietaken* kunnen het hulpprogramma voor promotiebeheer starten. Voor het aanmaken, plannen of verhogen van een taak moeten aan de gebruiker echter extra machtigingen worden verleend door de beheerder.

16.2.2 Onderdelen van gebruikersinterface

In dit hoofdstuk worden de GUI-onderdelen in het hulpprogramma voor promotiebeheer besproken.

- Werkbalk in werkruimte van Doorgiftebeheer
- Deelvenster Werkruimte
- Deelvenster Boomstructuur
- Venster Details
- De pagina Winkelwagentje en Taakweergave

Werkbalk in werkruimte van Promotiebeheer

In de volgende tabel geeft een overzicht van de opties op de werkbalk van de promotiebeheerwerkruimte evenals een uitleg van de taken die u met deze opties kunt uitvoeren:

Optie	Beschrijving
	Hiermee kunt u een nieuwe map maken. De nieuwe map wordt aangemaakt als een submap in de map *Promotietaken*.
	Hiermee kunt u de geselecteerde taak of map uit de huidige locatie kopiëren of verwijderen.
	Hiermee kunt u de geselecteerde taak of map uit de huidige locatie kopiëren.
	Hiermee kunt u de gekopieerde taak of map naar een nieuwe locatie plakken.
	Hiermee kunt u een bestaande taak of map verwijderen.
	Hiermee kunt u de startpagina vernieuwen om de bijgewerkte lijst met taken of mappen weer te geven.
Eigenschappen	Hiermee kunt u de eigenschappen van de geselecteerde taak bewerken. U kunt de titel, beschrijving en trefwoorden van de geselecteerde taak wijzigen.
Geschiedenis	Hiermee kunt u de geschiedenis van de geselecteerde taak weergeven.
Nieuwe taak	Hiermee kunt u een nieuwe taak maken.
Importeren	Hiermee kunt u BIAR-/LCMBIAR-bestanden of bestanden voor overschrijving importeren.
Bewerken	Hiermee kunt u de geselecteerde taak bewerken.
Verhogen	Hiermee kunt u de geselecteerde taak doorgeven.

Optie	Beschrijving
Terugzetten	Hiermee kunt u de doorgegeven taak verwijderen uit het doelsysteem. **Opmerking** Als er voor de taak objecten worden verhoogd naar de doellocatie, worden deze objecten met de actie Terugzetten verwijderd. Als er voor de taak objecten worden bijgewerkt op de doellocatie, wordt de vorige versie van de objecten met de actie Terugzetten hersteld.
1	Hiermee kunt u navigeren door de pagina's van een taaklijst. U kunt deze optie gebruiken om door één pagina te navigeren, of naar een bepaalde pagina te navigeren door het desbetreffende paginanummer in te voeren.
Zoeken	Hiermee kunt u zoeken naar specifieke taken. U kunt een taak zoeken op naam, trefwoorden, beschrijving of met alle drie de parameters.
Promotietaken	Hiermee kunt u de taken en mappen weergeven.
Promotiestatus	Hiermee worden de verhoogde taken weergegeven op basis van hun status, zoals Geslaagd, Mislukt of Gedeeltelijk geslaagd.

Deelvenster Werkruimte

Het venster Werkruimte op de startpagina Promotiebeheer geeft een overzicht van de taken. Gebruik dit deelvenster om de naam, status, aanmaaktijd en laatste uitvoeringstijd van de taak, de bron- en doelsystemen en de taakmaker weer te geven.

Deelvenster Boomstructuur

In het Structuurvenster op de startpagina van promotiebeheer wordt de boomstructuur weergegeven, met onder andere de mappen *Promotietaken* en *Promotiestatus*. De taken worden weergegeven in een hiërarchische structuur onder de map *Promotietaak*. In de map *Promotiestatus* worden de verhoogde taken weergegeven op basis van hun status.

Deelvenster Taakweergave

De pagina “Taakweergave” wordt weergegeven als een gebruiker een nieuwe taak maakt of een bestaande taak bewerkt. De pagina bevat een dynamisch gegenereerde lijst met InfoObjects die moeten worden verhoogd en bevat een deelvenster Details. De InfoObjects in de lijst worden onderverdeeld in gebruikersgroepen, universes en verbindingen. In het deelvenster Details wordt de inhoud weergegeven van de node die is geselecteerd in de lijst.

16.2.3 De optie Instellingen gebruiken

Via de optie Instellingen kunt u instellingen configureren voordat InfoObjects worden verhoogd van de ene BI-platformimplementatie naar de andere BI-platformimplementatie en SAP-implementatie. In deze sectie wordt beschreven hoe u de instellingsopties kunt gebruiken.

Klik op de vervolgkeuzelijst *Instellingen* op het scherm *Promotietaken*. In deze vervolgkeuzelijst worden de volgende opties weergegeven:

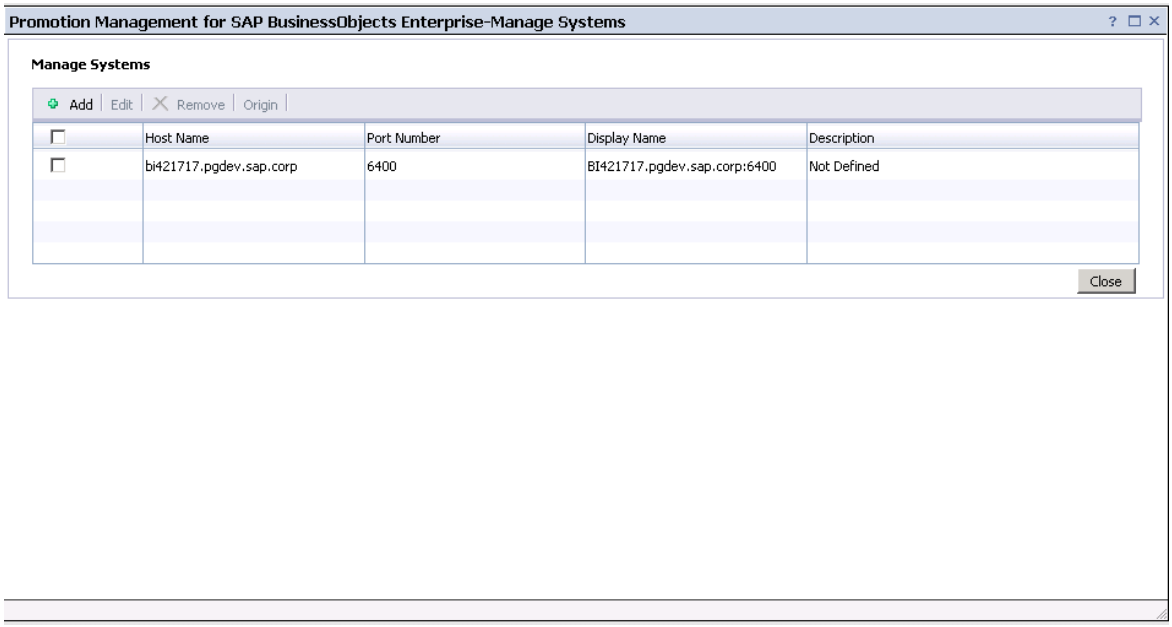
- *Systemen beheren*: hiermee kunt u alle vereiste systemen voor activiteiten van Promotiebeheer toevoegen.
- *Instellingen ongedaan maken*: hiermee kunt u een systeem selecteren waarvoor ongedaan maken is ingeschakeld.
- *Taakinstellingen*: hiermee kunt u voltooide exemplaren op de pagina Afhankelijkheden bekijken en kunt u opschoonactiviteiten voor taakexemplaren beheren. Ook kunt u filteren op aanmaakdatum voor de taak.
- *CTS-instellingen*: hiermee kunt u de webservice- en SAP BW-systeemgegevens voor de integratie van het Enhanced Change Transport System toevoegen.

16.2.3.1 De optie Systemen beheren gebruiken

In deze sectie wordt het gebruik van de optie Systemen beheren beschreven. Met deze optie kunt u hostsystemen toevoegen of verwijderen.

Voer de volgende stappen uit om een hostsysteem toe te voegen:

1. Klik in de werkbalk van de promotiebeheerwerkruimte op *Instellingen* en klik vervolgens op *Systemen beheren*.
   Het venster *Systemen beheren* wordt weergegeven. In dit venster wordt een lijst met hostnamen, poortnummers, weergavenamen en beschrijvingen weergegeven.



2. Klik op *Toevoegen*.
   Het dialoogvenster *Systeem toevoegen* wordt weergegeven.

3. Geef de hostnaam, het poortnummer, de weergavenaam en de beschrijving op in de desbetreffende velden.

> **Opmerking**
>
> Selecteer de optie *Markeren als oorsprong* om het systeem als het bronsysteem aan te duiden (het systeem waarvan de verbindingsgegevens afkomstig zijn). Deze optie is handig bij het werken met overrides.

4. Klik op *OK* om het systeem toe te voegen.
   Het hostsysteem wordt aan de lijst toegevoegd.

> **Opmerking**
>
> Als u een hostsysteem wilt verwijderen of bewerken, selecteert u een hostsysteem en klikt u op *Verwijderen* of *Bewerken*.

Verwante informatie

De optie Instellingen ongedaan maken gebruiken [pagina 593]
De optie Taakinstellingen gebruiken [pagina 593]

16.2.3.2 De optie Instellingen ongedaan maken gebruiken

Het proces van ongedaan maken is op systeemniveau standaard ingeschakeld. Met de optie *Instellingen ongedaan* maken kunt u het terugzetproces op systeemniveau uitschakelen.

Voer de volgende stappen uit als u het proces van ongedaan maken op systeemniveau wilt uitschakelen:

1. Selecteer het hostsysteem in de lijst met hostsystemen in het venster *Terugzetten* om het terugzetproces uit te schakelen.
2. Klik op *Opslaan en sluiten* om de wijzigingen op te slaan.

Verwante informatie

De optie Taakinstellingen gebruiken [pagina 593]

16.2.3.3 De optie Taakinstellingen gebruiken

Met de optie Taakinstellingen kunt u opgeven of u voltooide exemplaren wilt weergeven op de pagina “Afhankelijkheden beheren” en kunt u opgeven hoeveel taakexemplaren in het systeem kunnen bestaan. U kunt kiezen uit de volgende opties:

- *Voltooide exemplaren weergeven op de pagina Afhankelijkheden beheren* Met deze optie kunt u voltooide exemplaren weergeven op de pagina "Afhankelijkheden beheren" die kunnen worden toegevoegd aan de taak.
- *Overtollige exemplaren na N exemplaren verwijderen voor een taak* Met deze optie kunt u het maximum aantal exemplaren per taak opgeven in het systeem.
- *Overtollige exemplaren verwijderen na N dagen voor de taak* Met deze optie kunt u de taakexemplaren opgeven die moeten wordeen verwijderd en die zijn gemaakt vóór een opgegeven aantal dagen.
- In de lijst *Toon aangemaakte taken* kunt u de tijdsinterval selecteren voor het weergeven van de taken die gedurende een bepaalde periode zijn gemaakt.

Voer de volgende stappen uit om de optie *Taakinstellingen* in te schakelen:

1. Selecteer de optie en voer de gewenste waarde in.
2. Klik op *Opslaan* om de wijzigingen op te slaan.

U kunt op *Standaardinstellingen* klikken om de standaardwaarden in te stellen en u kunt op *Sluiten* klikken om het venster te sluiten.

> ⓘ Opmerking
>
> De oude taakexemplaren worden alleen verwijderd de volgende keer dat de taak wordt uitgevoerd.

Verwante informatie

Apache SubVersion gebruiken als Versiebeheersysteem [pagina 683]

16.2.3.4 De optie Instellingen voor overschrijven gebruiken

Met de optie Instellingen voor overschrijven kunt u overrides verhogen via een taakpromotie of een LCMBIAR-bestand. Met deze optie kunt u de gegevens van de databaseverbinding voor Crystal Reports- en Universe-verbindingen scannen, verhogen en bewerken. U kunt de optie ook gebruiken om de QAAWS-URL's te bewerken.

> ⓘ Opmerking
>
> Installeer Adobe Flash Viewer om de optie Instellingen voor overschrijven te gebruiken.

In de volgende procedures wordt de term *system* gebruikt. Er zijn drie soorten systemen:

- *Oorsprong*: het oorspronkelijke systeem voor alle verbindingsgegevens.
- *Central Promotion Management*: het systeem dat het hulpprogramma voor promotiebeheer uitvoert.
- *Doel*: het eindsysteem waaraan de BI-bronnen worden doorgegeven.

16.2.3.4.1 Overrides verhogen

Voeg een hostsysteem toe voordat u de overrides verhoogt. Zie De optie Systemen beheren gebruiken [pagina 592] voor informatie over het toevoegen van hostsystemen.

Voer de volgende stappen uit om de overschrijvingen te verhogen:

1. Klik op de werkbalk van de promotiebeheerwerkruimte op de optie *Instellingen overschrijven*.
   Het venster *Instellingen overschrijven* wordt weergegeven.
2. Selecteer in het deelvenster *Oorsprong* het gewenste bronsysteem uit het vervolgkeuzemenu.

   > **Opmerking**
   >
   > U kunt ook inloggen bij een *nieuw systeem*. Ga als volgt te werk om een nieuw systeem als bronsysteem te selecteren:
   > 1. Selecteer *Nieuw systeem* uit het vervolgkeuzemenu.
   > Het dialoogvenster Aanmelding oorsprong wordt weergegeven.
   > 2. Voer de geldige referenties in de velden *Systeem*, *Gebruikersnaam*, *Wachtwoord* en *Verificatie* in.
   > 3. Kies *Aanmelden*.

3. Kies *Aanmelden*.
4. Kies *Nu scannen*.

   Het scanproces wordt gestart. De *lijst met unieke verbindingen* wordt weergegeven.

   > **Opmerking**
   >
   > Kies *Instellingen terugkering* om een terugkerende scan te plannen.

5. Selecteer in de lijst met overrides de overrides die u wilt verhogen door de overeenkomstige selectievakjes bij elke override te selecteren.

   > **Opmerking**
   >
   > U kunt overrides zoeken in de lijst met overrides door gebruik van trefwoorden zoals overridenaam, datum laatste update enz.
   >
   > U kunt overrides ook filteren op de volgende parameters: All, Connection, Qwaas, Crystal Report.
   >
   > Daarnaast kunt u overrides in alfabetische volgorde sorteren.

6. Selecteer in het deelvenster *Doel* het gewenste doelsysteem uit het vervolgkeuzemenu. U kunt meerdere doelsystemen opgeven.

   > **Opmerking**
   >
   > U kunt ook inloggen bij een *nieuw systeem*. Ga als volgt te werk om een nieuw systeem als doelsysteem te selecteren:
   > 1. Selecteer *Nieuw systeem* uit het vervolgkeuzemenu.
   > Het dialoogvenster Aanmelding doel wordt weergegeven.
   > 2. Voer de geldige referenties in de velden *Systeem*, *Gebruikersnaam*, *Wachtwoord* en *Verificatie* in.
   > 3. Kies *Aanmelden*.

   Doe het volgende om de overrides als LCMBIAR-bestand te exporteren:

1. Selecteer Naar LCMBIAR-bestand exporteren in het vervolgkeuzemenu.
2. Kies *Exporteren*.
   Het dialoogvenster *Instellingen exporteren* wordt weergegeven.
3. Voer geldige referenties in in de respectieve velden.
4. Kies *Gereed*.

7. Kies *Verhogen*.

   Het dialoogvenster Meerdere doeloverrides wordt weergegeven.

   > **Opmerking**
   >
   > Standaard worden alle doelsystemen waarbij u momenteel bent aangemeld geselecteerd. U kunt ervoor kiezen overrides naar een bepaald doelsysteem te verhogen door het selectievakje dat hoort bij het gewenste doelsysteem te selecteren.

8. Kies *Gereed*.

   De promotie van overrides is voltooid.

9. Meld u aan bij een van de doelsystemen met geldige referenties.

   Een lijst met alle verhoogde objecten wordt weergegeven in een lijst met unieke verbindingen. De status van deze objecten is Inactief.

10. Kies *Actualiseren* voor de objecten die u wilt bewerken.

    Het dialoogvenster *Algemene verbindingseigenschappen* wordt weergegeven.

11. Actualiseer de vereiste waarden en selecteer *Gereed*.

    De status van de bewerkte objecten wordt Actief.

    > **Opmerking**
    >
    > U kunt een verbinding ook activeren door *Inactief* te selecteren; u hoeft de verbinding niet te bewerken in het doelsysteem.

12. Kies *Opslaan*.

16.2.3.4.2 Overrides verhogen met behulp van BIAR-bestanden

Voeg een hostsysteem toe voordat u de overrides verhoogt. Zie De optie Systemen beheren gebruiken [pagina 592] voor informatie over het toevoegen van hostsystemen.

Voer de volgende stappen uit als u de overschrijvingen via BIAR-bestanden wilt verhogen:

1. Klik op de werkbalk van de promotiebeheerwerkruimte op de optie *Instellingen overschrijven*.
   Het venster *Instellingen overschrijven* wordt weergegeven.
2. Als u bent aangemeld bij het centrale systeem voor promotiebeheer, meld u dan af van het systeem.
3. Klik op *Aanmelden* om een verbinding met het oorspronkelijke systeem te maken.
   Het venster *Aanmelden bij systeem* wordt weergegeven.
4. Selecteer in het venster *Instellingen overschrijven* het bronsysteem dat is gemarkeerd als *Oorsprong* om de objecten te scannen en meld u aan bij het systeem met geldige referenties.

5. In de vervolgkeuzelijst *Start* naast *Scan* selecteert u de optie *Start*.
   Het scanproces wordt gestart. De Lijst met overschrijvingen wordt weergegeven.

   > **Opmerking**
   >
   > Als u een terugkerende scan wilt plannen, selecteert u de optie *Terugkeerinstellingen* in de vervolgkeuzelijst.

6. Wijzig in de lijst van overschrijvingen de status van de objecten in Actief en klik op *Opslaan*.
7. Klik op *Overschrijvingen verhogen*.
   Het scherm *Overschrijvingen verhogen* wordt weergegeven, waarbij de lijst van doelsystemen wordt getoond.
8. Als u het bestand BIAR wilt coderen met behulp van een wachtwoord, schakelt u het selectievakje *Wachtwoordcodering* in.
   De velden *Wachtwoord* en *Wachtwoord bevestigen* worden geactiveerd.
9. Geef een wachtwoord op in het veld *Wachtwoord*. Geef hetzelfde wachtwoord nogmaals op in het veld *Wachtwoord bevestigen*.
10. Klik op *Exporteren* en sla het overschreven BIAR-bestand op naar een bestandssysteem.
11. Meld u via de CMC aan bij het doelsysteem en klik in het hulpprogramma Promotiebeheer op *Importeren* > *Bestand overschrijven* >.
    Het venster *LCMBIAR importeren* wordt weergegeven.
12. Klik op *Bladeren* om door het BIAR-bestand te bladeren.
13. Geef het wachtwoord voor het BIAR-bestand op in het veld *Wachtwoord*.

    > **Opmerking**
    >
    > Het veld *Wachtwoord* wordt alleen weergegeven als het geselecteerde bestand BIAR is versleuteld met een wachtwoord

14. Klik op *OK*. De promotie van overrides is voltooid.
15. Meld u af van het oorspronkelijke systeem.
16. Klik in het venster *Instellingen voor overschrijven* op *Aanmelden*.
    Het venster *Aanmelden bij systeem* wordt weergegeven.
17. Meld u aan bij het doelsysteem met geldige referenties.
    Er wordt een overzicht van geïmporteerde objecten weergegeven in de Lijst van overschrijvingen. De status van deze objecten is Inactief.
18. Schakel het selectievakje *Selecteren* in voor de objecten die u wilt bewerken, en klik op *Bewerken*. De bewerkte objecten worden met een pictogram aangeduid.

    > **Opmerking**
    >
    > U kunt de override-objecten verwijderen door op het pictogram te klikken.

19. Werk de gewenste waarden bij en klik op *Gereed*.
    De bewerkte objecten krijgen de status Actief.
20. Klik op *Opslaan*.

16.2.3.4.3 Overrides verhogen met behulp van CTS+

Voeg een hostsysteem toe voordat u de overrides verhoogt. Zie De optie Systemen beheren gebruiken [pagina 592] voor informatie over het toevoegen van hostsystemen.

Voer de volgende stappen uit als u overrides via CTS+ wilt verhogen:

> **Opmerking**
>
> Start het hulpprogramma voor promotiebeheer via SAP-verificatie om deze optie beschikbaar te maken.

1. Klik op de werkbalk van de promotiebeheerwerkruimte op de optie *Instellingen overschrijven*.
   Het venster *Instellingen overschrijven* wordt weergegeven.
2. Als u bent aangemeld bij het centrale systeem voor promotiebeheer, meld u dan af van het systeem.
3. Klik op *Aanmelden* om een verbinding met het oorspronkelijke systeem te maken.
   Het venster *Aanmelden bij systeem* wordt weergegeven.
4. Selecteer het bronsysteem dat is gemarkeerd als *Oorsprong* om de objecten te scannen en meld u aan bij het systeem met geldige referenties.
5. In de vervolgkeuzelijst *Start* naast *Scan* selecteert u de optie *Start*.
   Het scanproces wordt gestart. De *Lijst met overschrijvingen* wordt weergegeven.

   > **Opmerking**
   >
   > Als u een terugkerende scan wilt plannen, selecteert u de optie *Terugkeerinstellingen* in de vervolgkeuzelijst.

6. Wijzig in de lijst met overschrijvingen de status in Actief voor objecten die u wilt verhogen, en klik op *Opslaan*.
7. Klik op *Overschrijvingen verhogen*.
   Het scherm *Overschrijvingen verhogen* wordt weergegeven, waarbij de lijst van doelsystemen wordt getoond.
8. Selecteer in de vervolgkeuzelijst *Verhogingsopties* de optie *Verhogen met CTS+*.
9. Klik op *Verhogen*.
10. Geef de overrides naar het doelsysteem vrij door de volgende stappen te voltooien:
    a. Meld u aan bij de domeincontroller van CTS+ en open de web-UI van de *Transport Organizer*. Zie Transport Organizer Web UI voor meer informatie over de web-UI van de Transport Organizer.
    b. Als de status van de aanvraag *Bewerkbaar* is, klikt u op *Vrijgeven* om de transportaanvraag van de overrides vrij te geven. Zie Releasing Transport Requests with Non-ABAP Objects voor meer informatie over het vrijgeven van transportaanvragen met niet-ABAP-objecten.
    c. Sluit de web-UI van de *Transport Organizer*.
11. Importeer de overrides naar het doelsysteem door de volgende stappen te voltooien:
    a. Meld u aan bij de domeincontroller van CTS+.
    b. Roep de STMS-transactie op om het transportbeheersysteem in te voeren.
    c. Klik op het pictogram *Overzicht importeren*.

       Het venster *Overzicht importeren* wordt weergegeven en hierin kunt u de geïmporteerde wachtrij-items van alle systemen weergeven.
    d. Klik op het systeem-id voor het systeem voor Promotiebeheer van het doel.
       U kunt de lijst van transportaanvragen zien die in het systeem kunnen worden geïmporteerd.

e. Klik op *Vernieuwen* .
f. Importeer de relevante transportaanvragen. Raadpleeg de documentatie over Importing Requests voor meer informatie.

12. De promotie van overrides is voltooid.
13. Meld u aan bij een van de doelsystemen met geldige referenties.
    Er wordt een lijst met alle verhoogde objecten weergegeven in de lijst met overrides. De status van deze objecten is Inactief.
14. Schakel het selectievakje *Selecteren* in voor de objecten die u wilt bewerken, en klik op *Bewerken*.
15. Werk de gewenste waarden bij en klik op *Gereed*.
    De bewerkte objecten krijgen de status Actief.
16. Klik op *Opslaan*.

16.2.3.5 De optie CTS-instellingen gebruiken

U kunt deze optie gebruiken om webservices toe te voegen aan uw infrastructuur en om daar BW-systemen te beheren. Raadpleeg de sectie CTS+-instellingen configureren in het hulpprogramma Promotiebeheer [pagina 657] voor meer informatie over het gebruik van de optie CTS-instellingen en het instellen van CTS voor gebruik met het hulpprogramma Promotiebeheer.

16.3 Het hulpprogramma voor promotiebeheer gebruiken

Wanneer u het hulpprogramma Promotiebeheer start, wordt standaard de pagina *Promotietaken* geopend.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

De startpagina van het venster *Promotietaken* bevat een aantal tabs waarmee u de volgende taken kunt uitvoeren:

- Klik op *Nieuwe taak* om een nieuwe taak te maken. U kunt ook met de rechtermuisknop op de startpagina klikken en *Nieuwe taak* uit de lijst selecteren.
- Klik op *Importeren* > *Bestand importeren* om een BIAR-bestand of LCMBIAR rechtstreeks uit het bestandssysteem te importeren. U hoeft dan niet de hele procedure voor het maken van een nieuwe taak te doorlopen.
- Klik op *Importeren* > *Bestand overschrijven* om overrides te importeren.
- Selecteer een bestaande taak in de lijst en klik op *Bewerken* om de bestaande taak te selecteren.
- Selecteer een bestaande taak in de lijst en klik op *Verhogen* om de taak uit het bronsysteem te verhogen naar het doelsysteem of exporteer de taak naar een LCMBIAR-bestand.
- Selecteer een bestaande, eerder uitgevoerde taak in de lijst en klik op *Terugzetten* om de verhoogde objecten uit het doelsysteem te verwijderen.

- Selecteer een bestaande, eerder uitgevoerde taak in de lijst en klik op *Geschiedenis* om de vorige promotie-exemplaren van de geselecteerde taak te bekijken.
- Selecteer een bestaande taak in de lijst en klik op *Eigenschappen* om de eigenschappen van de geselecteerde taak (zoals titel, id, bestandsnaam en beschrijving) te bekijken.

In het toepassingsgebied *Promotietaken* wordt een overzicht van de taken en mappen weergegeven die in het systeem aanwezig zijn, samen met de volgende informatie over elke taak of map:

- *Naam:* Geeft de naam weer van de taak of map die is gemaakt.
- *Status:* Geeft de status van de taak weer, zoals Gemaakt, Geslaagd, Gedeeltelijk geslaagd, Actief of Mislukt.
- *Gemaakt:* Geeft de datum en tijd weer waarop de taak of map is gemaakt.
- *Laatst uitgevoerd:* Geeft de datum en tijd weer waarop de taak voor het laatst werd verhoogd.
- *Bronsysteem:* Geeft de naam van het systeem weer van waaruit de taak wordt verhoogd.
- *Doelsysteem:* Geeft de naam van het systeem weer waar naartoe de taak wordt verhoogd.
- *Gemaakt door:* Geeft de naam van de gebruiker weer die de desbetreffende taak of map heeft gemaakt.

> ⓘ Opmerking
>
> Het hulpprogramma Promotiebeheer maakt gebruik van de SDK van het BI-platform voor alle activiteiten.

16.3.1 Mappen maken en verwijderen

In deze sectie wordt beschreven hoe u een map kunt aanmaken en verwijderen in de startpagina van Promotietaken.

> ⓘ Opmerking
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

16.3.1.1 Een map maken

In deze sectie wordt het maken van een map beschreven.

Voer de volgende stappen uit om een map te maken:

1. Klik op op de werkbalk van promotiebeheer.
2. Voer in het dialoogvenster *Map maken* de mapnaam in.
3. Klik op *OK*.

Er wordt een nieuwe map aangemaakt.

Verwante informatie

Een taak maken [pagina 601]
Een map verwijderen [pagina 601]

16.3.1.2 Een map verwijderen

In deze sectie wordt het verwijderen van een map beschreven.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om een map te verwijderen:

1. Selecteer een map op de startpagina *Promotietaken*.
2. Klik op .
   Er wordt een bevestigingsdialoogvenster weergegeven.
3. Klik op *OK*.

De geselecteerde map wordt verwijderd.

Verwante informatie

Een taak maken [pagina 601]

16.3.2 Een taak maken

In deze sectie wordt beschreven hoe u een nieuwe taak kunt maken met het hulpprogramma voor promotiebeheer.

In de volgende tabel worden de GUI-elementen en velden beschreven, die u kunt gebruiken om een nieuwe taak te maken:

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Veld	Beschrijving
Naam	De naam van de taak die u wilt maken.
Beschrijving	De beschrijving van de taak die u wilt maken.
Trefwoorden	De trefwoorden voor de inhoud van de taak die u wilt maken.
Taak opslaan in	De map die standaard is geselecteerd, wordt weergegeven.
Bronsysteem	De naam van het BI-platformsysteem van waaruit u een taak wilt verhogen.
Doelsysteem	De naam van het BI-platformsysteem waarnaar u een taak wilt verhogen.
Gebruikersnaam	De aanmeldings-id waarmee u zich moet aanmelden bij het bron- of doelsysteem.
Wachtwoord	Het wachtwoord waarmee u zich moet aanmelden bij het bron- of doelsysteem.
Verificatie	Het verificatietype waarmee de aanmelding bij het bron- of doelsysteem heeft plaatsgevonden. Het hulpprogramma voor promotiebeheer ondersteunt de volgende verificatietypen: • Enterprise • Windows AD • LDAP • SAP

> **Opmerking**
>
> Controleer voordat u een taak maakt dat de instellingen voor overschrijven, indien van toepassing, gewijzigd en bijgewerkt zijn op het doelsysteem zodat de BI-platforminhoud automatisch bijgewerkt wordt. Zie "De optie Instellingen overschrijven gebruiken" voor meer informatie.

Voer de volgende stappen uit als u een nieuwe taak wilt maken met het hulpprogramma Promotiebeheer:

1. Start het hulpprogramma voor promotiebeheer.
2. Klik in de startpagina van *Promotietaken* op *Nieuwe taak*.
3. Voer de naam, beschrijving en sleutelwoorden in voor de taak in de desbetreffende velden.

   > **Opmerking**
   >
   > Het verschaffen van informatie in de velden Beschrijving, Trefwoorden en Doelsysteem is optioneel.

4. Blader in het veld *Taak opslaan in* naar de map waarin u de taak wilt opslaan.

   > **Opmerking**
   >
   > Standaard wordt het veld *Taak opslaan in* ingevuld met de naam van de geselecteerde map in het mappenvenster voordat op *Nieuwe taak* geklikt wordt.

5. Selecteer het bronsysteem en het doelsysteem in de desbetreffende vervolgkeuzelijsten.

Indien de naam van het systeem niet wordt weergegeven in de vervolgkeuzelijsten, klikt u op de optie *Aanmelden bij een nieuwe CMS*. Er wordt een nieuw venster geopend. Voer de naam in van het systeem, samen met de gebruikersnaam en het wachtwoord.

6. Klik op *Maken*.
   Het venster "Objecten toevoegen" wordt weergegeven.
7. Selecteer de objecten in het bronsysteem die moeten worden toegevoegd aan de taak en klik op *Toevoegen en sluiten*.
8. Klik op *Opslaan*.

De zojuist aangemaakte taak wordt opgeslagen in de CMS-gegevensopslagruimte van het bronsysteem.

> **Opmerking**
>
> Als u een taak maakt met een map als het primaire object en het betreft een terugkerende taak, wordt de inhoud die aan e map wordt toegevoegd bij de volgende uitvoering in de taak opgenomen.

Verwante informatie

De optie Instellingen voor overschrijven gebruiken [pagina 594]

16.3.2.1 Aanmelden bij een nieuwe CMS

In deze sectie wordt beschreven hoe u zich bij een nieuwe CMS kunt aanmelden.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij het uitvoeren van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om u aan te melden bij een nieuwe CMS:

1. Start de toepassing voor promotiebeheer.
2. Maak een nieuwe taak aan.
   Zie Een taak maken [pagina 601] voor meer informatie over het aanmaken van een nieuwe taak.
3. Selecteer *Aanmelden bij nieuwe CMS* in de vervolgkeuzelijst *Bronsysteem*.
   Het dialoogvenster *Aanmelden bij systeem* wordt weergegeven.
4. Selecteer het systeem uit de vervolgkeuzelijst of voer een nieuwe systeemnaam in.
5. Voer de gebruikersreferenties in, selecteer het geschikte verificatietype en klik op *Aanmelden*.
6. Selecteer *Aanmelden bij nieuwe CMS* in de vervolgkeuzelijst *Doelsysteem*.
7. Selecteer het systeem uit de vervolgkeuzelijst of voer een nieuwe systeemnaam in.
8. Voer de gebruikersreferenties in, selecteer het geschikte verificatietype en klik op *Aanmelden*.

Verwante informatie

Een taak bewerken [pagina 605]
Een informatieobject toevoegen aan een taak [pagina 606]
Een taak verhogen wanneer gegevensopslagruimten verbonden zijn [pagina 609]
Een taakverhoging plannen [pagina 615]

16.3.3 Een nieuwe taak maken door een bestaande taak te kopiëren

In deze sectie wordt beschreven hoe u een nieuwe taak kunt maken door een bestaande taak te kopiëren.

> ⓘ Opmerking
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om een nieuwe taak aan te maken door een bestaande taak te kopiëren:

1. Start het hulpprogramma Promotiebeheer.
2. Klik in de startpagina van *Promotietaken* op *Nieuwe taak*.
3. Klik op de optie *Bestaande taak kopiëren*.
   Het venster *Een bestaande taak kopiëren* wordt weergegeven in de lijst met taken in de map *Promotietaken*.
4. Selecteer de vereiste taak in de lijst en klik op *Maken*.
   De naam, trefwoorden en beschrijving van de taak en de velden *Taak opslaan in* en *Doel* worden weergegeven. Wijzig deze velden zo nodig.
5. Blader in het veld *Taak opslaan in* naar de map waarin u de taak wilt opslaan en klik op *Maken*.

Een nieuwe taak wordt gemaakt en het venster *Objecten toevoegen* wordt weergegeven.

Verwante informatie

Een informatieobject toevoegen aan een taak [pagina 606]
Een taak bewerken [pagina 605]
Een taak verhogen wanneer gegevensopslagruimten verbonden zijn [pagina 609]

16.3.4 Een taak zoeken

Met de zoekfunctie in het hulpprogramma Promotiebeheer kunt u een taak zoeken die beschikbaar is in de gegevensopslagruimte.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om een taak te zoeken:

1. Geef de tekst op waarnaar u wilt zoeken in het veld *Zoeken* op de startpagina.
2. Klik op de lijst naast het veld *Zoeken* om de zoekparameters op te geven. U kunt de volgende zoekparameters opgeven:
   - *Titel zoeken*: met deze optie wordt gezocht naar een taak op naam.
   - *Trefwoord zoeken*: met deze optie wordt gezocht naar een taak op trefwoorden.
   - *Beschrijving zoeken*: met deze optie wordt gezocht naar een taak op beschrijving.
   - *Alle velden zoeken*: met deze optie kunt u zoeken naar een taak op titel, trefwoorden en beschrijving.
3. Klik op het pictogram Zoeken.

Verwante informatie

Een informatieobject toevoegen aan een taak [pagina 606]
Een taak bewerken [pagina 605]

16.3.5 Een taak bewerken

In deze sectie wordt het bewerken van een map beschreven.

> **Opmerking**
>
> - Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.
> - Het bewerken van een taak is niet hetzelfde als het maken van een nieuwe taak.

Voer de volgende stappen uit om een taak te bewerken:

1. Start het hulpprogramma Promotiebeheer.
2. Selecteer de taak die u wilt bewerken in de startpagina van *Promotietaken*.
3. Klik op *Bewerken*.
   De details van de geselecteerde taak worden weergegeven. Voeg InfoObjects toe of verwijder deze, beheer afhankelijkheden of verhoog de taak (zo nodig).

U kunt tijdens het bewerken van een taak niet de naam van het bronsysteem wijzigen.

Verwante informatie

Een informatieobject toevoegen aan een taak [pagina 606]

Een taak verhogen wanneer gegevensopslagruimten verbonden zijn [pagina 609]
Een taakverhoging plannen [pagina 615]

16.3.6 Een informatieobject toevoegen aan een taak

Elke taak moet een reeks InfoObjects omvatten. Daarom moet u InfoObjects aan een taak toevoegen voordat u deze naar het doelsysteem verhoogd.

> **Opmerking**
>
> - Wanneer u een Crystal Reports-rapport verhoogt op basis van Business Views InfoObjects (Gegevensverbinding, Gegevensverzameling, Business Element en Business View), moet u de beveiligingsgegevens (DataAccess-recht op Gegevensverbinding en het ViewDataField-recht op Gegevensverzameling en Business Elements) opnemen om gegevens in een rapport op het doelsysteem weer te geven.
> - Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om een InfoObject aan een taak toe te voegen:

1. Start het hulpprogramma voor promotiebeheer.
2. Maak een nieuwe taak aan of bewerk een bestaande taak.
   Zie Een taak maken [pagina 601] en Een taak bewerken [pagina 605] voor meer informatie over het maken van een nieuwe taak.
3. Klik op *Objecten toevoegen* wanneer u een taak bewerkt.

   > **Opmerking**
   >
   > Het dialoogvenster *Objecten toevoegen* wordt weergegeven bij het maken van een nieuwe taak.

4. Navigeer naar de map waarin u het InfoObject wilt selecteren.
   De lijst met InfoObjects in de geselecteerde map wordt weergegeven.
5. Selecteer het InfoObject dat u wilt toevoegen aan de taak en klik op *Toevoegen*.

   Als u een InfoObject wilt toevoegen en het dialoogvenster "Objecten van het systeem toevoegen: `<NAAM>`" wilt afsluiten, klikt u op *Toevoegen en sluiten*. Het InfoObject wordt aan de taak toegevoegd en het dialoogvenster wordt gesloten.

Nadat u een InfoObject hebt toegevoegd aan een taak, kunt u met de rechtermuisknop op de pagina *Taakweergave* klikken en promotieprocessen selecteren om de promotietaak voort te zetten. U kunt de afhankelijkheden van het InfoObject dat u hebt geselecteerd, beheren met behulp van de optie *Afhankelijkheden beheren* op de pagina *Taakweergave*.

> **Opmerking**
>
> - Het winkelwagentje dat in het linkervenster van de pagina *Taakweergave* wordt weergegeven, geeft de taak en de afhankelijkheden weer in een platte boomstructuur.
> - Klik na het toevoegen van informatieobjecten op de optie *Opslaan* om de wijzigingen op te slaan. De gebruiker wordt anders gevraagd om de taak op te slaan wanneer het tabblad wordt gesloten.

Aanbevolen procedure: Het is raadzaam om in SAP BusinessObjects slechts een klein aantal InfoObjects (niet meer dan 100 tegelijk) te selecteren voor promotie, om zo optimale prestaties van het hulpprogramma Promotiebeheer te verkrijgen.

Verwante informatie

De afhankelijkheden van een taak beheren [pagina 607]
Een taak verhogen wanneer gegevensopslagruimten verbonden zijn [pagina 609]
Een taakverhoging plannen [pagina 615]

16.3.7 De afhankelijkheden van een taak beheren

In deze sectie wordt beschreven hoe u de afhankelijkheden van een informatieobject kunt beheren.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om afhankelijkheden van een informatieobject te beheren:

1. Start het hulpprogramma voor promotiebeheer.
2. Maak een nieuwe taak aan of bewerk een bestaande taak.
   Zie Een taak maken [pagina 601] en Een taak bewerken [pagina 605] voor meer informatie over het maken van een nieuwe taak.
3. Voeg de vereiste InfoObjects aan de taak toe en sluit het dialoogvenster *Objecten toevoegen* om terug te keren naar het venster *Taakweergave*.
4. Klik op *Afhankelijkheden beheren*.
   Het venster *Afhankelijkheden beheren* wordt weergegeven. In dit venster wordt een overzicht weergegeven van de informatieobjecten en hun afhankelijkheden. Klik op *Niet-geselecteerde afhankelijke objecten weergeven* om alleen de afhankelijke objecten weer te geven die niet geselecteerd zijn.
5. Selecteer in de vervolgkeuzelijst *Afhankelijkheden selecteren* de opties waarmee u de gegroepeerde afhankelijkheden wilt toevoegen aan de taak. De afhankelijkheden worden niet standaard geselecteerd; u moet de afhankelijkheden die u wilt verhogen expliciet selecteren.

   Als u bijvoorbeeld *Alle universes* selecteert in de vervolgkeuzelijst *Afhankelijke objecten selecteren*, worden alle universes die in de lijst met afhankelijke objecten zijn opgenomen geselecteerd. U kunt ook de afhankelijkheden afzonderlijk selecteren.

   U kunt op het *Type* klikken om de ondersteunde filteropties voor de InfoObjects weer te geven. Er wordt een vervolgkeuzelijst weergegeven. In deze lijst worden de ondersteunde filteropties weergegeven. Selecteer de filteropties en klik op *OK*. De gefilterde informatieobjecten worden weergegeven.

   Wanneer u de afhankelijkheden selecteert in de kolom *Afhankelijkheden* en op *Wijzigingen toepassen* klikt, worden de afhankelijkheden automatisch verplaatst naar de kolom *Objecten in taak*.

U kunt ook de naam van het afhankelijke element invoeren in het veld *Afhankelijkheden zoeken* om een afhankelijk element te zoeken.

Zie Afhankelijkheden zoeken [pagina 608] voor meer informatie over het zoeken naar afhankelijkheden.

6. Klik op *Wijzigingen toepassen* om de lijst met afhankelijkheden bij te werken en klik op *Wijzigingen toepassen en sluiten* om de wijzigingen op te slaan.

Afhankelijke objecten worden automatisch berekend door het hulpprogramma. Deze afhankelijkheden worden berekend op basis van de relaties of de eigenschappen van de informatieobjecten. Afhankelijkheden die niet aan een van deze vereisten voldoen, worden niet berekend in deze versie van het hulpprogramma.

> **Opmerking**
>
> Als u een map selecteert om te verhogen, wordt de inhoud van de geselecteerde map beschouwd als primaire bron.

Verwante informatie

Een taak verhogen wanneer gegevensopslagruimten verbonden zijn [pagina 609]

16.3.8 Afhankelijkheden zoeken

Met de geavanceerde zoekfunctie in het hulpprogramma Promotiebeheer kunt u de afhankelijkheden vinden van InfoObjects die beschikbaar zijn in de gegevensopslagruimte.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om de afhankelijkheden van een informatieobject te zoeken:

1. Start promotiebeheer.
2. Maak een nieuwe taak aan of bewerk een bestaande taak.
   Als u een nieuwe taak hebt gemaakt, voegt u informatieobjecten toe aan de taak. Als u een bestaande taak bewerkt, kunt u zo nodig objecten toevoegen.
3. Klik op *Afhankelijkheden beheren*.
4. Geef in het veld *Afhankelijkheden zoeken* de naam op van het afhankelijke element dat u wilt vinden.
5. Klik op het pictogram Zoeken.

Verwante informatie

De afhankelijkheden van een taak beheren [pagina 607]

16.3.9 Een taak verhogen wanneer gegevensopslagruimten verbonden zijn

In deze sectie wordt beschreven hoe u een taak kunt verhogen van het bronsysteem naar het doelsysteem als beide systemen live zijn.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

De volgende tabel bevat de typen InfoObjects die kunnen worden verhoogd met het hulpprogramma voor promotiebeheer:

Categorie	Objecttypen die kunnen worden verhoogd
Rapporten	Crystal reports, Web Intelligence, QaaWS, Lumira
Externe objecten	Rich text, tekstdocument, Microsoft Excel, Microsoft Power Point, Microsoft word, Flash, Adobe Acrobat
Gebruikers	Gebruikers en gebruikersgroepen
Server	Servergroepen
Business Intelligence-platform	Map, Programma, Gebeurtenissen, Profielen, Objectpakket, Hyperlink, Categorieën, Document uit Postvak IN, map Persoonlijk en Favorieten
Univese, werkruimte, sets	Universes UNV, verbindingen, sets
EPM-dashboard	Universes, verbindingen, rapporten en analyses
BusinessView	DataFoundation
Federatie • Herhalingslijst • Herhalingstaken	Met Herhalingslijst worden de volgende objecten verhoogd: Flash, .txt, discussies, .pdf, hyperlink, .xls, ObjectPackage, Crystal Reports-rapporten, Web Intelligence-documenten, universes, programma, verbindingen, DataFoundation, Business View-weergaven, .rtf, profiel, gebeurtenis, gebruikers en gebruikersgroepen. Via Herhalingsverbindingen worden herhalingstaken, externe verbindingen, publicaties, discussies en Pioneer-verbindingen verhoogd.
BI-services	Web Intelligence-documenten, universes en verbindingen
Nieuwe InfoObjects	Crystal Reports-rapporten (rpt/rptr), Pioneer, DSL-universe (UNX), bedrijfslaag (BLX), verbinding (CNX), gegevensverzameling (DFX), Webl, Data Federator, Data Steward, BI-werkruimte, enz.
Tenants	Promotiebeheer ondersteunt het verhogen van tenants met de bijbehorende afhankelijkheden van het bron- naar het doelsysteem door opties te bieden voor het selecteren en toevoegen van tenants en corresponderende tenantobjecten aan een taak. Promotiebeheer brengt ook een relatie tot stand tussen tenants en de corresponderende tenantobjecten als afhankelijkheden. De functie werkt in GUI- en CLI-modus van promotiebeheer.

BI-commentaar wordt ondersteund in promotiebeheer. Als u een document met opmerkingen verhoogt, worden opmerkingen over het document ook gemigreerd van het bron- naar het doelsysteem (Live naar Live, Live naar BIAR, BIAR naar Live). Selecteer *Verhogen* > *Instellingen voor opmerkingen* en schakel het selectievakje *Opmerkingen opnemen* in om een document met opmerkingen te verhogen.

> **Opmerking**
>
> Het selectievakje *Opmerkingen opnemen* is standaard uitgeschakeld.

Als u gerepliceerde objecten verhoogt, wordt de replicatiespecifieke informatie geassocieerd met de objecten ook gemigreerd van het bron- naar het doelsysteem (Live naar Live, Live naar BIAR, BIAR naar Live). Selecteer, om een document zonder replicatiespecifieke informatie te verhogen, *Verhogen* > *Instellingen Federatietaken* en deselecteer het selectievakje *Federatietaakrelatie opnemen*.

> **Opmerking**
>
> Het selectievakje *Federatietaakrelatie opnemen* is standaard ingeschakeld.

Voer de volgende stappen uit om een taak te verhogen:

1. Start promotiebeheer.
2. Selecteer de gewenste taak op de startpagina van *Promotietaken*.
   U kunt ook met de rechtermuisknop op de startpagina en vervolgens op *Verhogen* klikken.
3. Selecteer indien nodig een ander doelsysteem uit de lijst met *doel*systemen.

   > **Opmerking**
   >
   > Zorg ervoor dat u bent aangemeld bij zowel de bron- als doelsystemen voordat u de promotieprocedure start.

4. Geef de gewenste waarde op in het veld *Wijziging beheer-id* en klik op *Opslaan*.

   > **Opmerking**
   >
   > De wijzigingsbeheer-id wordt gebruikt voor het verkrijgen van informatie met betrekking tot logboeken, controle en taakgeschiedenis. Met het hulpprogramma voor promotiebeheer kunt u elke poging tot het maken van een taak toewijzen aan een wijzigingsbeheer-id. De wijzigingsbeheer-id is een attribuut dat tijdens het maken van een nieuwe taak door de gebruiker wordt ingesteld in de taakdefinitie. Het hulpprogramma maakt automatisch een id aan voor elke taak.

5. Selecteer zo nodig *Beveiligingsinstellingen*. De volgende opties worden weergegeven:
   - *Beveiliging niet verhogen*: dit is de standaardoptie.
   - *Beveiliging verhogen*: gebruik deze optie om taken samen met de gekoppelde beveiligingsrechten te verhogen.
   - *Objectbeveiliging verhogen*: gebruik deze optie om de beveiliging van objecten en mappen te verhogen.
   - *Gebruikersbeveiliging verhogen*: hiermee kunt u de rechten verhogen van gebruikers die deel uitmaken van de taak.
   - *Inclusief toepassingsrechten*: u kunt deze optie alleen selecteren als u ook *Gebruikersbeveiliging verhogen* selecteert. Als de objecten in de taak toepassingsrechten erven, wordt de taak samen met deze rechten verhoogd.
   - *Beveiliging op hoogste niveau verhogen*: gebruik deze optie om de beveiligingsrechten op het hoogste niveau te verhogen.

     > **Let op**
     >
     > De beveiligingsoptie *Beveiliging op hoogste niveau verhogen* overschrijft de beveiligingsrechten op het hoogste niveau die in het doelsysteem zijn gedefinieerd.

U kunt ook op *Beveiliging weergeven* klikken om de beveiligingsafhankelijkheden van de InfoObjects in de taak weer te geven.

> **Opmerking**
>
> De knop *Beveiliging weergeven* is uitgeschakeld totdat u de nieuwe job opslaat.

6. Klik op *Opslaan*.

   De knop *Beveiliging weergeven* is ingeschakeld. U kunt nu beveiligingsafhankelijkheden weergeven.
7. Klik op *Verhogingstest* om te controleren of er geen conflicten bestaan tussen CUID's van InfoObjects op de bron- en doelsystemen. De verhogingsdetails worden op de tabbladen *Geslaagd*, *Mislukt* en *Waarschuwing* weergegeven. In de eerste kolom worden de te verhogen objecten weergegeven en in de tweede kolom wordt de verhogingsstatus van elk InfoObject weergegeven. Het hulpprogramma voor promotiebeheer ordent de geselecteerde objecten in gebruikers, groepen en universes.

   > **Opmerking**
   >
   > Met deze optie worden geen InfoObjects doorgevoerd voor verhoging.

   Het resultaat van een verhogingstest kan als volgt zijn:
   - `Overschreven` Het InfoObject op het doelsysteem wordt overschreven door het InfoObject op het bronsysteem.
   - `Gekopieerd` Het InfoObject op het bronsysteem wordt naar het doelsysteem gekopieerd.
   - `Verwijderd` Het InfoObject wordt niet verhoogd van het bronsysteem naar het doelsysteem.
   - `Waarschuwing` Het InfoObject op het doelsysteem is nieuwer en u kunt het InfoObject uit de taak verwijderen. Als u echter wilt verhogen, wordt het InfoObject verhoogd.
   - `Toegewezen` Het InfoObject wordt toegewezen aan een InfoObject op het doelsysteem.
8. Klik op *Plannen* als u de verhoging op een bepaalde tijd of volgens een terugkerende planning wilt uitvoeren.
9. Klik op *Verhogen*.
   De geselecteerde taak wordt verhoogd.

Als u de taak niet wilt verhogen, kunt u met de optie *Opslaan* de wijzigingen, zoals de instellingen voor beveiliging, gewijzigde beheer-id en planning, opslaan.

16.3.10 Een taak verhogen met een LCMBIAR-bestand

Verhogen verwijst naar de activiteit van het overdragen van een BI-bron van de ene gegevensopslagruimte naar de andere. Als de bron- en doelsystemen zich op hetzelfde netwerk bevinden, gebruikt het hulpprogramma Promotiebeheer WAN of LAN om het InfoObject te verhogen. Het hulpprogramma Promotiebeheer maakt het echter ook mogelijk InfoObjects te verhogen ook al bevinden zich de bron- en doelsystemen niet op hetzelfde netwerk.

In gevallen waarin de bron- en doelsystemen zich niet op hetzelfde netwerk bevinden, kunt u met het hulpprogramma Promotiebeheer taken naar het doelsysteem verhogen door een taak uit het bronsysteem naar een LCMBIAR-bestand te exporteren en daarna de taak uit het BIAR-bestand in het doelsysteem te importeren.

In deze sectie wordt beschreven hoe u een taak naar een LCMBIAR-bestand kunt exporteren en vervolgens de taak uit het BIAR-bestand kunt importeren naar het doelsysteem.

> ⓘ Opmerking
>
> - Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij het uitvoeren van acties. Zie3350454 voor meer informatie.
> - Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij het uitvoeren van acties. Zie 3350454 voor meer informatie.

Verwante informatie

Een taak exporteren naar een LCMBIAR-bestand. [pagina 612]
Een taak importeren uit een LCMBIAR-bestand [pagina 613]

16.3.10.1 Een taak exporteren naar een LCMBIAR-bestand.

In deze sectie wordt beschreven hoe u een taak kunt exporteren naar een LCMBIAR-bestand.

Voer de volgende stappen uit als u een taak wilt exporteren naar een LCMBIAR-bestand:

1. Start het hulpprogramma voor promotiebeheer en maak een nieuwe taak.

   Voor meer informatie over het maken van een nieuwe taak raadpleegt u Een taak maken [pagina 601]
2. Selecteer in de vervolgkeuzelijst *Doel* de optie *Uitvoer naar LCMBIAR-bestand* en klik op *Maken*.
3. Klik op *Objecten toevoegen* om informatieobjecten aan de taak toe te voegen.

   U kunt met de optie *Afhankelijkheden beheren* de afhankelijke elementen van de geselecteerde taak beheren.
4. Als u het bestand LCMBIAR wilt coderen met behulp van een wachtwoord, schakelt u het selectievakje *Wachtwoordcodering* in.
5. Geef een wachtwoord op in het veld *Wachtwoord*.
6. Geef het wachtwoord nogmaals op in het veld *Wachtwoord bevestigen*.
7. Klik op *Verhogen*.
   Het venster *Verhogen* wordt weergegeven.
8. Stel desgewenst overige beveiligingsopties in en klik op *Exporteren*.
   Het LCMBIAR-bestand wordt gemaakt. U kunt een LCMBAIR-bestand opslaan in het bestandssysteem.
9. (optioneel) Klik op *Doel van LCMBIAR-bestand* en selecteer *FTP* of *SFTP* om het LCMBIAR-bestand te exporteren naar een FTP-server of een SFTP-server. Voer de hostnaam, poort, gebruikersnaam, het wachtwoord, de map en bestandsnaam in klik op *Exporteren*.

   > ⓘ Opmerking
   >
   > Als u *SFTP* selecteert als *Doel van LCMBIAR-bestand*, moet u ook de SFTP-vingerafdruk invoeren.
10. Selecteer in de vervolgkeuzelijst *Doel* de optie *Uitvoer naar LCMBIAR-bestand* en klik op *Doel van LCMBIAR-bestand*.

U kunt de export van een taak naar een LCMBIAR-bestand plannen. Zie de sectie Een taakverhoging plannen [pagina 615] voor meer informatie hierover.

Verwante informatie

Een informatieobject toevoegen aan een taak [pagina 606]
De afhankelijkheden van een taak beheren [pagina 607]

16.3.10.2 Een taak importeren uit een LCMBIAR-bestand

U kunt een taak importeren uit een LCMBIAR-bestand. Het LCMBIAR-bestand wordt van het opslagapparaat naar het doelsysteem gekopieerd.

Voer de volgende stappen uit om een LCMBIAR-bestand te importeren:

1. Start het hulpprogramma voor promotiebeheer.
2. Klik op de startpagina van *Promotietaken* op *Importeren* > *Bestand importeren*.
   Het venster *Importeren uit bestand* wordt weergegeven.
3. U kunt een BIAR-bestand importeren uit het bestandssysteem of van een FTP- of SFTP-server.
   - Voer de volgende stappen uit om een BIAR-bestand uit het bestandssysteem te importeren:
     1. Selecteer *Bestandssysteem*.
     2. Klik op *Bladeren* en selecteer een LCMBIAR-bestand in het bestandssysteem.
     3. Voer het wachtwoord voor het LCMBIAR-bestand in het veld *Wachtwoord* in.

        > **Opmerking**
        > Het veld Wachtwoord wordt alleen weergegeven als het bestand LCMBIAR is versleuteld met een wachtwoord.

     4. Klik op *Maken*. De taak wordt aangemaakt.

        > **Opmerking**
        > Als er al een taak met dezelfde naam is, wordt de pop-up Opslaan bevestigen weergegeven. Klik op Ja om de bestaande taak te overschrijven; klik op Nee om een taak te maken met een nieuwe naam `jobname_copy<CURRENT_DATE_AND_TIME>`
   - Voer de volgende stappen uit om een LCMBIAR-bestand te importeren van een FTP-server:
     1. Selecteer *FTP*.
     2. Voer de details in voor de velden host, poort, gebruikersnaam, wachtwoord, map en bestandsnaam en klik op *OK*.
   - Voer de volgende stappen uit om een LCMBIAR-bestand te importeren van een SFTP-server:
     1. Selecteer *SFTP*.
     2. Voer de juiste gegevens in de velden host, poort, gebruikersnaam, wachtwoord, map, vingerafdruk en bestandsnaam in en klik op *OK*.

4. Klik op *Verhogen*.
   Het venster *Verhogen - Taaknaam* wordt weergegeven.
5. Selecteer het doelsysteem in de vervolgkeuzelijst *Doel*. Als u *Aanmelden bij een nieuwe CMS* selecteert, wordt u gevraagd om referenties op te geven. Bevestig de aanmeldingsgegevens van het doelsysteem.
6. Klik op *Verhogen* om de inhoud te promoveren naar het doelsysteem.

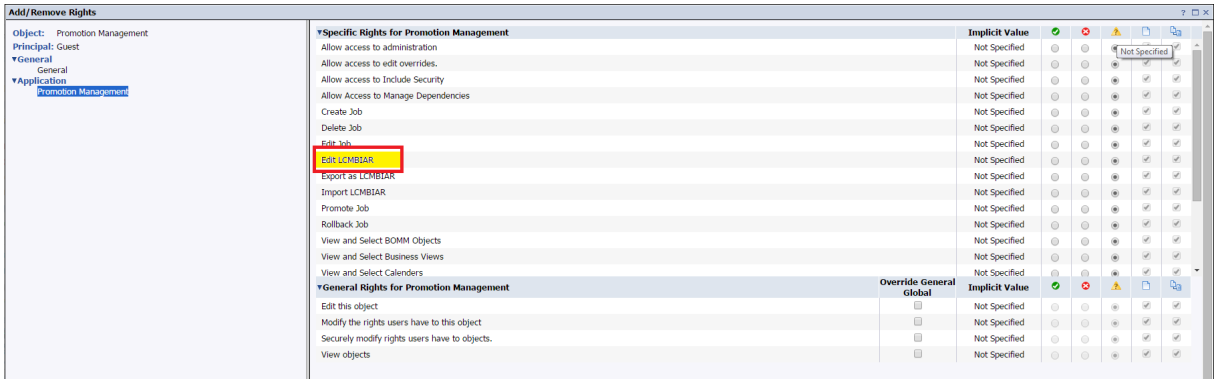
   U kunt ook dubbelklikken op de optie *Verhogen testen* om de objecten die u wilt verhogen en de promotiestatus weer te geven.
7. **Optioneel:** Als u een Web Intelligence-document importeert dat gebruikmaakt van aanpassing, controleert u op het tabblad *BI-voorkeuren gebruikersgroep* of *BI-voorkeuren gebruikersgroep overschrijven* is ingeschakeld, zodat de aanpassing kan worden geïmporteerd.

Verwante informatie

De afhankelijkheden van een taak beheren [pagina 607]

16.3.10.2.1 Selectief ophalen van objecten uit een LCMBIAR-bestand

Om selectief objecten te kunnen ophalen uit een LCMBIAR-bestand moet de gebruiker de bevoegdheid *LCMBIAR bewerken* hebben.



Voer de volgende handelingen uit om selectief objecten op te halen uit een LCMBIAR-bestand:

1. Selecteer de objecten die moeten worden verhoogd.
2. Klik op *Verhogen*.

> ⓘ Opmerking
>
> - Er wordt een nieuwe taak met de geselecteerde objecten gemaakt.
> - Dezelfde bewerking kan worden uitgevoerd met het opdrachtregelprogramma. Zie voor meer informatie Parameters opdrachtregelprogramma [pagina 628]
> - Selectieve verhoging wordt niet ondersteund voor het Live naar Live-scenario.

16.3.11 Een taakverhoging plannen

In deze sectie wordt beschreven hoe u de verhoging van een taak kunt plannen. Tevens wordt beschreven hoe u de terugkeeropties en -parameters kunt opgeven.

> ⓘ Opmerking
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij het uitvoeren van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om de verhoging van een taakexemplaar te plannen:

1. Klik in het dialoogvenster *Verhogen* op de optie *Plannen*.
2. Stel de gewenste optie in en klik op *Plannen*.

Als u InfoObjects aan een map in een taak toevoegt nadat de taak voor verhoging is gepland, worden deze ook op de geplande tijd naar het doel verhoogd. Dit is echter niet het geval wanneer u een promotie van een taak wilt plannen via een LCMBIAR-bestand, omdat LCMBIAR niet als 'werkelijke' destination wordt beschouwd.

> → Tip
>
> Nadat de verhoging van een taak is voltooid, kunt u alle exemplaren van de taak weergeven door de taak te selecteren op de pagina *Promotietaken* en op de werkbalk op *Geschiedenis* te klikken.

Promotie van een taak is ook mogelijk op basis van gebeurtenistriggers.

U kunt e-mailmeldingen selecteren op basis van taakpromotiestatus (zoals geslaagd/gedeeltelijk geslaagd/mislukt). Voor gedetailleerde informatie over de verschillende planningsopties en het configureren van uw meldingen, raadpleegt u de sectie Planning.

Verwante informatie

Een taak exporteren naar een LCMBIAR-bestand. [pagina 612]

16.3.11.1 Terugkerende en uitstaande taakpromoties bijwerken

Met het hulpprogramma voor promotiebeheer kunt u de status van promotietaakexemplaren traceren en deze exemplaren opnieuw plannen via de optie *Terugkerende en uitstaande exemplaren*.

Voer de volgende stappen uit om de status van promotietaakexemplaren te traceren en deze opnieuw te plannen:

1. Start het hulpprogramma voor promotiebeheer.
2. Selecteer een taak in de startpagina van *Promotietaak*.
3. Klik op *Geschiedenis*.
   Het venster *Taakgeschiedenis* wordt weergegeven.

4. Klik op *Terugkerende en uitstaande exemplaren*.
   Het venster *Taakgeschiedenis voor terugkerende en uitstaande exemplaren* wordt weergegeven. In dit venster wordt de lijst met terugkerende en uitstaande promotietaakexemplaren weergegeven.

   Indien nodig kunt u gebruikmaken van de volgende opties:
   - Klik op *Verhoogde exemplaren* om de lijst met verhoogde taakexemplaren weer te geven.
   - Klik op de optie *Onderbreken* om het geselecteerde uitstaande of terugkerende exemplaar te onderbreken.
   - Klik op de optie *Hervatten* om het onderbroken geplande promotietaakexemplaar te hervatten.
   - Klik op de optie *Opnieuw plannen* om het geselecteerde promotietaakexemplaar opnieuw te plannen.
   - Klik op om het geplande promotietaakexemplaar te verwijderen.
   - Klik op om de status van het geplande promotietaakexemplaar te vernieuwen.
   - U kunt de optie 1 gebruiken om door één pagina te navigeren, of naar een bepaalde pagina te navigeren door het desbetreffende paginanummer in te voeren.

   > **Opmerking**
   >
   > In de statuskolom van het venster *Taakgeschiedenis voor terugkerende en uitstaande exemplaren* wordt de status van het promotietaakexemplaar weergegeven, zoals terugkerend, uitstaand, enzovoort.

Verwante informatie

Een taak terugzetten [pagina 617]

16.3.12 De geschiedenis van een taak weergeven

In deze sectie wordt beschreven hoe u de geschiedenis van een taak kunt weergeven.

> **Opmerking**
>
> Als u de geschiedenis van een taak wilt weergeven, moet u ervoor zorgen dat de status van de taak een van deze opties is:
>
> - Geslaagd
> - Mislukt
> - Gedeeltelijk geslaagd

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om de geschiedenis van een taak te bekijken:

1. Start het hulpprogramma voor promotiebeheer.
   De startpagina *Promotietaken* wordt weergegeven.
2. Selecteer de taak waarvoor u de geschiedenis wilt weergeven, en klik op het tabblad *Geschiedenis*.

   De tijd van het taakexemplaar, de naam van de taak, de namen van de bron- en doelsystemen, de id van de gebruiker die de taak heeft verhoogd en de status (Geslaagd, Mislukt, of Gedeeltelijk geslaagd) van de taak worden weergegeven.

   U kunt de gedetailleerde status van de taak weergeven met behulp van de koppeling die in de kolom *Status* wordt weergegeven.

16.3.13 Een taak terugzetten

Met de optie Terugzetten kunt u de vorige status van het doelsysteem herstellen nadat een taak is verhoogd.

> **Opmerking**
>
> Beveiligingsuitbreidingen worden geïmplementeerd in de promotiebeheertool, wat leidt tot wijzigingen van bepaald gedrag bij de uitvoer van acties. Zie3350454 voor meer informatie.

Voer de volgende stappen uit om een taak terug te zetten:

1. Start het hulpprogramma voor promotiebeheer.
   De startpagina *Promotietaken* wordt weergegeven.
2. Voer een van de volgende handelingen uit:
   - Klik met de rechtermuisknop op de taak die u terug wilt zetten en selecteer *Terugzetten*.
   - Selecteer de taak die u wilt terugzetten en klik op het tabblad *Terugzetten*.

   Het venster *Terugzetten* wordt weergegeven.
3. Selecteer het exemplaar dat u wilt terugzetten en klik op *Volledig terugzetten*.
   Het exemplaar wordt teruggezet.

U kunt alleen het meest recente exemplaar van een promotietaak terugzetten. Het tegelijkertijd terugzetten van meerdere taakexemplaren is niet mogelijk.

16.3.13.1 De optie Gedeeltelijk ongedaan maken gebruiken

Met het hulpprogramma voor promotiebeheer kunt u de InfoObjects in een taak volledig of gedeeltelijk ongedaan maken in het doelsysteem.

Voer de volgende stappen uit om InfoObjects gedeeltelijk ongedaan te maken:

1. Start het hulpprogramma voor promotiebeheer.
   De startpagina *Promotietaken* wordt weergegeven.
2. Voer een van de volgende handelingen uit:
   - Klik met de rechtermuisknop op de taak die u ongedaan wilt maken en klik op *Ongedaan maken*.

- Selecteer de taak die u wilt terugzetten, en klik op het tabblad *Terugzetten*.

Het venster *Terugzetten* wordt weergegeven.

3. Selecteer het exemplaar in de lijst en klik op *Gedeeltelijk terugzetten*.

   De lijst met InfoObjects in de geselecteerde taak wordt op de pagina *Taakweergave* getoond.

4. Selecteer de InfoObjects die u ongedaan wilt maken, en klik op *Ongedaan maken*.

> **Opmerking**
>
> Zorg ervoor dat alle InfoObjects in een exemplaar zijn teruggezet voordat u InfoObjects in het volgende exemplaar terugzet.

> **Let op**
>
> Indien een taak is verhoogd met beveiliging, wordt tijdens het gedeeltelijk ongedaan maken van InfoObjects, de beveiliging van de geselecteerde afhankelijke InfoObjects mogelijk niet naar de vorige status hersteld.

Verwante informatie

Verschillende versies van BI-bronnen beheren [pagina 681]

16.3.13.2 Een taak terugzetten nadat het wachtwoord verloopt

In deze sectie wordt beschreven hoe u een taak terugzet nadat het wachtwoord is verlopen dat werd gebruikt om het de taak verhogen.

Voer de volgende stappen uit om taken terug te zetten nadat het wachtwoord is verlopen:

1. Selecteer de taak die u wilt terugzetten en klik op *Terugzetten*.
2. Selecteer *Volledig terugzetten* in het venster *Terugzetten*.
   Er wordt een foutbericht weergegeven. Het bericht geeft aan dat de taak niet teruggezet kan worden. U wordt ook gevraagd u aan te melden bij het bron- of doelsysteem.
3. Voer de nieuwe aanmeldingsgegevens in en klik op *Aanmelden*.

Er wordt een dialoogvenster weergegeven waarin wordt aangeduid dat het proces voor terugzetten is voltooid.

> **Opmerking**
>
> De taken die zijn verhoogd met behulp van de referenties voor bron- of doelsysteem, worden automatisch bijgewerkt.

Verwante informatie

InfoObjects gedeeltelijk terugzetten nadat het wachtwoord verloopt [pagina 619]
De optie Gedeeltelijk ongedaan maken gebruiken [pagina 617]

16.3.13.2.1 InfoObjects gedeeltelijk terugzetten nadat het wachtwoord verloopt

In deze sectie wordt beschreven hoe u InfoObjects gedeeltelijk kunt terugzetten nadat het wachtwoord voor het bron- of doelsysteem is verlopen.

Voer de volgende stappen uit om InfoObjects gedeeltelijk terug te zetten nadat het wachtwoord is verlopen:

1. Selecteer de taak die u wilt terugzetten en klik op *Terugzetten*.
   Het venster *Terugzetten* wordt weergegeven.
2. Selecteer de optie *Gedeeltelijk terugzetten*.
   Er wordt een foutbericht weergegeven. Het bericht geeft aan dat de InfoObjects niet kunnen worden teruggezet. U wordt ook gevraagd u aan te melden bij het bron- of doelsysteem.
3. Voer de nieuwe aanmeldingsgegevens in en klik op *Aanmelden*.
   De pagina *Taakweergave* wordt weergegeven. In deze pagina wordt de lijst met InfoObjects weergegeven.
4. Selecteer de gewenste InfoObjectsen klik op *Terugzetten*.

> **Opmerking**
>
> De taken die zijn verhoogd met behulp van de referenties voor bron- of doelsysteem, worden automatisch bijgewerkt.

Verwante informatie

Een taak terugzetten [pagina 617]
De optie Gedeeltelijk ongedaan maken gebruiken [pagina 617]
Een taak terugzetten nadat het wachtwoord verloopt [pagina 618]

16.4 Inhoud van volledige gegevensopslagruimte verhogen met het hulpprogramma voor Promotiebeheer

Als u de inhoud van een gegevensopslagruimte wilt verhogen, zijn de juiste planning, voorbereidingen en voldoende tijd vereist. In deze sectie worden de acties beschreven die zijn vereist voor verhoging van inhoud van een implementatie naar een andere.

16.4.1 Bron- en doelsystemen voorbereiden

Zorg ervoor dat de bron- en doelsystemen optimaal zijn geconfigureerd voordat u inhoud verhoogt.

1. Voer de volgende acties uit in het bronsysteem:
   a. Gebruik het hulpprogramma voor gegevensopslagruimten (RDT) om het bronsysteem te scannen en herstellen en corrigeer alle inconsistenties in gegevensopslagruimte en FRS. Zie *Gebruikershandleiding voor het hulpprogramma voor gegevensopslagruimte van Business Intelligence-platform* voor meer informatie over RDT.
   b. Minimaliseer systeemgebruik in het bronsysteem om ervoor te zorgen dat wijzigingen beperkt blijven tijdens verhoging. Bij actieve systeem kunnen er objectfouten optreden.

   > ⓘ Opmerking
   >
   > Als er fouten optreden, controleert u de taakstatus om eventuele problemen op te lossen.

2. Voer de volgende acties uit in het doelsysteem:
   a. Gebruik de sleutelcode van de licentie om ervoor te zorgen dat de juiste en voldoende licenties worden ingesteld in het doelsysteem.

   > ⓘ Opmerking
   >
   > Als u wilt voorkomen dat er fouten optreden tijdens verhoging van inhoud door ontbrekende licenties, gebruikt u identieke licentiëring voor beide systemen.

   b. Als u verificatiemethoden van derden gebruikt, configureert u deze optie en schakelt u deze in voor het doelsysteem voordat u inhoud verhoogt.

   > ⓘ Opmerking
   >
   > Wijs geen gebruikers of gebruikersgroepen toe. Hierdoor worden gebruikers of gebruikersgroepen gemaakt in het doelsysteem met verschillende CUID's. Tijdesn verhoging worden CUID's gebruikt om objecten te identificeren en toe te wijzen tussen bron- en doelsysteem. Als u gebruikers en gebruikersgroepen toewijst, komt de inhoud niet meer overeen en treden verhogingsfouten op.

   c. Zorg ervoor dat alle vereiste invoegtoepassingen in het bronsysteem ook zijn geïnstalleerd in het doelsysteem.

   > ⓘ Opmerking
   >
   > Installeer invoegtoepassingen zoals Analysis of Design Studio in het bronsysteem om ervoor te zorgen dat gegevens juist worden gemigreerd.

   d. Als u inhoud met QaaWS-verbindingen hebt, schakelt u de overrides in om ervoor te zorgen dat deze verbindingen de juiste webservices aanwijzen. Zie de sectie “Overrides” voor meer informatie over het instellen van overrides.
   e. Klik op *Voltooide exemplaren weergeven op de pagina Afhankelijkheden beheren* in de *Taakinstellingen* in Promotiebeheer.
3. Voer de volgende acties uit in het centrale systeem:
   a. U kunt het bronsysteem, het doelsysteem of een afzonderlijke systeem aanwijzen als het centrale systeem waarin de taken voor Promotiebeheer worden uitgevoerd. Als u een volledige gegevensopslagruimte verhoogt, werkt u met een grote hoeveelheid inhoud waarvoor aanvullende

systeembronnen zijn vereist in het centrale systeem. Gebruik de volgende informatie om het centrale systeem te configureren voor 10.000 objecten:

	Toewijzing tijdelijke ruimte	Geheugentoewijzing	Aanvullende configuratie
`LCM_CLI`	2 GB	2 GB	Werk het bestand `LCM_CLI.bat` bij en wijzig de parameter `-Xmx`.
Job Server Promotiebeheer	3 GB	3 GB	Voeg de parameter `-javaargs Xmx3g` toe in de CMC om de Job Server Promotiebeheer juist te starten. Raadpleeg SAP Note 2286419 voor meer informatie.

Bijvoorbeeld: als de taak naar schatting 50.000 objecten bevat:

- Wijs 10 GB aan geheugen toe aan `LCM_CLI` (50.000 ÷ 10.000 × 2)
- Wijs 15 GB aan geheugen toe aan de Job Server (50.000 ÷ 10.000 × 3)

> **Opmerking**
>
> Deze richtlijnen zijn van toepassing op de meeste omgevingen. De grootte van documenten heeft mogelijk wel gevolgen voor bronvereisten.

16.4.2 Migratiestrategieën

- Gebruik de opdrachtregelinterface (CLI) en niet het webhulpprogramma voor de CMC voor alle taakverhogingen.
  - De CLI overschrijdt de websessielimiet van twintig minuten tijdens een verhogingstaak voor meer dan 1.000 objecten.

    > **Opmerking**
    >
    > Voor de objectlimiet zijn voldoende systeembronnen vereist.

  - Met de CLI hebben gebruikers meer controle over inhoudverhoging met querytaal om de te migreren inhoud te selecteren. U kunt inhoud van hetzelfde type selecteren of inhoud die zich in dezelfde map bevindt.
  - De CLI kan in batches worden uitgevoerd en verhogingstaken kunnen worden gestart met andere scripthulpprogramma's.
- Stel de beveiliging in door eerst de principals (gebruikers en gebruikersgroepen) te verhogen.
  - Als u eerst de gebruikers en gebruikersgroepen verhoogt, blijft het beveiligingsmodel in het doelsysteem behouden en kan persoonlijke gebruikersinhoud (Postvak IN, Favorieten, persoonlijke categorieën) later ook worden gemigreerd.

> **Opmerking**
>
> Het is belangrijk dat u deze taak eerst uitvoert zodat de CUID's van de gebruikers en de gebruikersgroepen in het doelsysteem overeenkomen met de CUID's in het bronsysteem.

- Afhankelijkheidsberekening uitschakelen.
  - Afhankelijkheidsberekening is een van de meest intensieve taken bij het maken van een taak. Als de volledige gegevensopslagruimte wordt gemigreerd, worden alle objecten gemigreerd en is berekening niet nodig.

    > **Opmerking**
    >
    > Deze functie is alleen handig als u niet zeker weet welke afhankelijke objecten zijn vereist.

- Zorg ervoor dat u beveiligingsberekening zo min mogelijk uitvoert.
  - Beveiligingsberekening is de op een na intensiefste taak bij het maken van een taak. Splits de verhoging op in twee taken als u veel documenten in verschillende mappen hebt en beveiliging alleen is ingesteld in de mappen. De eerste taak moet alleen objecten bevatten waarvoor beveiliging is ingeschakeld en de tweede taak moet alleen objecten bevatten waarvoor beveiliging is uitgeschakeld. Op deze manier kunt u beveiligingsberekeningen alleen uitvoeren voor de mappen en voorkomt u dat deze berekeningen worden uitgevoerd voor alle documenten.

    > **Opmerking**
    >
    > De objectbeveiliging blijft behouden omdat deze wordt overgenomen uit de mapbeveiliging.

16.5 Stappen volledige systeemverhoging

Voor een volledige systeemverhoging moeten drie afzonderlijke verhogingstaken opeenvolgend worden uitgevoerd waarbij met elke taak bepaalde inhoudtypen worden verhoogd. Zie Knowledge Base Article 1969259 voor meer informatie over het doorgeven van meerdere objecten.

In de volgende tabel worden de inhoudtypen en parameterinstellingen beschreven voor elke verhogingstaak.

Promotietaak	Inhoudstype	`exportDependencies`	`includeSecurity`
1	Alle gebruikers en gebruikersgroepen	false	true
2	Alle afhankelijke objecten	false	true
3	Alle primaire objecten	false	true

Gebruik de opdrachtregelinterface (CLI) om elke taak te maken en uit te voeren. Zie de sectie De optie Opdrachtregel gebruiken [pagina 626] voor meer informatie over de CLI.

Algemene parameters

Gebruik de volgende parameters voor alle drie verhogingstaken:

> → Onthouden
>
> Zorg ervoor dat elke parameter op een nieuwe regel staat.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

16.5.1 Gebruikers en gebruikersgroepen (taak 1)

Als u identieke beveiligingsmodellen tot stand wilt brengen tussen bron- en doelsystemen en ervoor wilt zorgen dat de object-CUID's van gebruikers en gebruikersgroepen identiek zijn, verhoogt u eerst de gebruikers en gebruikersgroepen.

1. Maak het bestand `usersandgroups.properties` met de algemene parameters en voeg de volgende parameters toe aan het bestand om alle gebruikers en gebruikersgroepen te selecteren:

   ```
   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. Om de taak uit te voeren, navigeert u naar de map `<INSTALLDIR>\win64x64\scripts` en voert u de volgende opdracht uit:

   ```
   Lcm_cli.bat –lcmproperties=usersandgroups.properties
   ```

16.5.2 Afhankelijke objecten verhogen (taak 2)

Afhankelijke objecten zijn afhankelijk van de primaire objecten in de openbare map en in de map Favorieten van de gebruiker. Als u wilt dat de optie `includeDependencies` niet meer hoeft te worden ingesteld op `true` voor alle andere taken, verhoogt u de afhankelijke objecten als tweede. Onderstaande objecten zijn afhankelijke objecten:

- Toegangsniveaus

- Toepassingen
- Business Views
- Agenda's
- Categorieën
- Verbindingen
- Gebeurtenissen
- OLAP-verbindingen
- Profielen
- Projecten
- QaaWS
- Externe verbindingen
- Herhalingslijsten
- Servergroepen
- Universes

1. Maak het bestand dependencies.properties met de algemene parameters en voeg de volgende parameters toe aan het bestand om alle afhankelijke objecten te selecteren:

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
```

```
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. Om de taak uit te voeren, navigeert u naar de map `<INSTALLDIR>\win64x64\scripts` en voert u de volgende opdracht uit:

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

16.5.3 Primaire objecten verhogen (taak 3)

Primaire objecten zijn BI-kerndocumenten die zich in de openbare map en de map Favorieten van de gebruiker bevinden. Ervan uitgaande dat de tweede verhogingstaak al is uitgevoerd, wordt bij het migreren van alle afhankelijke objecten door het afsluitend verhogen van primaire objecten hun relatie met afhankelijke objecten hersteld.

1. Maak het bestand `primaryobjects.properties` met de algemene parameters en voeg de volgende parameters toe aan het bestand om alle gebruikers en gebruikersgroepen te selecteren:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

   Als u dezelfde taak opnieuw uitvoert, sluit u de LCM-taak uit met behulp van de volgende query:

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. Om de taak uit te voeren, navigeert u naar de map `<INSTALLDIR>\win64x64\scripts` en voert u de volgende opdracht uit:

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> **ⓘ Opmerking**
>
> Als de openbare map of de map Favorieten van de gebruiker meer dan 50.000 objecten bevatten, moet deze laatste taak mogelijk in kleinere taken worden gesplitst.

> **ⓘ Opmerking**
>
> Zorg ervoor dat de computers waarop de opdrachtregelinterfaceopdracht en de Job Server voor promotiebeheer worden uitgevoerd voldoen aan de eisen m.b.t. grootte. Zie de sectie “Aanpassen” voor meer informatie.

16.5.4 Na verhoging

Met Promotiebeheer worden alleen servergroepen verhoogd maar niet de bijbehorende servers. Als u wilt dat rapporten met toegewezen servers blijven werken, maakt u de servers opnieuw en wijst u deze toe aan de juiste servergroepen.

16.6 De optie Opdrachtregel gebruiken

Met de optie Opdrachtregel van het hulpprogramma promotiebeheer kunt u objecten van de ene BI-platformimplementatie verhogen naar een andere. U kunt een batchscript voor meerdere taken maken.

> **→ Tip**
>
> Gebruik de optie Opdrachtregel voor taken die een groot aantal objecten bevatten.

Het hulpprogramma voor promotiebeheer ondersteunt de volgende typen taakpromotie via de opdrachtregel:

- Een bestaande promotietaaksjabloon exporteren naar LCMBIAR met wachtwoordcodering
- Een bestaande promotietaaksjabloon exporteren naar LCMBIAR zonder wachtwoordcodering
- Eén of meer platformquery's exporteren
- Meerdere platformquery's verhogen
- Verhogen met een bestaande taaksjabloon
- Een bestaand LCMBIAR-bestand importeren en verhogen
- Live-to-Live-promotie uitvoeren

16.6.1 Het hulpprogramma voor opdrachtregels in Windows uitvoeren

Voer de volgende stappen uit om de optie Opdrachtregel uit te voeren:

1. Open een venster of shell van de opdrachtregel.
2. Navigeer naar de relevante map.

   Het mappad voor Windows is bijvoorbeeld `C:\Programmabestanden (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Voer een van de volgende handelingen uit:
   - Voer het LCMCLI-bestand uit en zorg ervoor dat het Java-pad is ingesteld voordat het programma wordt uitgevoerd.
     Opdracht: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <eigenschappenbestand>`
   - Voer het BAT-bestand uit via `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat`
     Opdracht: `lcm_cli.bat -lcmproperty <eigenschappenbestand>`

     > **Opmerking**
     >
     > Voer de geldige wachtwoorden in wanneer u daarom gevraagd wordt.

Het hulpprogramma voor de opdrachtregel van promotiebeheer gebruikt een `<eigenschappen>`bestand als parameter. Het bestand `<.properties>` bevat de vereiste parameters voor communicatie met het hulpprogramma Promotiebeheer over de uit te voeren acties, de verbinding met een bepaalde BI-platformimplementatie, verbindingsmethoden, te verhogen objecten enz.

Het bestand moet de volgende notatie hebben: `<BESTANDSNAAM>.properties`

Bijvoorbeeld: `<MijnEigenschappen.properties>`

16.6.2 Het hulpprogramma voor opdrachtregels in Unix uitvoeren

Voer de volgende stappen uit om de optie Opdrachtregel uit te voeren:

1. Start shell.
2. Navigeer naar de relevante map.

   Bijvoorbeeld`/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. Voer een van de volgende handelingen uit:
   - Voer het LCMCLI-bestand uit en zorg ervoor dat het Java-pad is ingesteld voordat het programma wordt uitgevoerd.
     Opdracht: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <eigenschappenbestand>`
   - Voer het BAT-bestand uit via `<installatiemap_pad>\sap_bobj\lcm_cli.sh`
     Opdracht: `lcm_cli.sh -lcmproperty <eigenschappenbestand>`

     > **Opmerking**
     >
     > Voer de geldige wachtwoorden in wanneer u daarom gevraagd wordt.

16.6.3 Parameters van opdrachtregelprogramma

De opdrachtregelparameters voor de opdrachtregeloptie van het hulpprogramma voor promotiebeheer worden volgens drie hoofdverhogingstypen georganiseerd:

- Objecten uit een LCMBIAR-bestand naar een live CMS verhogen
- Objecten uit een live bron-CMS naar een live doel-CMS verhogen
- Objecten uit een live CMS naar een LCMBIAR-bestand exporteren.

Naast de parameters waarop deze drie verhogingstypen betrekking hebben, zijn er ook parameters voor algemene opdrachten die in alle verhogingsscenario's kunnen worden gebruikt.

> → Onthouden
>
> Zet opdrachtregelparameters niet tussen aanhalingstekens.

> ⓘ Opmerking
>
> - Net als bij het maken van een taak vóór exporteren wordt met de optie Opdrachtregel een tijdelijke taak gemaakt tijdens runtime. Deze taaknaam kan een combinatie van `Query_<GEBRUIKER>_<Tijdstempel>` zijn. Dit is alleen specifiek voor `<exportQuery>`.
> - U kunt de taak alleen terugzetten via het hulpprogramma voor promotiebeheer. Het terugdraaien van taken met behulp van opdrachtregels wordt niet ondersteund.
> - Wanneer u met een groot aantal objecten werkt, verdient het aanbeveling de maximale Java-heapgrootte te verhogen door de parameter `-Xmx=8g` in te stellen in het script `LCMCLI`.

Verwante informatie

LCMBIAR-bestand naar een live CMS [pagina 632]
Live bron-CMS naar live doel-CMS [pagina 639]
Live CMS naar een LCMBIAR-bestand [pagina 635]
Lijst met alle opdrachtregelparameters [pagina 643]

16.6.3.1 Opdrachtregelparameters op promotiescenario

De opdrachtregelparameters worden in de aanbevolen volgorde voor elk promotiescenario gepresenteerd. De tabel geeft alle beschikbare parameters aan en hun status als verplicht of optioneel voor elk promotiescenario. Elke verplichte parameter wordt beschreven voor het overeenkomstige promotiescenario ervan. De optionele parameters worden in de sectie Lijst met alle opdrachtregelparameters beschreven. Raadpleeg de Verwante koppelingen voor alle parameterinformatie op scenario en de beschikbare aanvullende parameters.

Parametergroep	Parameter	LCMBIAR naar Live	Live naar LCMBIAR	Live naar Live	Terug-zetten
Eigenschappenbestand	`lcmproperty`	Optioneel	Aanbevolen	Aanbevolen	Aanbevo-len
Actietype	`action`	Verplicht actie=verhogen	Verplicht action=exporteren	Verplicht actie=verhogen	Verplicht actie=te-rugzetten
LCM-knooppunt	`LCM_CMS`	Verplicht			
	`LCM_userName`	Verplicht			
	`LCM_Password`	Verplicht Indien dit leeg is, is het vereist het in de console.			
	`LCM_authentication`	Optioneel: Standaard = `secEnterprise`			
	`LCM_SystemID`	Alleen verplicht voor SAP-verificatie			
	`LCM_ClientID`	Alleen verplicht voor SAP-verificatie			
Bron (Live of LCMBIAR)	`importLocation`	Verplicht	Niet van toepassing	Niet van toepassing	Niet van toepas-sing
	`lcmbiarpassword`	Verplicht (mag leeg zijn)	Niet van toepassing	Niet van toepassing	Niet van toepas-sing
	`Source_CMS`	Niet van toepassing	Verplicht	Verplicht	Niet van toepas-sing
	`Source_UserName`	Niet van toepassing	Verplicht	Verplicht	Niet van toepas-sing
	`Source_password`	Niet van toepassing	Verplicht Indien dit leeg is, is het vereist het in de console.	Verplicht Indien dit leeg is, is het vereist het in de console.	Niet van toepas-sing
	`Source_authentication`	Niet van toepassing	Optioneel Standaard = `secEnterprise`	Optioneel Standaard = `secEnterprise`	Niet van toepas-sing

Parametergroep	Parameter	LCMBIAR naar Live	Live naar LCMBIAR	Live naar Live	Terug-zetten
	`Source_systemID`	Niet van toepassing	Alleen verplicht voor SAP-verificatie	Alleen verplicht voor SAP-verificatie	Niet van toepassing
	`Source_clientID`	Niet van toepassing	Alleen verplicht voor SAP-verificatie	Alleen verplicht voor SAP-verificatie	Niet van toepassing
Doel (Live of LCMBIAR)	`Destination_CMS`	Verplicht	Niet van toepassing	Verplicht	Niet van toepassing
	`Destination_username`	Verplicht	Niet van toepassing	Verplicht	Niet van toepassing
	`Destination_password`	Verplicht	Niet van toepassing	Verplicht	Niet van toepassing
	`Destination_authentication`	Optioneel Standaard = `secEnterprise`	Niet van toepassing	Optioneel Standaard = `secEnterprise`	Niet van toepassing
	`Destination_systemID`	Alleen verplicht voor SAP-verificatie	Niet van toepassing	Alleen verplicht voor SAP-verificatie	Niet van toepassing
	`Destination_clientID`	Alleen verplicht voor SAP-verificatie	Niet van toepassing	Alleen verplicht voor SAP-verificatie	Niet van toepassing
	`ExportLocation`	Niet van toepassing	Verplicht	Niet van toepassing	Niet van toepassing
	`lcmbiarpassword`	Niet van toepassing	Verplicht (mag leeg zijn)	Niet van toepassing	Niet van toepassing
Taakgerelateerd	`JOB_CUID`	Niet van toepassing	Optioneel	Optioneel	Verplicht
	`Override`	Optioneel	Niet van toepassing	Niet van toepassing	Niet van toepassing

Parametergroep	Parameter	LCMBIAR naar Live	Live naar LCMBIAR	Live naar Live	Terug-zetten
	`forceOverride` Beschikbaar in SP4	Optioneel	Niet van toepassing	Niet van toepassing	Niet van toepas-sing
	`Timeout` Beschikbaar in SP4	Optioneel	Niet van toepassing	Optioneel	Niet van toepas-sing
Exportgerelateerd	`ExportDependencies`	Niet van toepassing	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
	`ExportQuery`	Niet van toepassing	Verplicht	Verplicht	Niet van toepas-sing
	`ExportQueriesTotal`	Niet van toepassing	Optioneel: Gebruik wanneer u meer dan één exportquery hebt	Optioneel: Gebruik wanneer u meer dan één exportquery hebt	Niet van toepas-sing
	`BatchJobQuery`	Niet van toepassing	Optioneel: Gebruik met exportquery	Optioneel: Gebruik met exportquery	Niet van toepas-sing
	`LimitQueryBatchSize`	Niet van toepassing	Optioneel	Optioneel	Niet van toepas-sing
Logboekgerelateerd	`Consolelog`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
	`ResultFileName`	Optioneel	Optioneel	Optioneel	Niet van toepas-sing
	`LogFileName` Beschikbaar in SP4	Optioneel	Optioneel	Optioneel	Niet van toepas-sing
Objectselectie	`Selected_CUIDS`	Optioneel	Niet van toepassing	Niet van toepassing	Niet van toepas-sing
	`selectUser` Beschikbaar in SP4	Niet van toepassing	Optioneel Standaard=`All`	Optioneel Standaard=`All`	Niet van toepas-sing

Parametergroep	Parameter	LCMBIAR naar Live	Live naar LCMBIAR	Live naar Live	Terug-zetten
	`selectGroup` Beschikbaar in SP4	Niet van toepassing	Optioneel Standaard=`All`	Optioneel Standaard=`All`	Niet van toepas-sing
Beveiliging	`IncludeApplicationSecurity`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
	`IncludeSecurity`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
	`IncludeTopLevelSecurity`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
Opmerkingen	`IncludeComments`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Optioneel Standaard = `False`	Niet van toepas-sing
Federatietaken	`IncludeFederationJobsRelationship`	Optioneel Standaard = `True`	Niet van toepassing	Optioneel Standaard = `True`	Niet van toepas-sing

Verwante informatie

LCMBIAR-bestand naar een live CMS [pagina 632]
Live CMS naar een LCMBIAR-bestand [pagina 635]
Live bron-CMS naar live doel-CMS [pagina 639]
Lijst met alle opdrachtregelparameters [pagina 643]

16.6.3.2 LCMBIAR-bestand naar een live CMS

Wanneer u objecten van een LCMBIAR-bestand naar een live CMS verhoogt, refereert u aan een eigenschappenbestand vanaf de opdrachtregel die de verhogingsopdracht als volgt specificeert:

- Importlocatie en het type promotieactie.
- Aanmeldingsferenties naar de CMS die hulpprogramma voor promotiebeheer host (voorheen genoemd het hulpprogramma voor beheer van levenscyclus LCM).
- Aanmeldingsreferenties voor de doel-CMS.
- Andere parameters die vereist zijn om de CMS succesvol te verhogen, zoals het LCMBIAR-wachtwoord of de overschrijfinstelling om indien vereist over bestaande objecten te schrijven.

U kunt andere optionele parameters opnemen die specifieke verhogingsbehoeften kunnen specificeren. Deze optionele parameters worden beschreven in de sectie Lijst met alle opdrachtregelparameters [pagina 643].

Het volgende voorbeeld toont een case voor een verhoging van LCMBIAR-bestand naar live CMS zonder een eigenschappenbestand in de opdrachtregel te gebruiken:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
lcmbiarpassword
```

Het volgende voorbeeld toont een case voor een verhoging van LCMBIAR-bestand naar live CMS met een eigenschappenbestand in de opdrachtregel:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

De volgende tabel vermeldt de vereiste parameters voor een succesvol eigenschappenbestand voor een verhoging van LCMBIAR-bestand naar live CMS:

Parametergroep	Parameter	Beschrijving
Actietype	`action`	Bewerking die de CLI moet uitvoeren. Waarde: export Voorbeeld: `action=export`

Parametergroep	Parameter	Beschrijving
LCM-knooppunt	`LCM_CMS`	CMS voor het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Gebruikersnaam van het account die het hulpprogramma moet gebruiken om verbinding te maken met de CMS van het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_userName=adminLCM`
	`LCM_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `LCM_password=my_adminpassword1`
Bron: LCMBIAR-bestand	`importLocation`	Locatie van het LCMBIAR-bestand dat de objecten bevat die moeten worden verhoogd. Waarde: Vrije tekst. Moet de extensie `<.lcmbiar>` hebben Voorbeeld: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Stelt de codering en decodering van BIAR-bestanden in met een wachtwoord. Waarde: Vrije tekst Voorbeeld: `lcmbiar=validlcmbiarpassword`

Parametergroep	Parameter	Beschrijving
Doel:Live CMS	`Destination_CMS`	CMS waarmee het hulpprogramma verbinding moet maken. Waarde: Geldige CMS-naam Voorbeeld: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Gebruikersaccount die het hulpprogramma voor promotiebeheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Geldige gebruikersnaam Voorbeeld: `Destination_username=adminLCM`
	`Destination_password`	Bijbehorend wachtwoord van het gebruikersaccount. Waarde: Geldig wachtwoord Voorbeeld: `Destination_password=my_adminpassword1`

Verwante informatie

Live CMS naar een LCMBIAR-bestand [pagina 635]
Live bron-CMS naar live doel-CMS [pagina 639]
Lijst met alle opdrachtregelparameters [pagina 643]

16.6.3.3 Live CMS naar een LCMBIAR-bestand

Wanneer u objecten van een live CMS naar een LCMBIAR-bestand verhoogt, refereert u aan een eigenschappenbestand vanaf de opdrachtregel die de verhogingsopdracht als volgt specificeert.

- Type verhogingsactie export
- Aanmeldingsferenties naar de CMS die hulpprogramma voor promotiebeheer host (voorheen genoemd het hulpprogramma voor beheer van levenscyclus LCM).
- Aanmeldingsreferenties voor de bron-CMS.

- Doeldirectory voor het LCMBIAR-bestand.
- Andere parameters vereist om de CMS succesvol te verhogen, zoals het LCMBIAR-wachtwoord of beveiligingsinstellingen.

U kunt andere optionele parameters opnemen die specifieke verhogingsbehoeften kunnen specificeren. Deze optionele parameters worden beschreven in de sectie Lijst met alle opdrachtregelparameters [pagina 643].

Het volgende voorbeeld toont een typisch eigenschappenbestand voor een verhoging live CMS naar LCMBIAR-bestand:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

De volgende tabel vermeldt de vereiste parameters voor een succesvol eigenschappenbestand voor een verhoging van LCMBIAR-bestand naar live CMS:

Parametergroep	Parameter	Beschrijving
Actietype	`action`	Bewerking die de CLI moet uitvoeren. Waarde: export Voorbeeld: `action=export`

Parametergroep	Parameter	Beschrijving
LCM-knooppunt	`LCM_CMS`	CMS voor het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Gebruikersnaam van het account die het hulpprogramma moet gebruiken om verbinding te maken met de CMS van het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_userName=adminLCM`
	`LCM_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `LCM_password=my_adminpassword1`
Bron: Live CMS	`Source_CMS`	CMS waarmee hulpprogramma voor promotiebeheer moet verbinden. Waarde: Vrije tekst Voorbeeld: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_userName`	Gebruikersaccount die het hulpprogramma voor promotiebeheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Vrije tekst Voorbeeld: `Source_username=adminLCM`

Parametergroep	Parameter	Beschrijving
	`Source_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `Source_password=my_adminpassword1`
Doel: LCMBIAR-bestand	`exportLocation`	Geeft de locatie op waar het LCMBIAR-bestand moet worden geplaatst nadat de objecten zijn ingepakt en geëxporteerd. Waarde: Vrije tekst. Moet de extensie `<.lcmbiar>` hebben Voorbeeld: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Steltde codering en decodering van BIAR-bestanden in met een wachtwoord. Waarde: Vrije tekst Voorbeeld: `lcmbiarpassword=validlcmbiarpassword`

Parametergroep	Parameter	Beschrijving
Exportgerelateerd	`exportQuery`	Voert query's op de bron-CMS uit om de vereiste objecten voor export naar het LCMBIAR-bestand op te halen. Waarde: Vrije tekst. Gebruik de CMS-querytaal. Voorbeeld: `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'` **Opmerking** U kunt een onbeperkt aantal query's in het eigenschappenbestand plaatsen, maar de naam moet de volgende notatie hebben: exportQuery1, exportQuery2.

Verwante informatie

LCMBIAR-bestand naar een live CMS [pagina 632]
Live bron-CMS naar live doel-CMS [pagina 639]
Lijst met alle opdrachtregelparameters [pagina 643]

16.6.3.4 Live bron-CMS naar live doel-CMS

Wanneer u objecten van een live bron-CMS naar een live doel-CMS doorgeeft, refereert u aan een eigenschappenbestand vanaf de opdrachtregel die de doorgifteopdracht als volgt specificeert:

- Type verhogingsactie Verhogen
- Aanmeldingsferenties naar de CMS die hulpprogramma voor promotiebeheer host (voorheen genoemd het hulpprogramma voor beheer van levenscyclus LCM).
- Aanmeldingsreferenties voor de bron-CMS.
- Aanmeldingsreferenties voor de doel-CMS.
- Andere parameters vereist om de CMS succesvol te verhogen, zoals beveiligings- of afhankelijkheidsparameters.

U kunt andere optionele parameters opnemen die specifieke verhogingsbehoeften kunnen specificeren. Deze optionele parameters worden beschreven in de sectie Lijst met alle opdrachtregelparameters [pagina 643].

Het volgende voorbeeld toont een typisch eigenschappenbestand voor een verhoging bron-CMS naar doel-CMS.

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

De volgende tabel vermeldt de vereiste parameters voor een succesvol eigenschappenbestand voor een verhoging van bron-CMS naar doel-CMS:

Parametergroep	Parameter	Beschrijving
Actietype	`action`	Bewerking die de opdrachtregel moet uitvoeren. Waarde: Verhogen Voorbeeld: `action=promote`
LCM-knooppunt	`LCM_CMS`	CMS voor het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_CMS=myCMS.mydomain.sap:6400`

Parametergroep	Parameter	Beschrijving
	`LCM_userName`	Gebruikersnaam van het account die het hulpprogramma moet gebruiken om verbinding te maken met de CMS van het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_userName=adminLCM`
	`LCM_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `LCM_password=my_adminpassword1`
Bron: Live CMS	`source_CMS`	CMS waarmee hulpprogramma voor promotiebeheer moet verbinden. Waarde: Vrije tekst Voorbeeld: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_username`	Gebruikersaccount die het hulpprogramma voor promotiebeheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Vrije tekst Voorbeeld: `Source_username=adminLCM`
	`Source_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `Source_password=my_adminpassword1`

Parametergroep	Parameter	Beschrijving
Doel: Live CMS	`Destination_CMS`	CMS waarmee het hulpprogramma verbinding moet maken. Waarde: Vrije tekst Voorbeeld: `Destination_CMS=myCMS1:myCMS2`
	`Destination_username`	Gebruikersaccount die het hulpprogramma voor promotiebeheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Vrije tekst Voorbeeld: `Destination_username=adminLCM`
	`Destination_password`	Bijbehorend wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `Destination_password=my_adminpassword1`

Parametergroep	Parameter	Beschrijving
Exportgerelateerd	`exportQuery`	Query´s die het LCM-hulpprogramma uitvoert om de vereiste objecten voor export naar de doel-CMS op te halen. Waarde: Vrije tekst. Gebruik de CMS-querytaal. Voorbeeld: `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'` **Opmerking** U kunt een onbeperkt aantal query's in het eigenschappenbestand plaatsen, maar de naam moet de volgende notatie hebben: exportQuery1, exportQuery2.

Verwante informatie

LCMBIAR-bestand naar een live CMS [pagina 632]
Live CMS naar een LCMBIAR-bestand [pagina 635]
Lijst met alle opdrachtregelparameters [pagina 643]

16.6.3.5 Lijst met alle opdrachtregelparameters

De volgende tabel beschrijft alle opdrachtregelparameters.

Opmerking

Wanneer ze binnen een opdrachtregel worden uitgevoerd, hebben parameters deze syntaxis-`<parameterName><space><parameterValue>`. Binnen een eigenschappenbestand hebben parameters deze syntaxis`<parameterName>=<parameterValue>`.

Parametergroep	Parameter	Beschrijving
Eigenschappenbestand	`lcmproperty`	Verwijst naar de waarden die zijn vereist voor het uitvoeren van een opdracht en die worden opgeslagen in een bestand. Waarde: Het volledige pad van de locatie waar het eigenschappenbestand is opgeslagen Voorbeeld: `-lcmproperty C:\MyPropertyFile.properties`
Actietype	`action`	Bewerking die de CLI moet uitvoeren. Waarde: Promote of export. Voorbeeld: `action=promote`
LCM-knooppunt	`LCM_CMS`	CMS voor het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Gebruikersnaam van het account die het hulpprogramma moet gebruiken om verbinding te maken met de CMS van het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_userName=adminLCM`
	`LCM_Password`	Wachtwoord van het gebruikersaccount. Indien dit leeg is, is het vereist het in de console. Waarde: Vrije tekst Voorbeeld: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Geeft aan welk verificatietype moet worden gebruikt. Waarde: secEnterprise, secWinAD, secLDAP,secSAPR3. Als deze optie niet is opgegeven, is `secEnterprise` de standaardinstelling. Voorbeeld: `LCM_authentication=secEnterprise`
	`LCM_systemID` **Opmerking** Verplicht voor SAP-verificatie	Alleen vereist voor SAP-verificatie. Waarde: Systeem-id Voorbeeld: `LCM_systemID=systemID`

Parametergroep	Parameter	Beschrijving
	`LCM_clientID` **Opmerking** Verplicht voor SAP-verificatie	Alleen vereist voor SAP-verificatie. Waarde: Client-id Voorbeeld: `LCM_clientID=clientID`
Bron: LCMBIAR-bestand	`importLocation`	Locatie van het LCMBIAR-bestand dat de objecten bevat die moeten worden verhoogd. Waarde: Vrije tekst. Moet de extensie `<.lcmbiar>` hebben Voorbeeld: `importLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Stelt de codering en decodering van BIAR-bestanden in met een wachtwoord. Waarde: Vrije tekst Voorbeeld: `lcmbiar=validlcmbiarpassword`
Bron: Live CMS	`Source_CMS`	CMS waarmee het hulpprogramma voor promotiebeheer een verbinding moet maken. Waarde: Vrije tekst Voorbeeld: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_UserName`	Gebruikersaccount die het hulpprogramma voor promotie-beheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Vrije tekst Voorbeeld: `Source_username=adminLCM`
	`Source_password`	Wachtwoord van het gebruikersaccount. Waarde: Vrije tekst Voorbeeld: `Source_password=my_adminpassword1`
	`Source_authentication`	Geeft aan welk verificatietype moet worden gebruikt. Waarde: secEnterprise, secWinAD, secLDAP,secSAPR3. Als deze optie niet is opgegeven, is `secEnterprise` de standaardinstelling. Voorbeeld: `Source_authentication=secEnterprise`

Parametergroep	Parameter	Beschrijving
	`Source_systemID`	Alleen vereist voor SAP-verificatie. Waarde: Systeem-id Voorbeeld: `Source_systemID=systemID`
	`Source_clientID`	Alleen vereist voor SAP-verificatie. Waarde: Systeem-id Voorbeeld: `Source_clientID=clientID`
Doel: LCMBIAR-bestand	`exportLocation`	Geeft de locatie op waar het LCMBIAR-bestand moet worden geplaatst nadat de objecten zijn ingepakt en geëxporteerd. Waarde: Vrije tekst. Moet de extensie `<.lcmbiar>` hebben Voorbeeld: `exportLocation=C:\Backup\New.lcmbiar`
	`lcmbiarpassword`	Steltde codering en decodering van BIAR-bestanden in met een wachtwoord. Waarde: Vrije tekst Voorbeeld: `lcmbiarpassword=validlcmbiarpassword`
Doel: Live CMS	`Destination_CMS`	CMS waarmee het hulpprogramma verbinding moet maken. Waarde: Geldige CMS-naam Voorbeeld: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	Gebruikersaccount die het hulpprogramma voor promotiebeheer moet gebruiken om verbinding te maken met de CMS van BI platform. Waarde: Geldige gebruikersnaam Voorbeeld: `Destination_username=adminLCM`
	`Destination_password`	Bijbehorend wachtwoord van het gebruikersaccount. Waarde: Geldig wachtwoord Voorbeeld: `Destination_password=my_adminpassword1`

> **Opmerking**
> Verplicht voor SAP-verificatie

Parametergroep	Parameter	Beschrijving
	`Destination_authentication`	Geeft aan welk verificatietype moet worden gebruikt. Waarde: secEnterprise, secWinAD, secLDAP, secSAPR3. Als deze optie niet is opgegeven, is `secEnterprise` de standaardinstelling. Voorbeeld: `Destination_authentication=secEnterprise`
	`Destination_systemID` **Opmerking** Verplicht voor SAP-verificatie	Alleen vereist voor SAP-verificatie. Waarde: Systeem-id Voorbeeld: `Destination_systemID=systemID`
	`Destination_clientID` **Opmerking** Verplicht voor SAP-verificatie	Alleen vereist voor SAP-verificatie. Waarde: Client-id Voorbeeld: `Destination_clientID=clientID`
Taakgerelateerd	`JOB_CUID`	Geeft door aan het hulpprogramma dat alle objecten in de taak naar het LCMBIAR-bestand moeten worden geëxporteerd. Waarde: De CUID van de opgeslagen beheertaak.
	`Override`	Wordt gebruikt om objecten uit een LCMBIAR-bestand selectief te verhogen. Indien `true`: maakt deze parameter het de gebruiker mogelijk om een bestaande taak te overschrijven. Indien `false`: maakt deze parameter het de gebruiker mogelijk om een nieuwe taak te maken met de naam `<JOB_NAME>_<TIME_STAMP>` . Waarde: true of false Voorbeeld: `Override=true`
	`forceOverride` Beschikbaar in SP4	Wordt gebruikt om een taak met dezelfde naam maar niet dezelfde CUID te overschrijven. Waarde: true of false Voorbeeld: `forceOverride=true`

Parametergroep	Parameter	Beschrijving
	`Timeout` Beschikbaar in SP4	Stelt een time-out in voor promote-actie. Waarde: Tijd in seconden Voorbeeld: `timeout=30`
Exportgerelateerd	`ExportDependencies`	Specificeert de objectafhankelijkheden die het hulpprogramma verzamelt voor export. Alleen van toepassing wanneer deze samen met de markering `Source_CMS` wordt gebruikt. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `false`. Voorbeeld: `ExportDependencies=false`
	`ExportQuery`	Query´s die het LCM-hulpprogramma uitvoert om de vereiste objecten voor export naar de doel-CMS op te halen. Waarde: Vrije tekst. Gebruik de CMS-querytaal. Voorbeeld: `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'` **Opmerking** U kunt een onbeperkt aantal query's in het eigenschappenbestand plaatsen, maar de naam moet de volgende notatie hebben: exportQuery1, exportQuery2.
	`ExportQueriesTotal`	Wordt gebruikt om het aantal uit te voeren exportquery´s op te geven. Als u x exportquery's hebt en deze allemaal wilt uitvoeren, stelt u deze parameterwaarde in op x. Waarde: positief geheel getal. Indien niet opgegeven is de standaardwaarde 1. Voorbeeld: `ExportQuery1=<your sql statement> ExportQuery2=<your sql statement> ExportQueriesTotal=2`

Parametergroep	Parameter	Beschrijving
	`BatchJobQuery`	Wordt gebruikt samen met `ExportQuery`. Maakt en start een job voor elke regel die door de taakquery geretourneerd wordt. Taakexportquery´s kunnen "tijdelijke aanduidingen" gebruiken die naar eigenschappen verwijzen die in de taakquery worden verhoogd. De notatie van de tijdelijke aanduiding is $b:PPTY$. Hierbij is de eigenschapsnaam niet hoofdlettergevoelig. De geldige <PPTY> zijn:- "cuid" - "name" - "id" Er wordt een fout gemeld als een tijdelijke aanduiding niet doot de taakquery wordt herkend of verhoogd. Waarde: Vrije tekst Voorbeeld: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")`
	`LimitQueryBatchSize`	Beperkt het aantal geretourneerde objecten standaard tot 1.000. Wanneer deze parameter op onwaar is ingesteld, worden alle objecten waarop een query is uitgevoerd geretourneerd. **Opmerking** U kunt de nieuwe limiet voor het aantal objecten dat de query retourneert ook expliciet instellen via `select TOP <number>` Waarde: true of false. Indien niet opgegeven is de standaardwaarde true Voorbeeld: `LimitQueryBatchSize=true`

Parametergroep	Parameter	Beschrijving
Logboekgerelateerd	`consolelog`	Wordt gebruikt om het volledige logboek weer te geven van de opdracht die door de gebruiker is uitgevoerd in het opdrachtenlogboek. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `false`. Voorbeeld: `consolelog=true`
	`ResultFileName`	De nsaam van het bestand op het lokale bestandssysteem wanneer de parameter `consolelog` wordt gebruikt. Waarde: bestandspad taakresultaat Voorbeeld: `ResultFileName=C:\Logs\ResultFile.txt`
	`LogFileName` Beschikbaar in SP4	Hiermee kan de gebruiker een vast pad opgeven dat voor het logboekbestand moet worden gebruikt. Waarde: bestandspad logboek Voorbeeld: `LogFileName=C:\Logs\LogFile.log`
Objectselectie	`Selected_CUIDS`	Hiermee kan de gebruiker selectief objecten (rapporten, gebruikers, universes enz.) met hun afhankelijkheden verhogen vanuit een LCMBIAR-bestand in plaats van het gehele bestand te moeten verhogen. Waarde: CUID's of objecten binnen het LCMBIAR-bestand die selectief moeten worden verhoogd.
	`selectUser` Beschikbaar in SP4	Filtert gebruikers op basis van verificatie door derden (LDAP, SAPR3, WindowsAD...). Waarde: all, none, excludeTP of onlyTP. Indien niet opgegeven is de standaardwaarde `all`. Voorbeeld: `selectUser=excludeTP`
	`selectGroup` Beschikbaar in SP4	Filtert gebruikersgroepen op basis van verificatie door derden (LDAP, SAPR3, WindowsAD...). Waarde: all, none, excludeTP of onlyTP. Indien niet opgegeven is de standaardwaarde `all`. Voorbeeld: `selectGroup=onlyTP`

Parametergroep	Parameter	Beschrijving
Beveiliging	`IncludeApplicationSecurity`	Hiermee wordt aan het hulpprogramma doorgegeven dat de beveiliging die is toegekend aan geselecteerde toepassingen, moet worden geëxporteerd of geïmporteerd. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `false`. Voorbeeld: `IncludeApplicationSecurity=true`
	`IncludeSecurity`	Hiermee wordt aan het hulpprogramma doorgegeven dat de beveiliging die is toegekend aan de geselecteerde objecten en gebruikers, moet worden geëxporteerd of geïmporteerd. Als toegangsniveaus worden gebruikt, worden deze hiermee ook geëxporteerd/geïmporteerd. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `false`. Voorbeeld: `IncludeSecurity=true`
Opmerkingen	`IncludeComments`	Hiermee wordt aan het hulpprogramma doorgegeven dat de opmerkingen die zijn toegekend aan geselecteerde toepassingen moeten worden geëxporteerd of geïmporteerd. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `false`. Voorbeeld: `IncludeComments=true`
Federatie-taken	`IncludeFederationJobsRelationship`	Het hulpprogramma krijgt de instructie de relaties van Federatie-taken (replicatielijsten en remote verbindingen) te behouden. Bij de instelling Onwaar worden gerepliceerde objecten reguliere objecten en wordt de Federatie-vlag verwijderd. Dit kan nuttig zijn als het gerepliceerde object het enige beschikbare object is en het bronobject niet langer beschikbaar is. Waarde: true of false. Indien niet opgegeven is de standaardwaarde `true`. Voorbeeld: `IncludeFederationJobsRelationship=false`

16.6.3.6 Terugzetten

U kunt de doorgegeven taak in het doelsysteem terugzetten via het hulpprogramma *Doorgiftebeheer*.

Als u een taak hebt doorgegeven via het hulpprogramma *Promotiebeheer* (bijvoorbeeld: om BI 4.2 SP07 bij te werken naar BI 4.3) en u wilt deze wijziging op een later moment terugzetten, kunt u de

opdrachtregelparameters gebruiken die zijn gedefinieerd in Opdrachtregelparameters op promotiescenario [pagina 628] en kunt u de terugzetbewerking uitvoeren.

Als u de terugzetbewerking uitvoert, moet u een eigenschappenbestand opgeven waarmee de doorgiftevolgorde als volgt wordt opgegeven:

- Type doorgifteactie: terugzetten
- Aanmeldingsferenties naar de CMS die hulpprogramma voor promotiebeheer host (voorheen genoemd het hulpprogramma voor beheer van levenscyclus LCM).
- Aanmeldingsreferenties voor de bron-CMS.
- Aanmeldingsreferenties voor de doel-CMS.
- Andere parameters vereist om de CMS succesvol door te geven, zoals beveiligings- of afhankelijkheidsparameters.

U kunt andere optionele parameters opnemen die specifieke verhogingsbehoeften kunnen specificeren. Deze optionele parameters worden beschreven in Lijst met alle opdrachtregelparameters [pagina 643].

U kunt het voorbeeldbestand met eigenschappen hieronder raadplegen om een terugzetbewerking uit te voeren:

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **Opmerking**
>
> U vindt de `job_cuid` voor een doorgegeven taak via *CMC-startpagina* > *Promotiebeheer* > *Eigenschappen* >.

De volgende tabel vermeldt de vereiste parameters voor een succesvol eigenschappenbestand voor een doorgifte van een LCMBIAR-bestand naar live CMS:

Parametergroep	Parameter	Beschrijving
Actietype	`action`	Bewerking die de CLI moet uitvoeren. Waarde: terugzetten Voorbeeld: `action=rollback`

Parametergroep	Parameter	Beschrijving
Taakgerelateerd	`job_cuid`	Geeft door aan het hulpprogramma dat alle objecten in de taak naar het LCMBIAR-bestand moeten worden ge-exporteerd. Waarde: De CUID van de opgeslagen beheertaak. Voorbeeld: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`
LCM-knooppunt	`LCM_CMS`	CMS voor het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	Gebruikersnaam van het account die het hulpprogramma moet gebruiken om verbinding te maken met de CMS van het hulpprogramma voor promotiebeheer. Waarde: Vrije tekst Voorbeeld: `LCM_userName=adminLCM`
	`LCM_password`	Wachtwoord van het gebruikersac-count. Waarde: Vrije tekst Voorbeeld: `LCM_password=my_adminpassword1`
	`LCM_authentication`	Verificatietype voor de gebruikersac-count. Waarde: Type verificatie Voorbeeld: `secEnterprise`

16.6.4 Voorbeeld van eigenschappenbestand

Dit is een voorbeeld van een `eigenschappenbestand`:

Voorbeeld

```
importLocation=C:/Backup/CR.lcmbiar
actie=verhogen
LCM_CMS=<CMS-naam:poortnummer>
LCM_userName=<gebruikersnaam>
LCM_password=<wachtwoord>
LCM_authentication=<verificatie>
LCM_systemID=<systeem-id>
LCM_clientID=<client-id>
Destination_CMS=<CMS-naam:poortnummer>
Destination_userName=<gebruikersnaam>
Destination_password=<wachtwoord>
Destination_authentication=<verificatie>
Destination_systemID=<systeem-id>
Destination_clientID=<client-id>
lcmbiarpassword=<password>
```

> **Opmerking**
>
> Als het `eigenschappenbestand` geen persoonlijke gegevens bevat, vraagt LCM CLI om hetzelfde in de console.

16.7 Het Enhanced Change and Transport System gebruiken

Het CTS (Change and Transport System) organiseert en ontwikkelt ontwikkelingsprojecten in de ABAP Workbench, en transporteert deze wijzigingen vervolgens tussen SAP-systemen in uw systeemomgeving. Het verbeterde CTS+ (Change and Transport System) is een add-on voor de CTS waarmee niet-ABAP-inhoud verhoogd wordt naar niet-ABAP-gegevensopslagruimten waarvoor CTS+ geactiveerd is.

BI-platform InfoObjects kunnen gebruikmaken van SAP Warehouse-inhoud als gegevensbron. Dankzij de integratie van CTS+ met het hulpprogramma Promotiebeheer kunt u de gegevensopslagruimte van het BI-platform net zo gebruiken als de SAP BW-gegevensopslagruimte (Business Warehouse) om taken te verhogen aan de hand van CTS-transportaanvragen. CTS+ biedt een optie voor het transport van niet-SAP-objecten binnen een systeemlandschap. Objecten die bijvoorbeeld gemaakt zijn in het ontwikkelingssysteem, kunnen worden gekoppeld aan transportaanvragen en worden doorgestuurd naar andere systemen binnen het landschap.

Zie Change and Transport System - Overview (BC-CTS) voor meer informatie over het Change and Transport System

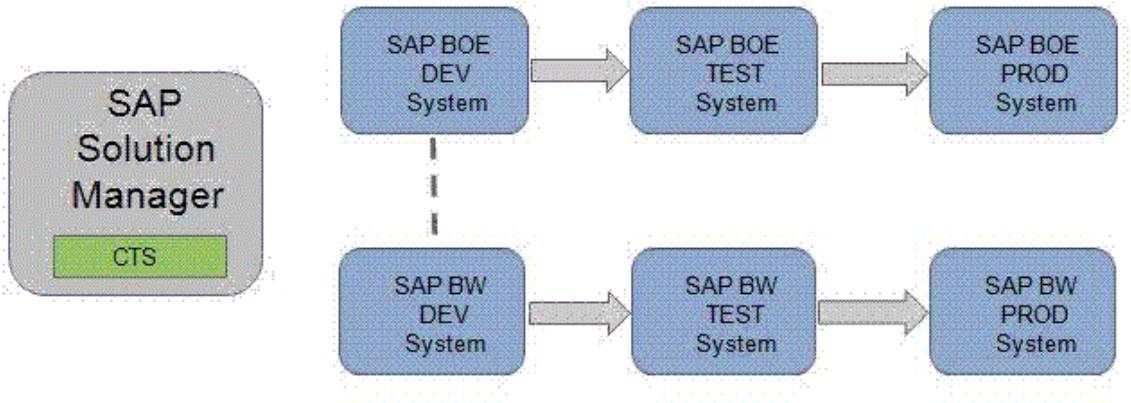
Zie Transporting Non-ABAP Objects in Change and Transport System voor meer informatie over CTS+ en niet-ABAP-transporten

16.7.1 Vereisten

Hieronder volgen de vereisten voor het transporteren van Business Intelligence-inhoud van het ene systeem naar een ander systeem met CTS+:

1. BI-platform 4.0 (of nieuwer) is geïnstalleerd.
2. SAP Solution Manager 7.1 of SAP Solution Manager 7.0 EHP 1 (minimaal SP25) is geïnstalleerd en wordt gebruikt als de domeincontroller voor CTS+, ten minste voor de configuratie van SAP BusinessObjects-systemen.
   Zie Configuring the Transport Domain voor meer informatie over de configuratie van het transportdomein.
3. De CTS-invoegtoepassing is geïnstalleerd op de SAP Solution Manager (CTS-invoegtoepassing wordt gehaald uit SL Toolset 1.0 SP02. Het is raadzaam de nieuwste CTS-invoegtoepassing te gebruiken).
   Zie 1533059 voor meer informatie over het installeren van de vereiste CTS-invoegtoepassing.
4. Systemen van *SAP Business Warehouse 7.0* (SPS 24 of hoger) zijn geïnstalleerd. Zie 1369301 voor meer informatie.
5. SAP Business Warehouse-transportlandschap (SAP BW) is geconfigureerd in het Change and Transport System (CTS).
6. 1692417 en 1860594 zijn geïmplementeerd op de computer waarop de CTS-implementatiewebservice wordt gehost.

16.7.2 Integratie van het BI-platform en CTS+ configureren



Het TMS (Transport Management System) is onderdeel van het Change and Transport System en wordt gebruikt om wijzigingen tussen de SAP-systemen in het landschap te transporteren. Hiermee worden de verbonden systemen beheerd, hun routes, en de importers in de bijbehorende systemen. Zie Transport Management System (BC-CTS-TMS) voor meer informatie over het Transport Management System

Met CTS+ kunt u bestanden extern verzamelen en binnen het transportlandschap distribueren. De web-UI van de Transport Organizer is onderdeel van CTS+ en beheert de transportaanvragen en de objecten die het bevat. Zie Transport Management System (BC-CTS-TMS) voor meer informatie.

U kunt promotiebeheer van het BI-platform integreren met CTS+ en SAP BW met behulp van CTS-transportaanvragen.

> ⓘ Opmerking
>
> Als u integratie van het BI-platform en SAP Solution Manager mogelijk wilt maken, moet u het toepassingstype "BOLM" definiëren in het SAP Solution Manager-landschap.

Voer de volgende stappen uit om het BI-platform en CTS+ te integreren:

1. Activeer de webservice CTS-export.
2. Configureer CTS-instellingen in het hulpprogramma Promotiebeheer.
3. Configureer het BI-platformimportsysteem in SAP Solution Manager.

Verwante informatie

De webservice CTS-export activeren [pagina 656]
CTS+-instellingen configureren in het hulpprogramma Promotiebeheer [pagina 657]
Integratie van het BI-platform en CTS+ configureren [pagina 655]

16.7.2.1 De webservice CTS-export activeren

Als u BI-platform wilt configureren, moet u de webservice CTS-export activeren in het webhulpprogramma voor SOA-beheer.

1. U start de toepassing door de transactiecode SOAMANAGER in uw SAP Solution Manager in te voeren. Nadat de vereiste verificatie is uitgevoerd, wordt de SOA-beheerconsole geopend in een webbrowser.

   Zie Een serviceprovider configureren voor meer informatie over SOA-beheer en de configuratie van een service-eindpunt met SAP Solution Manager 7.0. Zie Een serviceprovider configureren voor SAP Solution Manager 7.1.
2. Klik op het tabblad *Toepassings- en scenariocommunicatie* op *Configuratie van één service*.

   De webservice CTS-export heeft de naam `EXPORT_CTS_WS`.
3. Op het tabblad *Configuratie* maakt of bewerkt u het service-eindpunt.
4. Configureer op het tabblad *Beveiliging* het transportprotocol en de verificatiemethode.
5. Op het tabblad *Transportinstellingen* definieert u een alternatieve toegangs-URL om het service-eindpunt gemakkelijk te kunnen oproepen.

16.7.2.2 CTS+-instellingen configureren in het hulpprogramma Promotiebeheer

In de volgende sectie worden de configuratiestappen beschreven die in de CMC-toepassing moeten worden uitgevoerd om CTS+ in te stellen voor het gebruik van het hulpprogramma Promotiebeheer.

1. Klik op de pagina *Promotietaken* op *CTS-instellingen* en vervolgens op *BW-systemen*.
2. Klik op de pagina *BW-systemen* op *Toevoegen* om een BW-systeem toe te voegen aan de infrastructuur.
3. Voer de volgende details in op de pagina *Systeem toevoegen*:
   - *Host-BW-SID*: geeft de systeem-id (SID) van de SAP BW/ABAP-hostcomputer op.
   - *Hostnaam*: geef het IP-adres van de hostcomputer op.
   - *Systeemnummer*: voer het nummer van het hostsysteem in.
   - *Client*: verwijst naar de systeemdetails van de clientcomputer.
   - *Gebruiker* en *Wachtwoord*: geef in deze velden het gebruikersnaam en het wachtwoord voor de clientcomputer op.
   - *Taal*: geef in dit veld uw gewenste taal op.
4. Klik op *OK* om het systeem toe te voegen aan uw infrastructuur.

   > **Opmerking**
   >
   > Wanneer u een BW-systeem aan uw infrastructuur toevoegt, kunt u *Bewerken* of *Verwijderen* op de pagina *BW-systemen* om de systemen in uw infrastructuur te wijzigen.

5. Klik op de pagina *Promotietaken* op *CTS-instellingen* en vervolgens op *Instellingen van webservice*.
6. Op de pagina *Instellingen van webservice* voert u de Webservice-URL en gebruikersdetails in.

   > **Opmerking**
   >
   > Als u deze details niet hebt, vraagt u die op bij de Solution Manager-beheerder.

7. Klik op *Opslaan* en *Sluiten* om de webservice-instellingen te voltooien.
8. Maak een toewijzingsbestand voor het CMS-systeem voor Promotiebeheer van het BI-platform.

   Voltooi de volgende stappen in het ontwikkelingssysteem van BI-platform als u een tekstbestand wilt maken met verbindingsdetails om toewijzing in te schakelen.

   a. Ga in de CMS van Promotiebeheer van het BI-platform naar de hoofdmap en maak een map aan met de naam **`LCM`** in het pad `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/`
   b. Maak een tekstbestand aan met de naam `LCM_SOURCE_CMS_SID_MAPPING.properties` en voer een van de volgende gegevens in het bestand in:
      - `<De volledige naam van het bronsysteem van het SAP BI-platform met domein>@<CMS-poortnummer> = <logische naam voor bronsysteem zoals gebruikt in de CTS-configuratie >`
      - `<IP-nummer van het bronsysteem van het SAP BI-platform met domein>@<CMS-poortnummer> = <logische naam voor bronsysteem zoals gebruikt in de CTS-configuratie >`

   Bijvoorbeeld:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
```

```
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **Opmerking**
>
> In het geval van een omgeving met een cluster kopieert u het bestand `LCM_SOURCE_CMS_SID_MAPPING.properties` naar het systeem waarop Adaptive Processing Server wordt uitgevoerd.

Zie Making Transport Settings in the Application voor meer informatie over het uitvoeren van configuratiestappen voor niet-ABAP-systemen.

16.7.2.3 Het importsysteem van het BI-platform configureren in de SAP Solution Manager

1. Meld u aan bij het SAP Solution Manager-systeem.
2. Voer transactie `stms` in en druk op `Enter`.
3. Configureer BOLM als het toepassingstype.
   a. Ga naar *Overzicht* > *Systemen*.
   b. Ga naar *Extra's* > *Toepassingstype* > *Configureren*.
   c. Kies *New Entries* (Nieuwe ingangen).
   d. Voer in het veld *Toepassingstype* **`BOLM`** in.
   e. Voer de beschrijving in.
   f. Voer in het veld *Support Details* (Ondersteuningsdetails) de tekenreeks **`http://service.sap.com (ACH: BOJ-BIP-DEP)`** in.
   g. Kies *Tabelweergave* > *Opslaan*.
   h. Bevestig de aanwijzing door op *Ja* te klikken.
4. Als u met verschillende talen wilt werken, kunt u de vertaalde tekst als volgt behouden:
   a. Kies *Ga naar* > *Vertaling*.
   b. Selecteer de talen waarin u de tekst wilt vertalen.
   c. Voer de vertaalde waarden in de velden *Beschrijving* en *Ondersteuningsdetails* in.
   d. Bevestig het dialoogvenster.
   e. Kies *Doorgaan*.
   f. Kies *Tabelweergave* > *Opslaan*.
   g. Bevestig de aanwijzing.

   Het TMS-domein is nu gereed voor ondersteunend gebruik van bedrijfsintelligentie-inhoud in CTS.
5. Definieer in CTS+ het bronsysteem van het BI-platform als een exportsysteem.

   > **Opmerking**
   >
   > Zie Defining and Configuring Non-ABAP Systems voor meer informatie over het maken van een niet-ABAP-systeem als bronsysteem.
6. Configureer in CTS+ het importsysteem van het BI-platform door de volgende stappen uit te voeren:

> **Opmerking**
>
> U kunt een SID definiëren als verwijzing naar het importsysteem van het BI-platform.

a. Maak een niet-ABAP-systeem als een importsysteem.

   Zie Defining and Configuring Non-ABAP Systems voor meer informatie.

b. Geef de implementatiemethode op als *Overige* en hef de selectie van alle andere opties op.

c. Kies *Opslaan*.

d. Bevestig het distributiedialoogvenster.
   De tabelweergave voor configuratie van de importsysteeminstellingen wordt weergegeven.

e. Kies *Bewerken* > *Nieuwe ingangen*.

f. Voer de volgende stappen uit in het venster "Change View CTS: System details for handling of application types":

   1. Selecteer in het veld *Deploy Method* (Implementatiemethode) de optie *application specific Deployer (EJB)* (toepassingsspecifieke implementeerder).
   2. Voer in het veld *Implementatie-URI* de volgende URI in: **`http://<Naam BOE-webserver>:<Poort webserver>/BOE/LCM/CTSServlet?&cmsName=<Naam BOE-doel>:<CMSport>&authType=<Type BOE-verificatie>`**
      waarbij
      - 'Naam BOE-webserver' de naam of het IP-adres is van de computer waarop de webserver voor BI-platform wordt uitgevoerd.
      - 'Poort webserver' het poortnummer is van de webserver voor het BI-platform.
      - 'Naam BOE-doel' de naam van de computer is waarop de Central Management Server (CMS) van BI-platform wordt uitgevoerd.
      - 'CMS-poort' het poortnummer van de doel-CMS is.
      - "BOE-verificatietype" het type gebruikersverificatie is voor het importeren van Business Intelligence-inhoud. De ondersteunde verificatietypen zijn secEnterprise, secLDAP, secWinAD en secSAPR3.
   3. Voer in het veld *Gebruiker* de gebruikersnaam voor het BI-platform in.
   4. Voer in het veld *Wachtwoord* het wachtwoord van het BI-platform in.
   5. Kies *Save* om de instellingen op te slaan.

Als u meer dan één importsysteem nodig hebt, herhaalt u de bovenstaande stappen om alle vereiste doelsystemen te maken. Zie Configuring Transport Routes voor de configuratie van transportroutes tussen het bron- en doelsysteem nadat u de doelsystemen hebt gemaakt.

16.7.2.4 Vanuit BI-platform naar CTS+ met SSL exporteren

16.7.2.4.1 SSL voor CTS+ configureren

Als u SSL voor CTS+ wilt configureren, moet u SSL configureren op toepassingsserver ABAP. Zie Configuring the SAP Web AS for Supporting SSL voor meer informatie.

16.7.2.4.2 SSL-certificaat aan clientzijde configureren

Als u het SSL0-certificaat aan clientzijde wilt configureren, moet u het servercertificaat of het vertrouwde CA-certificaat in de JVM-keystore importeren.

1. Maak een back-up van de `cacerts`-bestanden in de map `<INSTALLDIR>\win64_x64\sapjvm\jre\lib\security`.
2. Importeer het certificaat in de JVM-host van Tomcat voor het bestand `BOE.war` met de volgende parameters:

   ```
   <INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer
   -keystore cacerts
   ```

3. Start Tomcat opnieuw.

16.7.2.4.3 De webserver CTS+-export configureren

Om de webservice voor CTS+-export te configureren waarbij HTTPS is ingeschakeld (`EXPORT_CTS_WS`), maakt u een nieuw HTTPS-eindpunt.

> ⓘ Opmerking
>
> Ook kunt u de optie inschakelen dat voor uw bestaand HTTP-eindpunt HTTPS wordt gebruikt.

1. Gebruik transactiecode **`soamanager`** en selecteer op het tabblad *Providerbeveiliging* onder *Communicatiebeveiliging* de optie *SSL over HTTP (beveiliging transportkanaal)* en selecteer onder *Verificatie transportkanaal* de optie *Gebruikersnaam/wachtwoord*.
2. Selecteer op het tabblad *Transportinstellingen* onder *Transportverbinding HTTPS* voor *Berekend protocol*.

16.7.2.4.4 Promotiebeheer voor SSL configureren

> → Onthouden
>
> Importeer het servercertificaat of het certificaat voor de vertrouwde CA in de JVM-keystore.

1. Klik in de CMC op het tabblad *Promotiebeheer* op *Instellingen* > *CTS-instellingen* > *Instellingen van webservice* >.
2. Controleer of de parameter *Web Service URL* `https://` en het hierboven geconfigureerde poortnummer bevat

   > ⓘ Opmerking
   >
   > De optie *Verhogen met CTS* wordt niet weergegeven in de lijst *Taaldoel* of het dialoogvenster *Overrides* als de opgegeven URL niet kan worden bereikt. Als de SSL-koppeling tussen Promotiebeheer en CTS+ mislukt, wordt er een fout opgenomen in het CMC-logboekbestand.

16.7.2.5 Vanuit CTS+ naar BI-platform met SSL exporteren

16.7.2.5.1 BI-platform Tomcat configureren voor gebruik van HTTPS

Voer de volgende stappen uit op de computer waarop het BI-platform is geïnstalleerd om het BI-platform Tomcat te configureren voor gebruik van HTTPS.

1. Maak een serversleutelpaar, een certificaat en een keystore.
   a. Voer `<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe` uit met de volgende parameters:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. Voer de volgende informatie in wanneer u hierom wordt gevraagd:
      - Uw voor- en achternaam
      - De naam van uw organisatie-eenheid
      - De naam van uw organisatie
      - De naam van uw plaats of locatie
      - De naam van uw provincie
      - De landcode van twee letters voor deze eenheid

      Er wordt een opgemaakte tekenreeks weergegeven (bijvoorbeeld `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Typ **`ja`** en druk op `Enter` om te bevestigen.
2. Stuur de aanvraag voor het servercertificaat naar een Certification Authority (CA).
3. Importeer het ondertekende servercertificaat in de serverkeystore met de volgende parameters:

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. Configureer het Tomcat-configuratiebestand `server.xml` om HTTPS in te schakelen en de serverkeystore die u hebt gemaakt te gebruiken.
5. Start Tomcat opnieuw en test de verbinding via de volgende URL in browser: `https://<SERVERNAAM>:<SSL-POORTNUMMER>`

Verwante informatie

SSL voor CTS+ configureren [pagina 659]

16.7.2.5.2 CTS+ voor SSL configureren

Om CTS+ te configureren voor SSL, maakt u een PSE voor een SSL-client en importeert u een certificaat.

Verwante informatie

SSL voor CTS+ configureren [pagina 659]

16.7.2.5.3 De test- en productiesystemen bijwerken in CTS+ voor gebruik van HTTPS

Ga als volgt te werk om HTTPS in te schakelen in de test- en productiesystemen:

1. Gebruik de transactiecode STMS.
2. Klik op *Systeemoverzicht*.
3. Selecteer uw test- en productiesysteem en klik op *Ga naar* > *Toepassingstypen* > *Implementatiemethode*.
4. Controleer of de parameter *Deploy URI* `https://` en een geconfigureerd HTTPS-poortnummer bevat

16.7.3 Een taak verhogen met CTS

In deze sectie wordt de werkstroom beschreven die hulpprogramma voor Promotiebeheer ondersteunt om CMS-objecten (Central Management Server) van het BI-platform te verhogen van het bronsysteem naar het doelsysteem met behulp van Change Transport System. Voer de volgende stappen uit om CTS te gebruiken om een taak te verhogen:

1. Start het hulpprogramma voor Promotiebeheer via SAP-verificatie en maak een taak.

   Zie de sectie "Een taak maken" in de verwante koppelingen onderin voor meer informatie over het maken van een nieuwe taak.

   > **Opmerking**
   >
   > Zorg ervoor dat u als verificatietype "SAP" selecteert in het aanmeldingsvenster op het bronsysteem.

2. In de vervolgkeuzelijst *Doel* selecteert u de optie *Verhogen met CTS*.

3. Klik op *Maken*.
   Het venster *Objecten van het systeem toevoegen* wordt weergegeven. Hier worden de mappen en submappen weergegeven in een boomstructuur.

4. Navigeer naar de map waarin u het InfoObject wilt selecteren.
5. Selecteer het informatieobject dat u wilt toevoegen aan de taak en klik op *Toevoegen*. Als u een InfoObject wilt toevoegen en het venster *Objecten toevoegen* wilt sluiten, klikt u op *Toevoegen en sluiten*.
   Het InfoObject wordt aan de taak toegevoegd en het venster *Taken verhogen* wordt geopend.

   > **Opmerking**
   >
   > In het venster Taken verhogen kunt u het volgende doen:
   > - Gebruik de optie *Objecten toevoegen* om meer InfoObjects toe te voegen aan de taak. Zie InfoObject toevoegen aan een taak voor meer informatie.
   > - Gebruik de optie *Afhankelijkheden beheren* om de afhankelijkheden van het geselecteerde InfoObject te beheren. De SAP BW-afhankelijkheden van het object worden weergegeven in de gebruikersinterface en kunnen door gebruikers geselecteerd worden.
   > Zie Taakafhankelijkheden beheren voor meer informatie.

6. Klik op *Verhogen*.
   Het venster *Verhogen* wordt weergegeven met de id, eigenaar en een korte beschrijving van de huidig ingestelde standaardtransportaanvragen.
7. U kunt de hyperlink *Transportaanvragen* gebruiken om het volgende te doen:
   - Details van de transportaanvraag weer te geven.
   - Instellingen van de standaardtransportaanvraag wijzigen.
   - Een andere transportaanvraag te kiezen.
   - Een transportaanvraag maken.

   1. Klik op de hyperlink *Transportaanvragen* om de web-UI van de *Transport Organizer* te openen.
   2. Als er gevraagd wordt om aanmeldingsreferenties, meldt u zich aan met geldige gebruikersreferenties voor het CTS-domeincontrollersysteem.
   3. Vernieuw het scherm *Verhogen* om uw updates weer te geven.

   Zie Transport Organizer Web UI voor meer informatie over het gebruik van de web-UI van de *Transport Organizer*.
8. Als u de details wilt weergeven voor de afhankelijkheden van de SAP BW-objecten, klikt u op de hyperlink *Afhankelijkheden van het tweede niveau*.

   > **Opmerking**
   >
   > Alleen objecten die in een aanvraag zijn ingesloten, worden weergegeven wanneer u op de hyperlink *Afhankelijkheden van het tweede niveau* klikt. Als de aanvraag is vrijgegeven, kunt u geen afhankelijkheden zien. Deze hyperlink wordt bovendien grijs weergegeven als er geen actieve afhankelijkheden op het tweede niveau zijn.

9. Klik op *Verhogen*.
10. Sluit de taak.
    Het hoofdscherm van promotiebeheer wordt geopend. De status van de taak die u hebt gemaakt, is nu *Geëxporteerd naar CTS*.
11. Geef het BI-platformobject vrij aan het doelsysteem door de volgende stappen te voltooien:
    a. Klik op de koppeling in de kolom status van de taak die u wilt verhogen.
       Het venster *Verhogingsstatus* wordt weergegeven.
    b. Klik op *Status van aanvraag*.
       De web-UI van de *Transport Organizer* wordt weergegeven.

c. Als de status van de aanvraag *Bewerkbaar* is, klikt u op *Vrijgeven* om de transportaanvraag van het BI-platformobject vrij te geven. Zie Releasing Transport Requests with Non-ABAP Objects voor meer informatie over het vrijgeven van transportaanvragen met niet-ABAP-objecten.
d. Sluit de web-UI van de *Transport Organizer*.

12. Als u de afhankelijkheden voor de SAP BW-objecten wilt weergeven, klikt u op de hyperlink *Lijst met BW-afhankelijkheden*.

> **Opmerking**
>
> Het is raadzaam contact op te nemen met het SAP BW-team om updates te verkrijgen voor SAP BW-afhankelijkheden en hun versie, aangezien er aan deze objecten gewerkt wordt door het team.

13. Sluit het venster *Verhogingstatus*.
14. Importeer het BI-platformobject naar het doelsysteem door de volgende stappen te voltooien:
    a. Meld u aan bij de CTS+-domeincontroller.
    b. Roep de **STMS**-transactie op om het transportbeheersysteem in te voeren.
    c. Klik op het pictogram *Overzicht importeren*.
    Het venster *Overzicht importeren* wordt weergegeven en hierin kunt u de geïmporteerde wachtrij-items van alle systemen weergeven.
    d. Kies de systeem-id voor het systeem voor Promotiebeheer van het doel.
    U kunt de lijst van transportaanvragen zien die in het systeem kunnen worden geïmporteerd.
    e. Klik op *Vernieuwen* .
    f. Importeer de relevante transportaanvragen. Zie Importing Requests voor meer informatie.

    Zie Importing Transport Requests with Non-ABAP Objects voor algemene informatie over het importeren van transportaanvragen met BOLM-inhoud.
15. Voer de volgende stappen uit als het geselecteerde object SAP BW-afhankelijkheden bevat:
    a. Geef de SAP BW-afhankelijkheden vrij aan het doelsysteem door de volgende stappen te voltooien:
        1. Meld u aan bij het SAP BW-bronsysteem.
        2. Roep een SE09-transactie op. Het venster *Transport Organizer* wordt weergegeven.
        3. Klik op *Weergeven*. De SAP BW-aanvraag wordt weergegeven.
        4. Klik op de SAP BW-aanvraag en vouw deze uit, zodat de taken worden weergegeven die voor de afhankelijkheden zijn gemaakt.
        5. Klik met de rechtermuisknop op de aanvraag die is gekoppeld aan het primaire SAP BW-object en selecteer *Direct vrijgeven*. Herhaal deze stap om alle taken vrij te geven die afzonderlijk aan elk afhankelijke element zijn gekoppeld.
        6. Klik met de rechtermuisknop op de aanvraag die is gekoppeld aan het primaire BW-object en selecteer *Direct vrijgeven*.
        7. Vernieuw het venster totdat alle aanvragen zijn vrijgegeven.

        > **Opmerking**
        >
        > U kunt de logboekvermeldingen van een aanvraag bekijken door erop te dubbelklikken.

    b. Importeer de SAP BW-afhankelijkheden naar het doelsysteem door de volgende stappen te voltooien:
        1. Meld u aan bij het SAP BW-doelsysteem.
        2. Roep de STMS-transactie op om het transportbeheersysteem in te voeren.
        3. Klik op het pictogram *Overzicht importeren*. Het venster *Overzicht importeren* wordt weergegeven.
        4. Dubbelklik op de systeem-id voor het SAP BW-doel. U kunt de lijst van transportaanvragen zien die in het systeem kunnen worden geïmporteerd.

5. Importeer de relevante transportaanvragen. Zie Importing Requests voor meer informatie.
   Zie Transports with Import Queues voor meer informatie over transporten met importwachtrijen.

16. Meld u aan bij het doelsysteem om de status weer te geven van de taak die u hebt verhoogd.

Zie Configuring Target Systems for Further Applications voor informatie over generieke CTS.

Verwante informatie

Een taak maken [pagina 601]
De afhankelijkheden van een taak beheren [pagina 607]

16.8 De wizard Doorgiftebeheer gebruiken

Met de wizard Doorgiftebeheer kunt u BI-bronnen (Business Intelligence) gemakkelijk, met enkele muisklikken, van de ene naar de andere gegevensopslagruimte kopiëren.

De wizard Doorgiftebeheer ondersteunt de volgende doorgiftescenario's:

- Een BI-bron uit een bronsysteem naar een LCMBIAR-bestand exporteren.
- Een BI-bron uit een bronsysteem naar een doelsysteem repliceren.
- Een LCMBIAR-bestand in een doelsysteem importeren.

Met de wizard Doorgiftebeheer kunt u nu de gehele inhoud of de gedeeltelijke inhoud van een gegevensopslagruimte doorgeven, zonder de commandoregel te gebruiken. De gebruiksvriendelijke grafische interface van de wizard Doorgiftebeheer maakt uw werk als beheerder gemakkelijker.

Zie SAP Note 2531264 voor meer informatie over de aanbevolen procedures voor de wizard Doorgiftebeheer.

> ⚠ Let op
>
> Terugzetten wordt niet ondersteund door de wizard Doorgiftebeheer. Dit houdt in dat u het doelsysteem na het doorgeven van BI-bronnen niet in zijn vorige staat kunt herstellen.

> ⓘ Opmerking
>
> Zorg ervoor dat u de geheugenwaarde controleert voordat u objecten gaat doorgeven. De Xms-waarde moet kleiner zijn dan of gelijk zijn aan de Xmx-waarde.

> ⓘ Opmerking
>
> Als u QaaWs-objecten hebt, moet u het doelsysteem op de juiste manier instellen.

→ Tip

U kunt de prestaties verhogen door Auditing en Monitoring in de CMC van het doelsysteem uit te schakelen. Zie de Beheerdershandleiding voor Business Intelligence-platform > Auditing voor meer informatie.

16.8.1 Objecten uitsluiten van doorgifte

U kunt objecten selecteren in onderstaande lijst en deze uitsluiten van een doorgiftetaak om schijfruimte te besparen en de migratietijd te verkorten.

Met een doorgiftetaak wordt elk BI-asset gemigreerd van het bron- naar het doelsysteem. Hierdoor worden de assets (die specifiek zijn voor het bronsysteem en niet bruikbaar zijn in het doelsysteem) ook gemigreerd. Doorloop de onderstaande stappen om BI-assets uit te sluiten van doorgifte:

1. Ga naar `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Open *PromotionManagementWizard.ini* in een teksteditor.
3. Zoek de string *# List of kinds to exclude automatically from full/selective export.* op.
   U vindt de code `-Dcom.sap.businessobjects.pmw.exclude.kind={}` onder de string.
4. Raadpleeg de onderstaande lijst met objecten en voeg de uit te sluiten objecten toe tussen `{}`.
5. Sla het bestand op.

De in de code genoemde objecten worden uitgesloten als u een doorgiftetaak uitvoert.

Raadpleeg onderstaande tabel voor de lijst met objecten die kunnen worden uitgesloten van een doorgiftetaak.

Aangepaste toegewezen kenmerken	DFS.Parameter	Discussies	GDPR-object
LCM JOBS	LCM Overrides	LCM Scan History	LCM Settings
LANDSCAPE	LANDSCAPE Connection	LIVE Office	MoN.MBEAN Config
MON.ManagedEntity Status	MON.MonAppDataStore	Mon.Probe	Mon.Subscription
NotificationScheduleObject	Override entry	PlatformSearchApplication Status	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator
XL.XcelsiusApllication	busobjectreporter	Explorer	Lumira Extensions

16.8.2 Wanneer moet u de wizard Doorgiftebeheer gebruiken

Er zijn verschillende opties beschikbaar voor doorgiftebeheer. Met behulp van deze tabel kunt u bepalen of de Wizard doorgiftebeheer de meest geschikte oplossing voor uw behoeften is.

Verschillende opties voor doorgiftebeheer

	Wizard doorgiftebeheer	Doorgiftebeheer met de optie Opdrachtregel	Doorgiftebeheer in de Central Management Console
Doel	Eenmalige doorgifte	Automatisering	Project
Doorgiftebereik	Aanzienlijk aantal BI-bronnen	Aanzienlijk aantal BI-bronnen	Een klein aantal BI-bronnen
Taak	Geen mogelijkheid om een taak te maken die opnieuw kan worden uitgevoerd door de taakserver	Mogelijkheid om een taak te maken die wordt uitgevoerd door de taakserver	Mogelijkheid om een taak te maken die wordt uitgevoerd door de taakserver

> **Opmerking**
>
> LCMBIAR-bestanden zijn compatibel met alle opties voor doorgiftebeheer, ongeacht de doorgiftebeheeroptie die u selecteert.

16.8.2.1 Instellingen voor doorgiftebeheer definiëren

1. Geef de gewenste instellingen voor doorgiftebeheer op. Hier vindt u informatie die u hierbij kan helpen:

Instelling	Beschrijving
Tijdelijke map	**Opmerking** Wijs voldoende vrije ruimte toe in de tijdelijke map. U hebt ten minste tweemaal zoveel vrije ruimte nodig als de benodigde ruimte.
Logboeklocatie	De logboeklocatie is standaard gedefinieerd. U kunt de logboeklocatie op een later tijdstip wijzigen. De wijzigingen worden direct meegenomen in de instellingen voor doorgiftebeheer.
Logboekniveau	U kunt het logboekniveau instellen op de volgende niveaus: • Standaard • Laag • Gemiddeld • Hoog Als u het logboekniveau niet wijzigt, wordt het ingesteld op “Standaard”.
Taal	U kunt in de Wizard doorgiftebeheer uw voorkeurstaal instellen.

2. Klik op *Volgende*

16.8.3 Scenario

De wizard Doorgiftebeheer ondersteunt drie typen doorgiftescenario's:

- Live systeem naar LCMBIAR: u kopieert objecten van een live CMS naar een LCMBIAR-bestand.
- Live CMS naar live doorgifte: u kopieert objecten van een live CMS-bronsysteem naar een live CMS-doelsysteem.
- LCMBIAR naar live systeem: u importeert objecten van een LCMBIAR-bestand naar een live CMS-doelsysteem.

16.8.3.1 Objecten van een live CMS-bronsysteem doorgeven aan een LCMBIAR-bestand

Om objecten van een live CMS aan een LCMBIAR-bestand door te geven:

1. Selecteer *Exporteren*.
2. Voer een van de volgende acties uit om de bron-CMS te definiëren:
   - Schakel het vakje *Maak van de centrale CMS de bron-CMS* in als u de centrale CMS als bron-CMS wilt gebruiken.
   - Voer in de sectie Bron de volgende gegevens in:
     - CMS-naam
     - Gebruiker
     - Wachtwoord
     - Verificatie
3. Klik in het veld *Doel* op *Selecteren* om de locatie van het LCMBIAR-bestand te selecteren.
4. (Optioneel) Voer een wachtwoord in om het LCMBIAR-bestand te encrypteren.

   > **Opmerking**
   >
   > Als u het LCMBIAR-bestand encrypteert, neemt het doorgifteproces meer tijd in beslag.

5. Klik op *Volgende* om de objecten die u wilt exporteren te selecteren.

16.8.3.2 Objecten van een live CMS-bronsysteem doorgeven aan een live CMS-doelsysteem

Om objecten van een live CMS-bronsysteem door te geven aan een live CMS-doelsysteem:

1. Selecteer *Doorgeven*.
2. Voer een van de volgende acties uit om de bron-CMS te definiëren:
   - Schakel het vakje *Maak van de centrale CMS de bron-CMS* in als u de centrale CMS als bron-CMS wilt gebruiken.

- Voer in de sectie Bron de volgende gegevens in:
  - CMS-naam
  - Gebruiker
  - Wachtwoord
  - Verificatie

3. Voer een van de volgende handelingen uit om de doel-CMS te definiëren:
   - Schakel het selectievakje *Van de centrale CMS de doel-CMS maken* in om de centrale CMS als doel-CMS te gebruiken.
   - Voer in de sectie *Doel* de volgende gegevens in:
     - CMS-naam
     - Gebruiker
     - Wachtwoord
     - Verificatie
4. Klik op *Volgende* om de objecten te selecteren die u van het bronsysteem naar het doelsysteem wilt kopiëren.

16.8.3.3 Objecten van een LCMBIAR-bestand doorgeven aan een live CMS-doelsysteem

Om objecten uit een LCMBIAR-bestand door te geven aan een live CMS:

1. Selecteer *Importeren*.
2. Voer een van de volgende handelingen uit om de doel-CMS te definiëren:
   - Schakel in de sectie *Doel* het vakje *Van de centrale CMS de doel-CMS maken* in.
   - Voer in de sectie *Doel* de volgende gegevens in:
     - CMS-naam
     - Gebruiker
     - Wachtwoord
     - Verificatie
3. Klik in de sectie *Bron* op *Selecteren* om het LCMBIAR-bestand dat u wilt importeren te selecteren.
4. (Optioneel) Voer een wachtwoord in om het LCMBIAR-bestand te encrypteren.

   > **Opmerking**
   >
   > Als u het LCMBIAR-bestand encrypteert, neemt het doorgifteproces meer tijd in beslag.

5. Klik op *Volgende* om de objecten die u wilt importeren te selecteren.

16.8.4 Objecten

Wizard doorgiftebeheer ondersteunt twee typen doorgifte voor inhoud:

- Doorgifte volledige inhoud
- Doorgifte selectieve inhoud

In onderstaande tabel wordt elk type toegelicht:

Typen doorgifte inhoud	Doorgegeven inhoud	Afhankelijkheden inhoud
Doorgifte volledige inhoud	U geeft de volgende inhoud volledig door van het bronsysteem aan het doelsysteem: • Objecten (gebruikers, documenten, universes, verbindingen enz.) • Exemplaren • Relaties tussen objecten • Objectbeveiliging	Omdat alle relaties worden verzorgd, hoeven afhankelijkheden niet te worden geëvalueerd. U gaat van de huidige stap Objecten direct naar de stap Samenvatting.
Doorgifte selectieve inhoud	U geeft de inhoud die u hebt geselecteerd door van het bronsysteem aan het doelsysteem. De inhoud is onder meer het volgende: • Objecten (gebruikers, documenten, universes, verbindingen enz.) • Exemplaren • Relaties tussen objecten • Objectbeveiliging	Omdat u niet alle inhoud van het bronsysteem doorgeeft aan het doelsysteem, moeten afhankelijkheden worden geëvalueerd.

16.8.4.1 Doorgifte van volledige inhoud

Om de volledige inhoud van het bronsysteem door te geven aan het doelsysteem:

1. Selecteer *Doorgifte volledige inhoud*.

   Alle objecten worden voor de doorgifte geselecteerd.
2. Klik op *Volgende* om de inhoud die u hebt geselecteerd te controleren.

16.8.4.2 Info over doorgifte selectieve inhoud

Voordat u de selectieve inhoud van het bronsysteem naar het doelsysteem doorgeeft, moet u de exportopties definiëren. Als u exportopties definieert, kunt u instellingen ophalen die zijn opgegeven voor het bronsysteem die u wilt doorgeven naar het doelsysteem.

16.8.4.2.1 Info over exportopties

Als u instellingen die zijn opgegeven in het bronsysteem wilt ophalen en wilt doorgeven aan het doelsysteem, moet u de volgende parameters definiëren in Exportopties:

- Objectexemplaren
- Objectafhankelijkheden
- Beveiliging
- Commentaar
- Federatietaken
- Conflict naamomzetting

Objectexemplaren

Objectexemplaren	Beschrijving
Alle exemplaren van een object exporteren wanneer het object wordt geselecteerd	U kunt de geselecteerde objecten exporteren met alle bijbehorende exemplaren.
Alleen terugkerende exemplaren van een object exporteren wanneer het object wordt geselecteerd.	U exporteert de geselecteerde objecten met alleen hun terugkerende exemplaren. Als u bijvoorbeeld een wekelijkse en maandelijkse vernieuwing voor een document hebt gepland, worden dit document en de twee bijbehorende terugkerende exemplaren tijdens de export geëxporteerd.
Export geen objectexemplaren	U exporteert alleen de geselecteerde objecten. De exemplaren hiervan worden niet geëxporteerd.

Objectafhankelijkheden

Objectafhankelijkheden	Beschrijving
Afhankelijkheden opnemen bij het selecteren van objecten	U exporteert de geselecteerde objecten met alle bijbehorende afhankelijkheden. **Opmerking** De optie is standaard ingeschakeld.
Afhankelijkheden uitsluiten bij het selecteren van objecten	U exporteert alleen de geselecteerde objecten zonder alle bijbehorende afhankelijkheden.

Beveiliging

Beveiliging	Beschrijving
Objectbeveiliging opnemen	U exporteert de geselecteerde objecten met bijbehorende beveiligingsinstellingen.
Gebruikersbeveiliging opnemen	U exporteert de geselecteerde objecten met de bijbehorende instellingen voor gebruikersbeveiliging.
Applicatiebeveiliging opnemen	U exporteert de geselecteerde objecten met bijbehorende instellingen voor applicatiebeveiliging.
Beveiliging op het hoogste niveau opnemen	U exporteert de beveiligingsinstellingen die zijn gedefinieerd in de hoofdmap. **⚠ Let op** Deze optie overschrijft de beveiligingsinstellingen die zijn gedefinieerd in het doelsysteem. Gebruik deze optie met mate.

Commentaar

Commentaar	Beschrijving
Opmerkingen opnemen	U exporteert de geselecteerde objecten met alle bijbehorende opmerkingen.
BI-startpuntvoorkeuren voor gebruikersgroep	Als u het selectievakje inschakelt, worden de BI-startpuntvoorkeuren van het bronsysteem voor een gebruikersgroep ingesteld als standaardvoorkeuren en gebruikt in het doelsysteem.

BI-voorkeuren gebruikersgroep

BI-voorkeuren gebruikersgroep	Beschrijving
BI-voorkeuren gebruikersgroep overschrijven	Als u het selectievakje inschakelt, worden de BI-startpuntvoorkeuren van het bronsysteem voor een gebruikersgroep ingesteld als standaardvoorkeuren en gebruikt in het doelsysteem. **ⓘ Opmerking** Als u een Web Intelligence-document doorgeeft dat gebruikmaakt van aanpassing met behulp van een BIAR-bestand moet u deze optie inschakelen om de aanpassing te importeren.

Federatietaken

Federatietaken	Beschrijving
Federatietaakrelatie opnemen	U importeert de geselecteerde objecten met verzorgde bijbehorende Federatietaakrelaties.

Conflict naamomzetting

Conflict naamomzetting	Beschrijving
Conflict naamomzetting	Als een geselecteerd object dezelfde naam heeft als een object in het doelsysteem, maar een andere CUID heeft, wordt in het doelsysteem een kopie van het geselecteerde object gemaakt. Als u deze optie niet activeert, wordt het geselecteerde object met dezelfde naam als een object in het doelsysteem maar met een andere CUID niet gekopieerd naar het doelsysteem.

16.8.4.2.2 Doorgifte selectieve inhoud

Om selectieve inhoud van het bronsysteem aan het doelsysteem door te geven:

1. Selecteer *Doorgifte selectieve inhoud*.
2. Voor het definiëren van *Exportopties* klikt u op *Opties*.
3. (Optioneel) Selecteer *Tijdfilter toepassen* om objecten op datum en periode te filteren.
4. Selecteer de objecten die u wilt exporteren.
5. Om de afhankelijkheden van een object te evalueren, selecteert u het bijbehorende vak onder het pictogram Afhankelijkheden

   > **Opmerking**
   >
   > De vakjes Afhankelijkheden zijn standaard allemaal aangevinkt. Deselecteer het vakje als u de afhankelijkheden van een object niet wilt evalueren.

6. Klik op *Volgende* om de afhankelijkheden te evalueren.

16.8.5 Afhankelijkheden

Als u ervoor kiest om selectieve inhoud van het bronsysteem naar het doelsysteem door te geven, kunnen de afhankelijkheden van de selectieve inhoud worden geëvalueerd. De stap *Afhankelijkheden* biedt een overzicht van de geselecteerde objecten die als afhankelijkheden zijn geïdentificeerd.

U kunt de volgende informatie over de afhankelijkheden van de geselecteerde objecten weergeven:

- Titel
- CUID
- Datum

U kunt als afhankelijkheden geïdentificeerde objecten selecteren:

1. Afhankelijk van het detailleringsniveau dat u wilt weergeven, voert u een van de volgende acties uit:
   - Klik op *Alles uitvouwen* om de details van alle afhankelijkheden weer te geven.
   - Klik op *Alles samenvouwen* om alleen de afhankelijke objecten weer te geven.
2. Selecteer de afhankelijkheden die u wilt doorgeven.

   > **Opmerking**
   >
   > De vakjes Afhankelijkheden zijn standaard allemaal aangevinkt. Deselecteer het vakje als u de afhankelijkheden van een object niet wilt doorgeven.

3. Klik op *Volgende* om de objecten te controleren die u voor de doorgifte hebt geselecteerd.

16.8.6 Samenvatting

Voordat u de doorgifte uitvoert, moet u de objecten die u hebt geselecteerd voor de doorgifte controleren.

U kunt de volgende informatie over elk object bekijken:

- Titel
- CUID
- Datum

> **Let op**
>
> Zorg ervoor dat alle objecten die u wilt kopiëren zijn opgenomen, omdat u het doorgifteproces niet kunt annuleren als het eenmaal is gestart. Terugzetten wordt niet ondersteund door de wizard Doorgiftebeheer.

U kunt objecten controleren:

1. Afhankelijk van het detailleringsniveau dat u wilt controleren, voert u een van de volgende acties uit:
   - Klik op *Weergeven* om de details van elk object weer te geven.
   - Klik op *Verbergen* om het bovenliggende object van elk object weer te geven.

   > **Opmerking**
   >
   > Het detailleringsniveau varieert in het CSV-bestand met doorgifteresultaten, afhankelijk van of u *Weergeven* of *Verbergen* selecteert.

2. Controleer de *Minimaal vereiste tijdelijke ruimte* om ervoor te zorgen dat u voldoelde ruimte op uw harde schijf hebt voor de doorgifte.
3. Klik op *Start* om de objecten door te geven.

   Nadat de doorgifte is gestart, kan deze niet worden geannuleerd.

16.8.7 (Optioneel) eigenschappenbestand

U kunt de volgende parameters configureren in het eigenschappenbestand van de Wizard doorgiftebeheer:

- SSL-instellingen
- Parameters

Het eigenschappenbestand van de Wizard doorgiftebeheer bevindt zich in:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

16.8.7.1 SSL-instellingen configureren

Als u gebruikmaakt van SSL, moet u de SSL-instellingen van de Wizard doorgiftebeheer configureren in

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Open `PromotionManagementWizard.ini` in een teksteditor.
2. Om de SSL-modus te activeren, verwijdert u de opmerkingen bij de regels die beginnen met "-D".
3. Voer de waarden voor elke instelling in.

Instelling	Waarde
`-Dbusinessobjects.orb.oci.protocol`	De waarde: ssl **Opmerking** Met het invoeren van deze waarde wordt SSL-communicatie ingeschakeld.
`-DcertDir`	De locatie van sleutels en certificaten
`-DtrustedCert`	De naam van het vertrouwde certificaatbestand **Opmerking** Als u meer dan één bestand opgeeft, scheid dan uw gegevens met een puntkomma (bijv. bestandA; bestandB).
`-DsslCert`	Het SDK-certificaat
`-DsslKey`	De privésleutel van het SDK-certificaat
`-Dpassphrase`	De locatie van het bestand dat de wachtwoordzin voor de privésleutel bevat

Instelling	Waarde
`-Dpsecert`	Het PSE-certificaatbestand

> ⚠ Let op
>
> Zorg ervoor dat u geen andere instellingen of waarden toevoegt of bewerkt.

4. Sla `PromotionManagementWizard.ini` op

Voorbeeld: SSL-instellingen in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

16.8.7.2 Parameters configureren

Al naargelang uw behoeften kunt u opties configureren in het eigenschappenbestand van de Wizard doorgiftebeheer in:

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Open `PromotionManagementWizard.ini` in een teksteditor.
2. Verwijder opmerkingen bij de regels die beginnen met "-D" om de opties te activeren.
3. Voer de waarden voor elke parameter in.

Parameter	Waarde
`-Dbusinessobjects.connectivity.directory`	De locatie van de verbindingsserverdirectory.
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` ⓘ Opmerking Deze waarde mag niet worden gewijzigd of bewerkt.
`-Xms8g`	De geheugenwaarde wordt standaard ingesteld op 8 GB.

Parameter	Waarde
	De Xms-waarde moet kleiner zijn dan of gelijk zijn aan de Xmx-waarde.
`-Xmx10g`	De geheugenwaarde wordt standaard ingesteld op 10 GB. Een geheugen van 10 GB is voldoende voor een repository van 65 000 objecten.
`-Dbobj.biar.suggestSplit=512`	Standaardwaarde (aanbevolen) Wij raden u aan de parameter `-Dbobj.biar.suggestSplit` te gebruiken. Wanneer u objecten van een live CMS aan een LCMBIAR-bestand doorgeeft, kunt u het LCMBIAR-bestand met deze instelling splitsen in meerdere LCMBIAR-bestanden.
`-Dbobj.biar.forceSplit=768`	Standaardwaarde (aanbevolen) Als de parameter `-Dbobj.biar.suggestSplit` niet kan worden toegepast, is de parameter `-Dbobj.biar.forceSplit` van toepassing als noodoplossing.
`-Dcom.businessobjects.lcm.commit`	• `KEEP_TS`: Standaardwaarde. Met deze waarde kunt u de wijzigingsdatums van de bron behouden. • `LEGACY`: De wijzigingsdatums komen overeen met de uitvoeringsdatum in het doelsysteem. Dit is gebruikelijk in versies voorafgaand aan 4.2 SP5
`-Dcom.sap.businessobjects.pmw.exclude.list`	Met deze parameter kunt u objecten permanent uitsluiten als u objecten doorgeeft van een bronsysteem aan een doelsysteem of wanneer u een bronsysteem exporteert naar een LCMBIAR-bestand. De waarde (CUID) kan een object zijn (document, map enz.). Als een map wordt opgegeven, worden alle onderliggende elementen van de map uitgesloten.

4. Sla `PromotionManagementWizard.ini` op.

Voorbeeld: Opties Wizard doorgiftebeheer in `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
```

```
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

16.8.8 De wizard Doorgiftebeheer in Linux

U kunt de wizard Doorgiftebeheer in Linux uitvoeren.

Voordat u de wizard Doorgiftebeheer in Linux start, moet u ervoor zorgen dat de Java-runtime in de systeemvariabele `PATH` is ingesteld.

Voer de volgende stappen uit om de wizard Doorgiftebeheer in Linux te starten:

1. Op een shell en ga naar de installatiemap, zoals de volgende:

   `/usr/sap_bobj/enterprise_xi40`
2. Voer de volgende opdracht uit:

   `./PromotionManagementWizard`

   Wizard doorgiftebeheer start.

   Raadpleeg uw OS-documentatie voor meer informatie over het gebruik van SSH en X11-omleiding.

17 Versiebeheer

17.1 Verschillende versies van een informatieobject beheren

Met de toepassing voor versiebeheer kunt u versies beheren van BI-bronnen die zich in de gegevensopslagruimte van het BI-platform bevinden. Zowel de SubVersion- als de GIT-versiebeheersystemen worden ondersteund. In deze sectie wordt beschreven hoe u de versiebeheerfunctie kunt gebruiken in het hulpprogramma voor promotiebeheer.

Voer de volgende stappen uit om verschillende versies van een informatieobject te maken en te beheren:

1. Start het hulpprogramma voor promotiebeheer.
2. Klik met de rechtermuisknop op een taak, selecteer *VMS-acties* en klik op *Toevoegen aan VM*. (U kunt ook op het tabblad *VMS-acties* klikken en vervolgens op *Toevoegen aan VM*.)

   > **Opmerking**
   >
   > Als u op *Toevoegen aan VM* klikt, wordt er een basisversie van het object gemaakt in de VMS-gegevensopslagruimte. Er is een basisversie vereist voor daaropvolgende controles.

3. Klik op *Controle* om het document bij te werken dat zich in de VMS-gegevensopslagruimte bevindt.
   Het dialoogvenster *Opmerkingen inchecken* wordt weergegeven.
4. Voer uw opmerkingen in en klik op *OK*.
   Het gewijzigde versienummer van het geselecteerde informatieobject wordt weergegeven in de VMS en kolommen van het Content Management System.
5. Als u de meest recente versie van het document op de VMS wilt verkrijgen, selecteert u het vereiste informatieobject en klikt u op *Nieuwste versie ophalen*.
6. Als u een kopie wilt maken van de nieuwste versie, klikt u op *Kopie maken*.
   Er wordt een kopie gemaakt van de geselecteerde versie.
7. Selecteer *Geschiedenis* om alle versies weer te geven die beschikbaar zijn voor de geselecteerde bron.
   Het venster *Geschiedenis* wordt weergegeven. De volgende opties worden weergegeven:
   - *Versie ophalen*: als er meerdere versies zijn en u hebt een bepaalde versie van de BI-bron nodig, kunt u de vereiste bron selecteren en op *Versie ophalen* klikken.
   - *Kopie van versie ophalen*: met deze optie kunt u een kopie van de geselecteerde versie ophalen.
   - *Kopie van versie exporteren*: met deze optie kunt u een kopie van de geselecteerde versie ophalen en deze opslaan op uw lokale systeem.

17.1.1 Toegangsrechten voor Versiebeheer

In deze sectie worden de toegangsrechten voor de toepassing Versiebeheer beschreven.

- U kunt toegangsrechten voor de toepassing Versiebeheer instellen in de CMC.
- U kunt granulaire toepassingsrechten instellen voor verschillende functies in de toepassing Versiebeheer.

Voer de volgende stappen uit als u specifieke rechten wilt instellen in de toepassing Versiebeheer:

1. Meld u aan bij CMC en selecteer *Toepassingen*.
2. Dubbelklik op *Versiebeheer*.
3. Klik op *Gebruikersbeveiliging* en selecteer een gebruiker. U kunt beveiligingsrechten weergeven voor of toewijzen aan de geselecteerde gebruiker.
4. Voor Versiebeheer zijn momenteel de volgende specifieke rechten beschikbaar:
   - Inchecken toestaan
   - Kopie maken toestaan
   - Revisie verwijderen toestaan
   - Revisie ophalen toestaan
   - Vergrendelen en ontgrendelen toestaan
   - Weergave en versie van BOMM-objecten
   - Weergave en versie van Business Views
   - Weergave en versie van agenda's
   - Weergave en versie van verbindingen
   - Weergave en versie van profielen
   - Weergave en versie van QaaWS
   - Weergave en versie van rapportobjecten
   - Weergave en versie van beveiligingsobjecten
   - Weergave en versie van universes
   - Verwijderde bronnen weergeven
5. Als u rechten aan een geselecteerde gebruiker wilt toewijzen, selecteert u het relevante recht en klikt u op *Beveiliging toewijzen*.

17.1.2 Back-ups van Subversion-bestanden maken en herstellen

In deze sectie worden procedures voorgesteld voor het uitvoeren van back-ups van Subversion-bestanden en het herstellen ervan. Een herstel- en back-upplan bestaat uit voorzorgsmaatregelen die getroffen worden in geval van een systeemfout vanwege een natuurramp of een catastrofale gebeurtenis.

17.1.2.1 Back-ups van Subversion-bestanden maken

Voer de volgende stappen uit om een back-up te maken van Subversion-bestanden:

1. Ga in Windows naar `<INSTALLDIR>\SAP BusinessObjects Enterprise 4.0\CheckOut` of ga in Unix naar `<INSTALLDIR>/sap_bobj/enterprise_40/Subversion/CheckOut`
2. Kopieer de map `CheckOut` en sla deze op een back-upapparaat op.
3. Kopieer de volledige `<LCM_Repository>` en sla deze op een back-upapparaat op.

17.1.2.2 Subversion-bestanden herstellen

Voer de volgende stappen uit om Subversion-bestanden te herstellen:

1. Herstel de map CheckOut vanuit de locatie waar u de back-up hebt opgeslagen.

   > **Opmerking**
   >
   > Klik in CMC op *Toepassingen* > *Versiebeheer* > *VMS-instellingen* en zorg dat het juiste CheckOut-pad in het veld *Map van werkruimte* is ingevoerd.

2. Herstel de LCM_Repository vanuit de locatie waar u de back-up hebt opgeslagen.

   > **Opmerking**
   >
   > Klik in CMC op *Toepassingen* > *Versiebeheer* > *VMS-instellingen* en zorg dat het juiste CheckOut-pad in het veld *Installatiepad* is ingevoerd.

17.2 Verschillende versies van BI-bronnen beheren

Met de toepassing voor versiebeheer kunt u verschillende versies van BI-bronnen beheren die zich in de gegevensopslagruimte van het BI-platform bevinden. Ter ondersteuning van deze functie bevat het hulpprogramma het SubVersion-versiebeheersysteem.

Voer de volgende stappen uit om verschillende versies van taken of andere informatieobjecten te beheren:

1. Meld u aan bij de CMC-toepassing en selecteer *Versiebeheer*.
2. Selecteer in het linkerpaneel van het venster *Versiebeheer* de map om de taak of de andere InfoObjects te bekijken waarvan u de versies wilt beheren.
3. Selecteer de informatieobjecten en klik op *Toevoegen aan VM*.

   > **Opmerking**
   >
   > Door op *Toevoegen aan VM* te klikken, wordt een basisversie van het object aangemaakt in de VMS (Version Management System)-gegevensopslagruimte. Er is een basisversie vereist voor daaropvolgende controles.

4. Klik op *Inchecken* bij volgende wijzigingen in het document en de versie van het incrementeel gewijzigde document. Het document dat in de VMS-gegevensopslagruimte staat wordt hiermee bijgewerkt.

   Het dialoogvenster *Opmerkingen inchecken* wordt weergegeven.

5. Voer uw opmerkingen in en klik op *OK*.
   De wijziging in het versienummer van het geselecteerde InfoObject wordt weergegeven in de kolommen *VMS-versie* en *CMS-versie (Central Management Server)*.
6. Als u de meest recente versie van het document op de VMS wilt verkrijgen, selecteert u het vereiste informatieobject en klikt u op *Nieuwste versie ophalen*.
   De nieuwste versie van de VMS-gegevensopslagruimte wordt in de CMS geïmporteerd.
7. Als u een kopie wilt maken van de nieuwste versie, klikt u op *Kopie maken*.
   In de gegevensopslagruimten van VMS en CMS wordt een kopie van de geselecteerde versie gemaakt.

8. Selecteer *Geschiedenis* om alle versies weer te geven die beschikbaar zijn voor het geselecteerde informatieobject.
   Het venster *Geschiedenis* wordt weergegeven. De volgende opties worden weergegeven:
   - *Versie ophalen* - Indien er meerdere versies zijn en u hebt een bepaalde versie van de BI-bron nodig, kunt u het vereiste InfoObject selecteren en op *Versie ophalen* klikken.
   - *Kopie van versie ophalen*: met deze optie kunt u een kopie van de geselecteerde versie ophalen.
   - *Kopie van versie exporteren*: met deze optie kunt u een kopie van de geselecteerde versie ophalen en deze opslaan op uw lokale systeem.
   - *Vergelijken*: met deze optie kunt u de metagegevens van twee versies van een taak vergelijken. Zie "Verschillende versies van dezelfde taak vergelijken" voor meer informatie.
9. Selecteer een informatieobject en klik op *Vergrendelen* om het te vergrendelen, of op *Ontgrendelen* om het te ontgrendelen, of op *Verwijderen* om alle versie-inhoud uit de VMS-gegevensopslagruimte te verwijderen. Dit heeft geen invloed op de CMS.

   > **Opmerking**
   >
   > Als u een informatieobject vergrendelt, kunt u geen acties meer uitvoeren op het desbetreffende informatieobject.

10. Wanneer de versie in de CMS recenter is dan de versie in de VMS, wordt een indicator weergegeven naast het bijgewerkte informatieobject. Wanneer u de cursor op de indicator plaatst, wordt de tooltip `De versie in CMS is recenter` weergegeven.
11. Als u een lijst wilt weergeven van alle gecontroleerde bronnen die wel in de VMS maar niet in de CMS voorkomen, klikt u op *Verwijderde bronnen weergeven*.
    Klik op alle verwijderde bronnen om de geschiedenis van de desbetreffende bron weer te geven. U kunt een verwijderde bron selecteren en op *Versie ophalen* klikken om de desbetreffende versie van de bron weer te geven.

    Klik op *Verwijderen* om het object ook tijdelijk uit de VMS-gegevensopslagruimte weg te halen.

    > **Opmerking**
    >
    > Als u *Versie ophalen* gebruikt, wordt de bron verplaatst van de lijst met ontbrekende bestanden op de VMS naar de CMS.

12. Selecteer een informatieobject en klik op om de eigenschappen van het informatieobject weer te geven.
    U kunt ook met de rechtermuisknop op het informatieobject klikken en stap 3 t/m 12 uitvoeren.
13. U kunt naar BI-assets zoeken in de toepassing *Versiebeheer*. U kunt opties zoals *Alle velden zoeken*, *Zoektitel*, *Zoektrefwoord* en *Zoekbeschrijving* om een specifieke zoekopdracht uit te voeren waarbij resultaten sneller worden opgehaald.

    > **Opmerking**
    >
    > De zoekfunctionaliteit in de toepassing *Versiebeheer* is contextafhankelijk. Dit betekent dat als u een map zoals *Controle* selecteert en u een zoekreeks invoert om een document te zoeken, in BI-platform alleen naar het document wordt gezocht in de map *Controle*. Als u de optie *Alle mappen* selecteert en een zoekopdracht uitvoert, wordt in BI-platform in elke map naar het informatieobject gezocht.

17.3 Subversion handmatig starten en stoppen in Unix

In Unix start Subversion mogelijk niet automatisch als de computer opnieuw wordt gestart. Vanaf BI-platform 4.1 SP 2 kunt u `<INSTALLDIR>/svn_startup.sh` uitvoeren om Subversion te starten en `<INSTALLDIR>/svn_shutdown.sh` om het te stoppen.

> **Opmerking**
>
> `svn_shutdown.sh` werkt alleen als `svnserve` wordt gestart met `svn_startup.sh`

> **Beperking**
>
> Als het Subversion-proces wordt uitgevoerd voordat de SP2-patch is geïnstalleerd, werkt `svn_shutdown.sh` niet nadat de patch is geïnstalleerd. Om Subversion opnieuw te starten, moet u het proces `svnserve` handmatig beëindigen en vervolgens `svn_startup.sh` uitvoeren.

17.4 Vereiste bestanden voor Subversion in Solaris 10 en RedHat Linux 5

De volgende bestanden zijn vereist om Subversion uit te voeren.

> **Opmerking**
>
> Als een van de volgende binaire bestanden ontbreekt voordat de installatie van BI-platform 4.1 SP1 wordt uitgevoerd, voert de gebruiker `<INSTALLDIR>/sap_bobj/lcm_installer.sh <SUBVERSION_PASSWORD> <CMS_PASSWORD>` uit en start deze de Adaptive Processing Server opnieuw om Versiebeheer correct uit te voeren.

- In Solaris 10 installeert u de pakketten `CSWlibiconv2` en `CSWlibgcc-s1` die `libiconv.so.2` en `libgcc_s.so.1` bevatten.

  > **→ Onthouden**
  >
  > Als u de pakketten hebt geïnstalleerd, controleert u of het pad naar deze bibliotheken is opgenomen in de omgevingsvariabele `LD_LIBRARY_PATH` van de gebruiker.

- In RedHat Linux 5 implementeert u `libexpat.so.1`.

17.5 Apache SubVersion gebruiken als Versiebeheersysteem

U kunt Apache SubVersion instellen als uw Versiebeheersysteem en de instellingen configureren vanuit de Central Management Console (CMC).

1. Klik op *Toepassingen* in de CMC.
2. Dubbelklik op *VMS*.
   Het scherm Versiebeheerinstellingen wordt weergegeven.
3. Selecteer *VMS-instellingen*.
4. Selecteer *Subversion* in de lijst *Versiebeheersystemen*.
   Het serverpoortnummer, het wachtwoord, de naam van de gegevensopslagruimte, de servernaam, de gebruikersnaam, de naam van de werkruimtemap en de naam van het installatiepad (die tijdens de installatie van het hulpprogramma voor promotiebeheer zijn opgegeven) worden weergegeven in de desbetreffende velden.
5. Wijzig zo nodig de velden.

   > **Opmerking**
   >
   > Zorg ervoor dat u het installatiepad invoert dat het `.exe`-bestand bevat.

   In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   In Unix: `<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin`
6. Selecteer *SVN*, *HTTP* of *HTTPS*.

   > **Opmerking**
   >
   > Zie de *Apache Subversion-documentatie* voor meer informatie over het verbinding maken met Subversion met HTTPS.
7. (Optioneel) klik op *VMS testen* om uw VMS-instellingen te valideren.
8. Klik op *Opslaan*.

   > **Opmerking**
   >
   > - Als u wilt dat Subversion uw standaard-VMS is, selecteert u *Als standaard-VMS gebruiken*.
   > - Start de Adaptive Processing Server opnieuw als u de velden hebt gewijzigd.

17.6 Git gebruiken als versiebeheersysteem

U kunt Git instellen als uw Versiebeheersysteem en de instellingen configureren vanuit de Central Management Console (CMC).

1. Selecteer op de CMC-startpagina *Toepassingen*.
2. Dubbelklik op *Versiebeheer*.
   Het scherm *VMS-instellingen* in *Instellingen versiebeheer* wordt weergegeven.
3. Kies *Git* in de lijst *Versiebeheersystemen*.
   Git-instellingen en de vereiste parameters worden weergegeven.
4. Selecteer een protocol en voer de waarde in de lege velden in. Raadpleeg de onderstaande tabel voor meer informatie over elk veld.

Terminologie van de gebruikersinterface	Beschrijving
Protocol	Kies Lokaal als Git op uw lokale systeem is geïnstalleerd en kies HTTP(s) als Git op een externe server is geïnstalleerd.
Gebruikersnaam	Voer de gebruikersnaam in van de server waarop Git is geïnstalleerd.
Wachtwoord	Voer het wachtwoord in voor toegang tot de server waarop Git is geïnstalleerd.
Server-URL	Voer de koppeling in naar de server waarop Git is geïnstalleerd.
Map van werkruimte	Voer het bestandspad in waarin u de werkruimte wilt opslaan.
Naam serveropslagruimte	Voer een naam in voor de serveropslagruimte.
GIT-installatiepad	Voer de installatiemap van Git in.

> **Opmerking**
>
> Als u wilt dat Git uw standaardversiebeheersysteem is, selecteert u *Gebruiken als standaard-VMS*.

5. Selecteer *VMS testen* om uw VMS-instellingen te valideren (optioneel).
6. Selecteer *Opslaan*.
7. Ga naar *Servers* > *Lijst met servers* > en selecteer *Server opnieuw starten* in het contextmenu van de *Adaptive Processing Server*.

U hebt Git als uw versiebeheersysteem geconfigureerd.

17.7 Standaardinstellingen van Versiebeheersysteem

Als de CMS opnieuw wordt geïnitialiseerd, worden alle toepassingsinstellingen gewist. De standaardinstellingen van het Versiebeheersysteem zijn:

Parameter	Waarde
Servernaam	`localhost`
Serverpoort	`3690`
Gebruikersnaam	`LCM`
Wachtwoord	Ingevoerd tijdens installatie.
Installatiepad	In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion` In Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/subversion/bin`

Parameter	Waarde
Naam van gegevensopslagruimte	In Windows: `svn_repository` In Unix: `LCM_repository`
Map van werkruimte	In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut` In Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/CheckOut`
Protocol	`SVN`

17.8 Verschillende versies van dezelfde taak vergelijken

U kunt de verschillen tussen twee versies van dezelfde taak bekijken door de volgende stappen uit te voeren:

1. Meld u aan bij de CMC-toepassing.
2. Selecteer *Versiebeheer* op de CMC-startpagina.
3. Selecteer in het scherm Versiebeheer de taak waarvoor u de versies wilt vergelijken.
4. Klik op *Geschiedenis*.
   De pagina Geschiedenis wordt nu geopend en hierop worden alle versies van het geselecteerde InfoObject weergegeven.
5. Selecteer twee versies om deze te vergelijken.
6. Klik op *Vergelijken*.
   Het vergelijkingsproces wordt gestart en de verschillen worden met oranje en de ontbrekende objecten met rood gemarkeerd.
7. Klik op *Opslaan* om het verschillenrapport op te slaan.

17.9 Upgrade van Subversion-inhoud uitvoeren

Als u oude subversie-inhoud hebt die is gemaakt met een eerdere versie van het BI-platform, kunt u de inhoud aan de hand van de volgende stappen naar de nieuwste versie upgraden:

1. Meld u aan bij VMS op de SAP BusinessObjects Enterprise 4.2.x-computer.
2. Check een object in. Check bijvoorbeeld de objecten beheerder en gast tweemaal in.
3. Klik in de CMC op *Gebruikers* en controleer of 2 wordt weergegeven in het VMS- en CMS-versienummer.
4. Meld u af van VMS.
5. Ga naar de opdrachtprompt en vervolgens naar `C:\Program Files\Subversion\bin`. Voer de volgende exportopdracht uit: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Kopieer het bestand `dumrepo` naar de BI-platformcomputer

7. Ga naar de opdrachtaanwijzing op de BI-platformcomputer en vervolgens naar `C:\Program Files (x)\SAP`. Voer de volgende opdrachten uit:

   ```
   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. Start de SIA opnieuw op nadat de opdrachten zijn uitgevoerd.
9. Meld u aan bij de CMC en klik op *Versiebeheer*.
10. Klik op *Gebruikers* en controleer of de VMS-versie 2 is.
11. Selecteer het object *Beheerder* en klik op *Laatste versie ophalen*.
12. Het versienummer op VMS en CMS zijn nu hetzelfde.

    Zie Releaseopmerkingen voor Apache Subversion 1.10 voor meer informatie over de upgrade van Apache Subversion.

17.10 Subversion configureren voor geclusterde Job Servers voor verwerking

17.10.1 Optie A: De Subversion-hoofdcomputer vóór eventuele bewerkingen in het versiebeheersysteem configureren

1. Controleer dat de werkkopiemap niet is gemaakt in `<INSTALLDIR>\CheckOut`
2. Maak een map voor uw Subversion-werkkopiebestanden en deel deze, en zorg ervoor dat andere computers naar deze bestanden kunnen schrijven.
3. Wijzig in de CMC op de pagina met instellingen voor het versiebeheersysteem de *Servernaam* van **`localhost`** in het adres van uw hoofdcomputer.
4. Wijzig de *Werkruimtemap* in uw werkkopieaandeel in de volgende indeling: `\\<HOSTNAME>\<SHARENAME>`
5. Stop de Server Intelligence Agent (SIA) en wijzig de account van LocalSystem in de beheerder van het besturingssysteem.

   > **Opmerking**
   >
   > LocalSystem heeft geen netwerktoegang tot de gedeelde map.

6. Start de SIA.

   > **Opmerking**
   >
   > Als de SIA al wordt uitgevoerd onder een account met netwerktoegang tot de gedeelde map, hoeft u alleen alle Job Servers voor verwerking die het versiebeheersysteem hosten opnieuw te starten om de stappen 3 en 4 te implementeren.

17.10.2 Optie B: Subversion configureren nadat het versiebeheersysteem een werkkopiemap heeft gemaakt

1. Controleer dat Subversion is geïnstalleerd als onderdeel van het BI-platform.
2. Deel de werkkopiemap in `<INSTALLDIR>\CheckOut` en zorg ervoor dat andere computers naar deze map kunnen schrijven.
3. Maak de naam van de werkruimte via een van de volgende methoden:
   - Voer een versiebeheersysteembewerking uit op de hoofdcomputer. Controleer vervolgens de Subversion-werkkopiemap om de naam van de werkruimte te bepalen.
   - Bereken de naam van de werkruimte door het symbool @ te verwijderen en alle dubbele punten te vervangen door het teken *B*. Als de cluster bijvoorbeeld de naam `ABCD-LCM:6400` heeft, gebruikt het versiebeheersysteem `ABCD-LCMB6400` als de werkruimtenaam.

> **Opmerking**
>
> Subversion slaat zijn gegevensopslagruimte op in de werkkopiemap.

4. Wijzig de standaard-URL van **`localhost`** in een URL die elke computer kan gebruiken via de volgende opdracht:

```
svn switch --relocate svn://localhost:3690/
svn_repository svn://<SUBVERSION_MACHINE>:3690/svn_repository \
\<SUBVERSION_SHARE>\CheckOut\<WORKSPACE_NAME>-LCMB6400\WORKSPACE
```

5. Voer desgevraagd het wachtwoord van de beheerder van het besturingssysteem, de gebruiker en het wachtwoord in.

   > **Opmerking**
   >
   > Standaard is de gebruiker LCM en het wachtwoord het wachtwoord dat tijdens de installatie is ingesteld.

6. Wijzig in de CMC op de pagina met instellingen voor het versiebeheersysteem de *Servernaam* van **`localhost`** in het adres van uw hoofdcomputer.
7. Wijzig de *Werkruimtemap* van **`localhost`** in uw werkkopieaandeel: `\\<SUBVERSION_SHARE>\CheckOut`
8. Stop de Server Intelligence Agent (SIA) en wijzig de account van LocalSystem in de beheerder van het besturingssysteem
9. Start de SIA.

   > **Opmerking**
   >
   > Als de SIA al wordt uitgevoerd onder een account met netwerktoegang tot de gedeelde map, hoeft u alleen alle Job Servers voor verwerking die het versiebeheersysteem hosten opnieuw te starten.

17.10.3 Andere SubVersion-computers configureren

Als u andere SubVersion-computers wilt configureren, stopt u de Server Intelligence Agent (SIA) en wijzigt u de account van LocalSystem in een account met netwerktoegang zodat de Job Server voor verwerking toegang

heeft tot de gedeelde map (bijvoorbeeld: de account voor de beheerder van het besturingssysteem). Start de SIA opnieuw.

> **Opmerking**
>
> Als de SIA al wordt uitgevoerd onder een account met netwerktoegang tot de gedeelde map, hoeft u alleen alle Job Servers voor verwerking die het versiebeheersysteem hosten opnieuw te starten.

18 Toepassingen beheren

18.1 GDPR-pop-upbericht uitschakelen

Sinds de 4.2 SP5-release van SAP BusinessObjects Business Intelligence-platform, is het disclaimerpop-upbericht voor GDPR (Global Data Protection Regulation) verplicht voor alle gebruikers als deze zich aanmelden bij BI-platformwebtoepassingen zoals:

- BI-startpunt
- CMC
- BI-startpunt van Fiori
- Open Document

Het GDPR-disclaimerbericht is dus verplicht, maar u hebt de mogelijkheid om weergave van het bericht uit te schakelen.

> ⚠ Let op
>
> Het GDPR-disclaimerpop-upbericht **mag niet** en **kan niet** proactief worden uitgeschakeld. Om ervoor te zorgen dat er wordt voldaan aan de EU-wetgeving inzake GDPR, moeten alle gebruikers het bericht actief accepteren voordat ze doorgaan.

Het GDPR-bericht uitschakelen voor gebruikers die zich aanmelden bij het BI-startpunt

1. Ga in de standaardinstallatie voor Tomcat naar het eigenschappenbestand:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Maak een nieuwe bestand met de naam `<Infoview.properties>` en typ `<properties file>` in het aangepaste pad in:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Maak een nieuwe eigenschap voor`<disclaimer.enabled>` en stel deze in op `<false>`:
   `disclaimer.enabled=false`
4. Sla het bestand op.
5. Start Tomcat opnieuw.

Het GDPR-bericht uitschakelen voor gebruikers die zich aanmelden bij CMC

1. Ga in de standaardinstallatie voor Tomcat naar het eigenschappenbestand:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
2. Maak een nieuwe bestand met de naam `<CMCApp.properties>` en typ `<properties file>` in het aangepaste pad in:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Maak een nieuwe eigenschap voor`<disclaimer.enabled>` en stel deze in op `<false>`:
   `disclaimer.enabled=false`
4. Sla het bestand op.
5. Start Tomcat opnieuw.

Het GDPR-bericht uitschakelen voor gebruikers die zich aanmelden bij het BI-startpunt van Fiori

1. Ga in de standaardinstallatie voor Tomcat naar het eigenschappenbestand:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Maak een nieuwe bestand met de naam `<FioriBI.properties>` en typ `<properties file>` in het aangepaste pad in:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Maak een nieuwe eigenschap voor`<disclaimer.enabled>` en stel deze in op `<false>`:
   `disclaimer.enabled=false`
4. Sla het bestand op.
5. Start Tomcat opnieuw.

Het GDPR-bericht uitschakelen voor Open Document

1. Ga in de standaardinstallatie voor Tomcat naar het eigenschappenbestand:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Maak een nieuwe bestand met de naam `<OpenDocument.properties>` en typ `<properties file>` in het aangepaste pad in:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Voorbeeld: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`

3. Maak een nieuwe eigenschap voor`<disclaimer.enabled>` en stel deze in op `<false>`:
   `disclaimer.enabled=false`
4. Sla het bestand op.
5. Start Tomcat opnieuw.

18.2 Toepassingen beheren via de CMC

18.2.1 Overzicht

In het beheergebied *Toepassingen* van de CMC kunt u wijzigingen aanbrengen in de weergave en functionaliteit van webtoepassingen, zoals de CMC en BI-startpunt, zonder enige kennis van programmeren. U kunt ook de toegang van gebruikers, groepen en beheerders tot toepassingen aanpassen door hun rechten te wijzigen.

In deze sectie vindt u contextuele informatie, procedures en instructies voor het beheren van diverse instellingen. De volgende toepassingen hebben instellingen die kunnen worden gewijzigd via de CMC:

- *Meldingstoepassing*
- *Analysis-editie voor OLAP*
- *´Analysis voor Office Runtime*
- *Configuratie verificatieserver*
- *BEx-webtoepassingen*
- *Cockpit BI-beheerder*
- *BI-startpunt*
- *BI-werkruimten*
- *Central Management Console*
- *Samenwerking*
- *Toepassing BI-commentaar*
- *Crystal Reports-configuratie*
- *HANA-verificatie*
- *Hulpprogramma voor informatieontwerp*
- *Toepassing Information Steward*
- *BI-beheerdersstudio*
- *Beheerprogramma voor multitenancy*
- *Document openen*
- *Toepassing voor platform zoeken*
- *Doorgiftebeheer*
- *Toepassing prullenbak*
- *RESTful webservice*
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- *Hulpprogramma voor vertaalbeheer*
- *Hulpprogramma voor universe-ontwerp*

- *Versiebeheer*
- *Versiebeheer*
- *Visual Difference*
- *Web Intelligence*
- *Webservice*
- *Workflowassistent*

18.2.2 Algemene instellingen voor toepassingen

18.2.2.1 Gebruikersrechten instellen voor toepassingen

U kunt rechten gebruiken om de toegang van gebruikers tot bepaalde functies in toepassingen te beheren. Met het gebied *Toepassingen* in de CMC kunt u principals toewijzen aan de toegangscontrolelijst voor een toepassing, de rechten van een principal weergeven en de rechten wijzigen die een principal tot een toepassing heeft. Zie voor meer informatie over het beheer van rechten de *Beheerdershandleiding voor SAP BI-platform*.

18.2.2.2 Het niveau voor het traceringslogboek voor webtoepassingen instellen in de CMC

Als u andere webtoepassingen wilt traceren, moet u het bijbehorende `BO_trace.ini`-bestand handmatig configureren.

1. Klik in het gebied *Toepassingen* van de CMC met de rechtermuisknop op een toepassing en selecteer *Instellingen van traceringslogboek*.

   > **Opmerking**
   >
   > Deze toepassingen hebben instellingen voor traceringslogboeken: Fiorified BI-startpunt, CMC, Open Document, Promotiebeheer, Versiebeheer, Visueel verschil en Webservice.

   Het dialoogvenster *Instellingen van traceringslogboek* wordt weergegeven.
2. Selecteer een instelling in de lijst *Logboekniveau*.
3. Klik op *Opslaan en sluiten*.
4. Start de webtoepassingsserver opnieuw.

Het nieuwe niveau van het traceringslogboek wordt van kracht na de volgende aanmelding bij de webtoepassing.

Verwante informatie

Niveaus voor traceringslogboeken [pagina 694]

18.2.2.2.1 Niveaus voor traceringslogboeken

De volgende traceringslogboekniveaus zijn beschikbaar voor BI-platformonderdelen:

Niveau	Beschrijving
Onbepaald	Het niveau voor het traceringslogboek wordt opgegeven via een andere methode, meestal een `INI`-bestand.
Geen	Er wordt geen tracering uitgevoerd.
Laag	Met het filter van het traceringslogboek kunnen foutberichten worden geregistreerd, terwijl waarschuwingen en statusberichten worden genegeerd. Belangrijke statusberichten worden geregistreerd voor het opstarten en afsluiten van onderdelen en begin- en eindverzoeken. Dit niveau wordt niet aanbevolen voor foutopsporing.
Gemiddeld	Het filter voor het traceringslogboek is zo ingesteld dat fout-, waarschuwings- en de meeste statusberichten worden opgenomen. De minder belangrijke of zeer uitgebreide statusberichten worden weggefilterd. Dit niveau is niet uitgebreid genoeg voor foutopsporing.
Hoog	Er worden geen berichten gefilterd. Dit niveau wordt aanbevolen voor foutopsporing. ⚠ Let op Dit niveau van het traceringslogboek heeft een aanzienlijk effect op systeembronnen, verhoogt CPU-gebruik en neemt opslagruimte in.

18.2.3 Toepassingsspecifieke instellingen

18.2.3.1 CMC-toepassingsinstellingen beheren

18.2.3.1.1 Verificatie en programmaobjecten

U kunt instellen welke typen programmaobjecten door gebruikers kunnen worden uitgevoerd en u kunt de referenties configureren die nodig zijn om programmaobjecten te kunnen uitvoeren.

Wees bedacht op de potentiële beveiligingsrisico's die het toevoegen van programmaobjecten aan de gegevensopslagruimte met zich meebrengen. Het toegangsniveau voor bestanden van de account waaronder een programmaobject wordt uitgevoerd, bepaalt welke wijzigingen het programma kan aanbrengen in bestanden.

Typen programmaobjecten in- of uitschakelen

Als eerste beveiligingsmaatregel kunt u configureren welke typen programmaobjecten voor gebruik beschikbaar zijn.

Verificatie op alle platforms

In het beheergebied *Mappen* van de CMC moet u referenties opgeven voor de account waaronder het programma wordt uitgevoerd. Met deze functie kunt u een specifieke gebruikersaccount voor het programma instellen en aan deze account de juiste rechten toewijzen, zodat het programmaobject onder die account wordt uitgevoerd.

Ook kunnen gebruikers die programmaobjecten aan Information Platform Services toevoegen, hun eigen referenties aan een programmaobject toewijzen en het programma toegang geven tot het systeem. Op die manier wordt het programma onder die gebruikersaccount uitgevoerd en zijn de rechten van het programma beperkt tot de rechten van de gebruiker. Als u geen gebruikersaccount voor een programmaobject opgeeft, wordt het uitgevoerd onder de standaardsysteemaccount die meestal lokaal rechten heeft en dus geen rechten elders in het netwerk.

> **Opmerking**
>
> Als er geen referenties zijn opgegeven, kunt u geen programmaobject plannen. U kunt standaardreferenties opgeven door *CMC* te selecteren in het beheergebied *Toepassingen*. Klik in het menu *Acties* op *Rechten voor programmaobjecten*. Klik op *Plannen met de volgende referenties van het besturingssysteem* en geef een standaardgebruikersnaam en -wachtwoord op.

Verificatie voor Java-programma's

Met Information Platform Services kunt u de beveiliging voor alle programmaobjecten instellen. Information Platform Services dwingt voor Java-programma's het gebruik van een Java Policy File af. Een Java Policy File bevat een standaardinstelling die consistent is met de Java-standaard voor onbeveiligde code. Gebruik het Java Policy Tool (dat beschikbaar wordt gesteld in de Java Development Kit) om het Java Policy File zo te wijzigen dat deze aan uw specifieke behoeften voldoet.

Het Java Policy Tool heeft twee codebase-vermeldingen. De eerste vermelding verwijst naar de SAP BusinessObjects Enterprise Java SDK en verschaft programmaobjecten de volledige rechten voor alle JAR-bestanden van SAP BusinessObjects Enterprise. De tweede codebase-vermelding is van toepassing op alle lokale bestanden. Deze gebruikt dezelfde beveiligingsinstellingen voor onbeveiligde code als de Java-standaard voor onbeveiligde code.

> **Opmerking**
>
> De instellingen voor de Java Policy zijn universeel voor alle Program Job Servers die op dezelfde computer worden uitgevoerd.

> **Opmerking**
>
> De Java Policy File wordt standaard geïnstalleerd in de Java SDK-map in de hoofdmap van Information Platform Services. Onder Windows bevindt deze map zich meestal op de volgende locatie: `C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

18.2.3.1.1.1 Een type programmaobject in- of uitschakelen

1. Selecteer in het gebied *Toepassingen* de *Central Management Console*.
2. Klik op *Acties* > *Rechten voor programmaobjecten*.
   Het dialoogvenster *Rechten voor programmaobjecten* wordt weergegeven.
3. Selecteer in het gebied *Gebruikers het volgende toestaan* de typen programmaobjecten waartoe u gebruikers toegang wilt geven.

   U kunt *Scripts/binaire bestanden uitvoeren* of *Java-programma's uitvoeren* selecteren.

   Als u *Java-programma's uitvoeren* hebt geselecteerd, kunt u het selectievakje *Imitatie gebruiken* in- of uitschakelen. Deze optie voorziet het Java-programma van een token voor aanmelding bij Information Platform Services.
4. Klik op *Opslaan en sluiten*.

> **Opmerking**
>
> Als u een upgrade uitvoert naar SAP BusinessObjects Business Intelligence Platform 4.3 Support Package 3, worden programmaobjectrechten standaard voor iedereen geweigerd. Een beheerder-gebruiker (of eender welke gebruiker in de beheerdergroep) kunnen dit inschakelen.
>
> Onder *Java-programma's uitvoeren* staat het aankruisvakje *Imitatie gebruiken*. In 4.3 Support Package 3 is het aankruisvakje *Imitatie gebruiken* verwijderd.

18.2.3.1.2 Uitbreidingsmodules registreren in het systeem

> **Opmerking**
>
> Deze functie is niet van toepassing op Web Intelligence-documenten.

Voordat u uw programma-uitbreidingen op bepaalde objecten kunt toepassen, moet u uw bibliotheek met code beschikbaar stellen voor elke computer waarop de plannings- of weergaveaanvragen worden verwerkt. Bij de installatie van het BI-platform wordt op elke Job Server, verwerkingsserver en RAS (Report Application Server) een standaardmap voor uw uitbreidingsmodules gemaakt. U wordt aangeraden uw uitbreidingsmodules naar de standaardmap op elke server te kopiëren. Onder Windows is de standaardmap `C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\ProcessExt`. Onder Unix is de standaardmap `sap_bobj/ProcessExt`.

> → Tip
>
> Bestanden voor uitbreidingsmodules kunnen worden gedeeld.

Afhankelijk van de functionaliteit in de programma-uitbreiding, kopieert u de bibliotheek naar de volgende computers:

- Als uw uitbreidingsmodule alleen planningsaanvragen onderschept, kopieert u de bibliotheek naar elke computer die als Adaptive Job Server wordt uitgevoerd.
- Als uw uitbreidingsmodule alleen weergaveaanvragen ondervangt, kopieert u de bibliotheek naar elke computer die als Crystal Reports Processing Server of RAS wordt uitgevoerd.
- Als uw uitbreidingsmodule plannings- en weergaveaanvragen onderschept, kopieert u de bibliotheek naar elke computer die als een Adaptive Job Server Crystal Reports -verwerkingsserver of RAS wordt uitgevoerd.

> ⓘ Opmerking
>
> Als de programma-uitbreiding alleen is vereist voor plannings-/weergaveverzoeken aan een bepaalde servergroep, hoeft u alleen de bibliotheek te kopiëren naar alle verwerkingsservers in die groep.

18.2.3.1.2.1 Een uitbreidingsmodule registreren in het systeem

1. Ga naar het beheergebied *Toepassingen* in CMC.
2. Selecteer *Central Management Console*.
3. Klik op ▶ *Acties* ▸ *Uitbreidingsmodules* ▶.
   Het dialoogvenster *Uitbreidingsmodules: CMC* wordt weergegeven.
4. Geef in het vak *Naam* een weergavenaam op voor uw uitbreidingsmodule.
5. Typ in het vak *Locatie* de bestandsnaam en eventueel het pad van uw uitbreidingsmodule.
   - Als u uw uitbreidingsmodule naar de standaardmap op de desbetreffende computers hebt gekopieerd, hoeft u alleen de bestandsnaam (zonder extensie) te typen.
   - Als u uw uitbreidingsmodule naar een submap van de standaardmap hebt gekopieerd, typt u het pad als volgt: **`<submap>/<bestandsnaam>`**
6. Gebruik het vak *Beschrijving* om informatie over uw uitbreidingsmodule toe te voegen.
7. Klik op *Toevoegen*.

   > → Tip
   >
   > Als u een uitbreidingsmodule wilt verwijderen, selecteert u de gewenste module in de lijst *Bestaande extensies* en klikt u op *Verwijderen*. (Zorg ervoor dat er geen terugkerende taken op deze uitbreidingsmodule zijn gebaseerd; deze taken zullen mislukken.)
8. Klik op *Opslaan en sluiten*.
   De uitbreidingsmodule wordt in CMC geregistreerd.

U kunt deze uitbreidingsmodule nu selecteren om de business logic op bepaalde objecten toe te passen.

18.2.3.1.2.2 Programma-uitbreidingen voor meerdere servers delen

> **Opmerking**
>
> Deze functie is niet van toepassing op Web Intelligence-documenten of -rapporten gemaakt in SAP Crystal Reports voor Enterprise.

Als u alle uitbreidingsmodules op één locatie wilt plaatsen, kunt u de standaardmap voor uitbreidingsmodules voor elke Adaptive Job Server, Crystal Reports-verwerkingsserver en RAS overschrijven. Kopieer eerst uw programma-uitbreidingen naar een gedeelde map op een netwerkstation dat voor alle servers toegankelijk is. Wijs het netwerkstation toe op elke servercomputer.

> **Opmerking**
>
> toegewezen stations onder Windows zijn geldig totdat u de computer opnieuw opstart.

Als u servers in Windows en UNIX uitvoert, moet u een DLL- en een SO-versie van elke uitbreidingsmodule naar de gedeelde map kopiëren. Bovendien moet het gedeelde netwerkstation voor Windows- en UNIX-computers zichtbaar zijn (via Samba of een ander systeem voor het delen van bestanden).

Ten slotte wijzigt u de opdrachtregels van alle servers om de standaardmap voor programma-uitbreidingen aan te passen. Als u de opdrachtregel wilt wijzigen, gaat u naar het tabblad Servers in de CMC, selecteert u een server en opent u de pagina Eigenschappen. Voeg `-report_ProcessExtPath <absolute path>` toe aan de opdrachtregel. Vervang `<absoluut pad>` door het pad naar de nieuwe map, met inachtneming van de bestandsnaamconventies voor het besturingssysteem op de server (bijvoorbeeld `M:\code\uitbreidingsmodules`, `/hoofdmap/gedeeld/code/uitbreidingsmodules`, enzovoort).

Als u de standaardmap voor de uitbreidingsmodules wilt wijzigen, stopt u de server vanuit de CMC. Geef vervolgens de eigenschappen van de server weer om de opdrachtregel te wijzigen. Start de server opnieuw wanneer u klaar bent.

18.2.3.1.3 CMC-tabtoegang beheren

18.2.3.1.3.1 Gedelegeerd beheer en CMC-tabtoegang

De systeembeheerder van BI-platform beheert meestal een groot aantal documenten, mappen, gebruikers, servers en andere objecten. In grootschalige bedrijfsomgevingen is één beheerder soms echter niet voldoende. Een systeembeheerder die zich alleen op de belangrijkste taken wil concentreren, kan gedelegeerde beheerders maken en subreeksen met managementtaken aan deze beheerders toewijzen (bijvoorbeeld het beheer van een afdeling of tenants). In tegenstelling tot systeembeheerders voeren gedelegeerde beheerders een beperkte reeks taken uit en hebben ze minder rechten tot objecten in het systeem.

Met de standaardconfiguratie van de Central Management Console hebben gebruikers toegang tot alle beschikbare CMC-tabbladen. De systeembeheerder kan CMC-tabtoegang beheren om te bepalen welke tabbladen worden weergegeven aan principals (gebruikers of gebruikersgroepen). Teneinde de gebruikerservaring en werkstroom van de gedelegeerde beheerder te verbeteren, kan een systeembeheerder ook CMC-tabbladen verbergen die een gedelegeerde beheerder waarschijnlijk niet zal gebruiken.

> ⚠ Let op
>
> Beheer van CMC-tabtoegang heeft alleen invloed op de visuele weergave van de CMC-gebruikersinterface. CMC-tabbladen verbergen zorgt niet voor verhoogde beveiliging, omdat beveiligingsrechten voor objecten op tabbladen niet worden ingesteld of gewijzigd. U zorgt dat gebruikers geen onbevoegde bewerkingen op niet-geautoriseerde objecten uitvoeren (bijvoorbeeld het beheer van servers via de Central Configuration Manager of software van derden op basis van de BI-platform SDK), moet u de toepasselijke beveiligingsrechten voor objecten instellen, bijvoorbeeld serverobjecten.

Verwante informatie

CMC-tabtoegang voor andere gebruikers beheren [pagina 700]
Rechten beheren om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te configureren [pagina 702]

18.2.3.1.3.2 Met CMC-tabtoegang werken

18.2.3.1.3.2.1 CMC-tabtoegang voor andere gebruikers beheren

Een systeembeheerder heeft altijd toegang tot alle CMC-tabbladen. Aan de hand van onderstaande richtlijnen kunt u bepalen tot welke CMC-tabbladen principals toegang hebben:

- Voor een vereenvoudigd beheerproces, minder onderhoud en een kleiner aantal problemen is het raadzaam dat beheerders CMC-tabtoegang op gebruikersgroepsniveau beheren (en niet op gebruikersniveau).
- Voor CMC-tabbladen met mappen op het hoogste niveau moet een beheerder toegang tot een tabblad verlenen en het recht *Weergave* voor de map op het bovenste niveau van het tabblad verlenen. De volgende CMC-tabbladen bieden ondersteuning voor mappen op het hoogste niveau:
  - *Toegangsniveaus*
  - *Agenda's*
  - *Categorieën*
  - *Verbindingen/Universeverbindingen*
  - *Cryptografiesleutels*
  - *Gebeurtenissen*
  - *Federaties*
  - *Mappen*
  - *Postvakken IN*
  - *OLAP-verbinding*
  - *Persoonlijke categorieën*
  - *Persoonlijke mappen*

- *Profielen*
- *Herhalingslijsten*
- *Servers en groepen*
- *Tijdelijke opslag*
- *Universes*
- *Gebruikers en groepen*
- *Webservicequery*

- Voor verbeterde systeembeveiliging hebben alleen leden van de groep Beheerders toegang tot de volgende CMC-tabbladen. Als systeembeheerders hebben leden van de groep Beheerders toegang tot alle CMC-tabbladen, ongeacht de toegangsrechten voor CMC-tabbladen. Toegangsrechten voor CMC-tabbladen zijn ontworpen om toegang tot CMC-tabbladen te beheren voor gedelegeerde beheerders, dat wil zeggen, gebruikers die niet lid zijn van de groep Beheerders.
  - *Controlefunctie*
  - *Verificaties*
  - *Cryptografiesleutels*
  - *Licentiesleutels*
  - *Toezicht*
  - *Sessies*
  - *Instellingen*
  - *Beheer van gebruikersattributen*

> ⚠ Let op
>
> Beheer van CMC-tabtoegang heeft alleen invloed op de visuele weergave van de CMC-gebruikersinterface. CMC-tabbladen verbergen zorgt niet voor verhoogde beveiliging, omdat beveiligingsrechten voor objecten op tabbladen niet worden ingesteld of gewijzigd. U zorgt dat gebruikers geen onbevoegde bewerkingen op niet-geautoriseerde objecten uitvoeren (bijvoorbeeld het beheer van servers via de Central Configuration Manager of software van derden op basis van de BI-platform SDK), moet u de toepasselijke beveiligingsrechten voor objecten instellen, bijvoorbeeld serverobjecten.

18.2.3.1.3.2.1.1 CMC-tabtoegang voor andere gebruikers beheren

1. Meld u aan bij de CMC.
2. Klik met de rechtermuisknop op een principal op het tabblad *Gebruikers en groepen* en selecteer *CMC-tabconfiguratie*.

   > ⓘ Opmerking
   >
   > Als de CMC-tabtoegang onbeperkt is, wordt het volgende bericht weergegeven: `Waarschuwing: toegang tot CMC-tabbladen is momenteel onbeperkt. Als u CMC-toegang wilt beperken, klikt u op de tab Toegang, selecteert u 'CMC' en stelt u de toegang tot CMC-tabbladen in op beperkt. De volgende instellingen worden van kracht nadat toegang tot CMC-tabbladen beperkt is.` U kunt CMC-tabtoegang nog steeds configureren. De configuratie wordt echter pas geïmplementeerd wanneer u CMC-tabtoegang beperkt.

Er wordt een tabel weergegeven in het dialoogvenster *CMC-tabtoegang configureren*:

- □ of □ geeft aan tot welke CMC-tabbladen de principal toegang heeft.
- *Overgenomen* geeft aan dat tabtoegang is overgenomen van de bovenliggende gebruikersgroep(en).
- *Expliciet* geeft aan dat tabtoegang expliciet is opgegeven op het niveau van de principal.

3. Bekijk de rechten voor CMC-tabtoegang. U kunt de rechten wijzigen via de knoppen op de werkbalk:
   - Klik op *Verlenen* om expliciet toegang tot een tabblad te verlenen.
   - Klik op *Weigeren* om expliciet toegang tot een tabblad te weigeren.
   - Klik op *Overnemen* om een overgenomen toegangsrecht te gebruiken.

   > **Opmerking**
   >
   > Wanneer u op een knop klikt, worden de wijzigingen onmiddellijk op de principal toegepast.

4. Klik op *Sluiten* als u klaar bent.

De nieuwe tabtoegang die van kracht is, wordt weergegeven in de kolom *Recht* van de tabel.

Verwante informatie

CMC-tabtoegang beperken [pagina 704]

18.2.3.1.3.2.1.2 Overname van CMC-tabtoegang

CMC-tabtoegangsrechten en het recht om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te beheren, worden op dezelfde manier toegepast en overgenomen als andere beveiligingsrechten van het BI-platform. Als er niet expliciet tabtoegang voor principals is opgegeven, nemen zij de tabtoegang over van de gebruikersgroepen waarvan zij lid zijn.

Als een gebruiker lid is van twee gebruikersgroepen, wordt tabtoegang op dezelfde manier bepaald als alle andere rechten van het BI-platform. Als bijvoorbeeld toegang tot een CMC-tab in een van de groepen wordt verleend en in de andere groep wordt geweigerd, heeft de principal geen toegang tot de CMC-tab.

> **Opmerking**
>
> - Wanneer het CMC-tabtoegangsrecht van een gebruikersgroep wordt gewijzigd, wordt dezelfde tabtoegang voor alle gebruikers of gebruikersgroepen gewijzigd die rechten overnemen van de gebruikersgroep, als hun CMC-tabtoegang is ingesteld op *Overgenomen*.
> - Tabtoegang dat is ingesteld op het gebruikersniveau, heeft altijd voorrang op tabtoegang dat is overgenomen van gebruikersgroepen.

18.2.3.1.3.2.1.3 Gebruikersgroepen met gedelegeerde beheerders

U kunt een reeks gebruikersgroepen met gedelegeerde beheerders maken om CMC-tabbeheer te vereenvoudigen. U voorkomt dat u afzonderlijke CMC-tabtoegang moet configureren door een bestaande gebruiker of gebruikersgroep lid te maken van een gebruikersgroep met gedelegeerde beheerders. De volgende configuratie wordt aangeraden, maar kan worden afgestemd op specifieke bedrijfsvereisten.

> **Opmerking**
>
> Lidmaatschap van meerdere groepen resulteert in extra rechten, als de rechten zijn ingesteld op *Overgenomen*.

Gebruikersgroep met gedelegeerde beheerders	Aanbevolgen rechten
Systeembeheerders	Verleen toegang tot alle tabbladen.
Gebruikerbeheerders	Verleen toegang tot *Toegangsniveaus*, *Mappen*, *Postvakken IN*, *Persoonlijke mappen*, *Persoonlijke categorieën*, *Queryresultaten*, *Sessies* en *Gebruikers en groepen*. Stel alle andere tabbladen in op *Overgenomen*.
Inhoudbeheerders	Verleen toegang tot *Kalenders*, *Categorieën*, *Gebeurtenissen*, *Mappen*, *Exemplaarbeheer*, *Persoonlijke categorieën*, *Persoonlijke mappen*, *Profielen*, *Queryresultaten* en *Universes*. Stel alle andere tabbladen in op *Overgenomen*.
Serverbeheerders	Verleen toegang tot *Servers* en *Toepassingen.* Stel alle andere tabbladen in op *Overgenomen*.

18.2.3.1.3.2.1.4 Rechten beheren om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te configureren

In een grootschalige bedrijfsomgeving moet een systeembeheerder het beheer van CMC-tabtoegang mogelijk delegeren aan een gedelegeerde beheerder. In een systeem met meerdere tenants heeft elke tenant mogelijk een gedelegeerde beheerder die verantwoordelijk is voor het beheer van CMC-tabtoegang voor andere gebruikers en gebruikersgroepen.

1. Meld u aan bij de CMC.
2. Klik met de rechtermuisknop op het tabblad *Gebruikers en groepen* op een principal en selecteer *CMC-tabconfiguratie*.
   In het dialoogvenster *CMC-tabtoegang configureren* wordt *Rechten voor configuratie van CMC-tabtoegang voor andere gebruikers of gebruikersgroepen* weergegeven voor de principal.

   > **Opmerking**
   >
   > Als dit recht wordt verleend, kan de principal CMC-tabtoegang beheren (alleen voor tabbladen waarvoor de principal toegang heeft) voor gebruikers waarvoor de principal het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* heeft. Bovendien kan de principal

> het beheer van CMC-tabtoegang aan andere gebruikers delegeren door *Rechten voor configuratie van CMC-tabtoegang voor andere gebruikers of gebruikersgroepen* te verlenen aan gebruikers waarvoor de principal het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* heeft.

- □ of □ geeft aan of de principal het recht heeft om CMC-tabbladen voor andere gebruikers of gebruikersgroepen te configureren.
- *Overgenomen* geeft aan dat het recht is overgenomen van de bovenliggende gebruikersgroep(en).
- *Expliciet* geeft aan dat het recht expliciet is opgegeven op het niveau van de principal.

3. Bekijk de rechten om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te configureren. Als u de rechten wilt wijzigen, kunt u een van de volgende instellingen in de lijst selecteren:
   - Klik op *Verlenen* om expliciet het recht te verlenen om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te beheren.
   - Klik op *Weigeren* om expliciet het recht te weigeren om CMC-tabtoegang voor andere gebruikers of gebruikersgroepen te beheren.
   - Klik op *Overnemen* om het recht voor beheer van CMC-tabtoegang voor andere gebruikers of groepen over te nemen.

   > ⓘ Opmerking
   >
   > Wanneer u een instelling in de lijst selecteert, wordt het recht van de principal onmiddellijk gewijzigd.

4. Klik op *Sluiten* als u klaar bent.

Het nieuwe recht dat van kracht is, wordt weergegeven.

Verwante informatie

Gedelegeerd beheer en CMC-tabtoegang [pagina 698]
Overname van CMC-tabtoegang [pagina 701]

18.2.3.1.3.2.1.5 Een tabblad Aanpassing toevoegen voor een gebruiker of gebruikersgroep

CMC-tabtoegang moet worden ingesteld op “Beperkt” voordat u een tabblad *Aanpassing* voor een gebruiker of gebruikersgroep kunt toevoegen.

1. Ga in de CMC naar het beheergebied *Gebruikers en groepen*.
2. Klik met de rechtermuisknop op een gebruiker of gebruikersgroep en selecteer *CMC-tabconfiguratie*.

   Het dialoogvenster *CMC-tabconfiguraties* wordt weergegeven met de titel van elk CMC-tabblad en het machtigingsniveau voor de gebruikersgroep.

   Als de volgende waarschuwing rood boven aan het dialoogvenster wordt weergegeven, moet u CMC-tabtoegang instellen op beperkt voordat u een tabblad *Aanpassing* kunt toevoegen:

   ```
   Waarschuwing: toegang tot CMC-tabbladen is momenteel onbeperkt. Als u CMC-
   toegang wilt beperken, klikt u op de tab Toegang, selecteert u 'CMC' en stelt
   ```

```
u de toegang tot CMC-tabbladen in op beperkt. De volgende instellingen worden
van kracht nadat toegang tot CMC-tabbladen beperkt is:
```

3. (Indien vereist) Toegang tot CMC-tabbladen instellen op beperkt:
   a. Klik in het beheergebied *Toepassingen* van de CMC met de rechtermuisknop op *Central Management Console* en selecteer *Configuratie van CMC-tabtoegang*.
   b. Selecteer onder *CMC-tabtoegang* de optie *Beperkt* en klik op *Opslaan en sluiten*.
4. Selecteer in het dialoogvenster *CMC-tabbladen configureren* voor de gebruikersgroep voor elk CMC-tabblad de optie *Verleend*, *Geweigerd* of *Overgenomen*.
   Wanneer u de machtiging voor een tabblad wijzigt, wordt de machtiging van een gebruikersgroep in het dialoogvenster CMC-tabbladen configureren bijgewerkt om tabtoegang voor andere gebruikers of gebruikersgroepen te configureren.
5. Klik op *Sluiten*.

18.2.3.1.3.2.2 CMC-tabtoegang beperken

Het is raadzaam om CMC-tabtoegang eerst voor principals te configureren en vervolgens CMC-tabtoegang te beperken. Als u tabtoegang eerst beperkt en vervolgens configureert, hebben uw gebruikers geen toegang tot CMC-tabbladen tot een beheerder toegang verleent.

Teneinde consistentie met eerdere versies van het BI-platform te garanderen, is CMC-tabtoegang bij de installatie van BI-platform onbeperkt, en heeft een gebruiker met toegang tot de CMC ook toegang tot alle beschikbare tabbladen. Een systeembeheerder kan CMC-tabtoegang beperken om te voorkomen dat gebruikers toegang hebben tot tabbladen waarvoor ze geen toegangsrechten hebben.

In noodgevallen of als u problemen met de configuratie van CMC-tabtoegang wilt oplossen, kunt u de beperking van CMC-tabtoegang opheffen (bijvoorbeeld wanneer een gedelegeerde beheerder geen toegang heeft tot een essentieel CMC-tabblad).

1. Meld u aan bij de CMC.
2. Klik met de rechtermuisknop op het tabblad *Toepassingen* op *Central Management Console* en selecteer *Configuratie van CMC-tabtoegang*.
   Nu wordt het dialoogvenster *CMC-tabtoegang* weergegeven.
3. Configureer de regel voor CMC-tabtoegang.
   - Selecteer *Beperkt* om de toegang van uw gebruikers te beperken tot tabbladen waarvoor ze rechten hebben.
   - Selecteer *Onbeperkt* om uw gebruikers toegang tot alle tabbladen te verlenen.
4. Wanneer u klaar bent, klikt u op *Opslaan en sluiten*.

De regel voor CMC-tabtoegang wordt op het systeem toegepast.

Verwante informatie

Problemen met CMC-tabtoegang oplossen [pagina 705]

18.2.3.1.3.2.3 Problemen met CMC-tabtoegang oplossen

U kunt problemen met de CMC-tabtoegangsrechten van een gebruiker oplossen om onbevoegde toegang te voorkomen of om problemen met de beperkte toegang van een gebruiker tot CMC-tabbladen op te lossen.

1. Meld u als beheerder bij de CMC aan.

   > **Opmerking**
   >
   > Zorg dat u toegang hebt tot het tabblad waarvoor u problemen wilt oplossen, en dat u het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* voor de gebruiker hebt.

2. Klik met de rechtermuisknop op een principal op het tabblad *Gebruikers en groepen* en selecteer *CMC-tabconfiguratie*.
   Nu wordt het venster *CMC-tabtoegang configureren* weergegeven.
3. Bekijk de huidige CMC-tabtoegang. U kunt toegang tot beschikbare tabbladen expliciet verlenen of weigeren.

   Als de CMC-tabtoegang wordt overgenomen, maar de huidige tabtoegang sluit niet aan op de vereisten van de gebruiker:

   a. Stel een lijst samen van alle gebruikersgroepen waarvan de geselecteerde principal lid is.
   b. Herhaal stap 1-3 voor elke groep waarvan de gebruiker tabtoegang overneemt.
   c. Corrigeer CMC-tabtoegang op principalniveau of onder het groepsniveau, waar nodig.

   > **Opmerking**
   >
   > Wanneer u deze taak op het groepsniveau uitvoert, heeft dit effect op de CMC-tabtoegang voor alle gebruikers die lid zijn van deze gebruikersgroep, en alle gebruikers die lid zijn van gebruikersgroepen die van deze gebruikersgroep zijn overgenomen, mits CMC-tabtoegang voor deze gebruikers is ingesteld op *Overgenomen*.

4. Klik op *Sluiten* als u klaar bent.

Verwante informatie

CMC-tabtoegang voor andere gebruikers beheren [pagina 700]
Overname van CMC-tabtoegang [pagina 701]

18.2.3.2 Instellingen van het BI-startpunt beheren

Deze sectie helpt u bij het beheren van de volgende instellingen in het BI-startpunt:

- Weergave-instellingen voor het BI-startpunt wijzigen.
- Configureren van RESTful URL-details in Central Management Console voor aanmelding bij het BI-startpunt.
- Instellen van tabblad Verificatie en CMS-zichtbaarheid in het BI-startpunt.

- Configureren van e-mailkoppeling voor optie *Contact opnemen met beheerder* in het BI-startpunt.

18.2.3.2.1 Configureren van RESTful URL-details in CMC voor aanmelding bij het aan SAP Fiori aangepaste BI-startpunt.

Nadat u BI 4.2 SP4 hebt geïnstalleerd of geüpgraded, moet u RESTful Web Services URL configureren voor een gebruiker zodat deze zich kan aanmelden bij het aan SAP Fiori aangepaste BI-startpunt.

Voer de volgende stappen uit om RESTful Web Services URL-details in CMC te configureren:

1. Meld u als beheerder aan bij de CMC.
2. Navigeer naar *Beheren* > *Applicaties* > *RESTful Web Services* > *Eigenschappen*.
3. Geef de WACS URL op (hostnaam of volledig gekwalificeerde naam waar de WACS-server wordt geïmplementeerd).

18.2.3.2.2 Proxyinstellingen configureren om Web Assistant te activeren in het Fiorified BI-startpunt

Nadat u BI 4.2 SP5 hebt geïnstalleerd of geüpgraded, moet u proxyinstellingen configureren voor een gebruiker zodat deze toegang krijgt tot de in-app Help van Web Assistant in het Fiorified BI-startpunt.

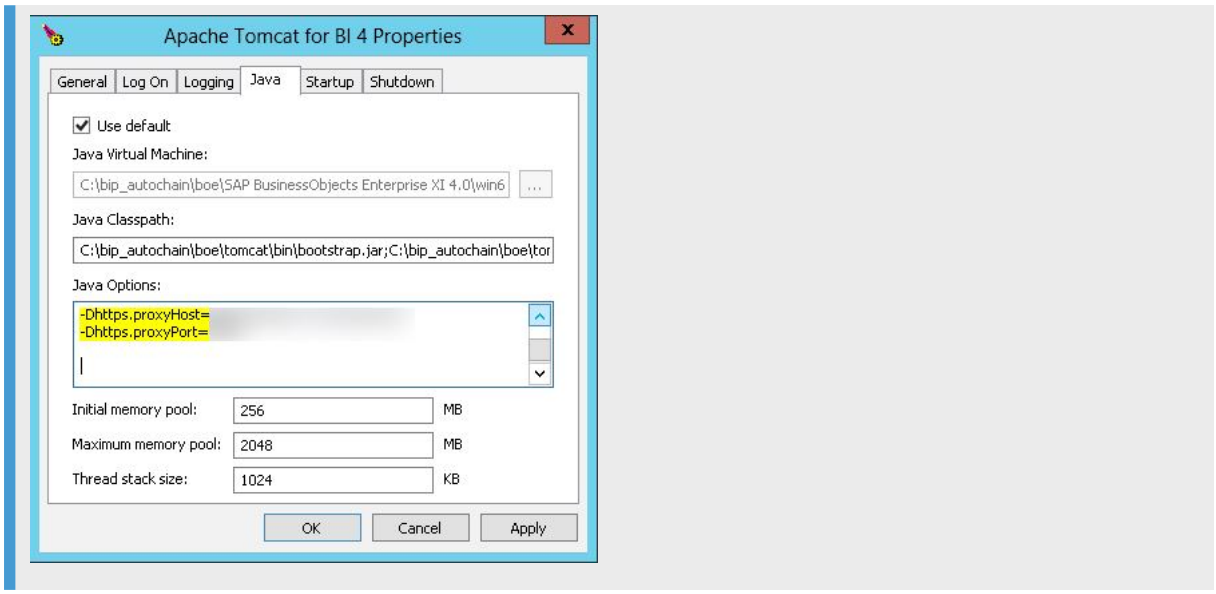
Voer de volgende stappen om proxyinstellingen te configureren voor Web Assistant in het Fiorified BI-startpunt:

Vereisten:

U hebt verbinding met internet.

1. Navigeer naar de systeemeigenschappen van de webserver.
2. Voeg de eigenschappen `https.proxyHost` en `https.proxyPort` toe.

> **Voorbeeld**
>
> Besturingssysteem: Windows, Web Server: Tomcat 8.5
>
> 1. Navigeer naar *Windows* > *Tomcat*.
> Het venster *Apache Tomcat for BI 4 Properties* (Eigenschappen Apache Tomcat for BI 4)wordt geopend.
> 2. Kies het tabblad *Java*.
> 3. Voeg in het veld met opties voor Java de volgende eigenschappen toe aan de lijst:
> `-Dhttps.proxyHost=<proxy_host>`
> `-Dhttps.proxyPort=<proxy_port>`
> 4. Start Tomcat opnieuw.



18.2.3.2.3 Configureren van e-mailkoppeling voor optie Contact opnemen met beheerder in het aan SAP Fiori aangepaste BI-startpunt

Voer de volgende stappen uit om de e-mailkoppeling voor optie *Contact opnemen met beheerder* in het aan SAP Fiori aangepaste BI-startpunt te configureren:

1. Ga naar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Als de Tomcat-versie samen met BI-platform is geïnstalleerd, kunt u ook toegang verkrijgen tot de volgende locatie: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Creëer met Notepad een nieuw bestand en sla dit op onder de volgende naam: 'FioriBI.properties'.
3. Wijzig de volgende eigenschap in het bestand: `admin.user.email=administrator@bilp.com` om de e-mail-ID van de beheerder op te nemen.

18.2.3.2.4 Instellen van tabblad Verificatie en CMS-zichtbaarheid in het aan SAP Fiori aangepaste BI-startpunt

Voer de volgende stappen uit om het tabblad Verificatie en CMS-zichtbaarheid in het aan SAP Fiori aangepaste BI-startpunt.in te stellen:

1. Ga naar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

Als u Tomcat gebruikt die bij BI-platform is geïnstalleerd, kunt u ook toegang verkrijgen tot de volgende locatie: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.

2. Creëer met Notepad een nieuw bestand en sla dit op onder de volgende naam: 'FioriBI.properties'.
3. Als u de verificatieopties wilt opnemen in het aanmeldingsvenster van BI-startpunt, voegt u het volgende toe: `authentication.visible=true`.

   Vervang <authentication> door standaardverificatietypen: "secEnterprise, secLDAP, secWinAD, secSAPR3".
4. Als u het standaardverificatietype wilt wijzigen, voegt u het volgende toe: `authentication.default=<authentication>`.
5. Als u gebruikers wilt vragen om de CMS-naam in het aanmeldingsvenster van BI-startpunt, voegt u het volgende toe: `cms.visible=true`.
6. Sla het bestand op en sluit het.
7. Start de webtoepassingsserver opnieuw op.

18.2.3.2.5 Weergave-instellingen voor het BI-startpunt wijzigen

1. Ga naar het gebied *Toepassingen* in de CMC en dubbelklik op *BI-startpunt*.
   Het dialoogvenster *Eigenschappen van BI-startpunt* wordt weergegeven.
2. Schakel het selectievakje *Tabblad Filters weergeven op de pagina Planning* in om filters voor planning in te schakelen.

   Deze instelling bepaalt of gebruikers formules voor record- of groepselectie kunnen invoeren als ze een Crystal Reports-rapport plannen.
3. Klik op *Opslaan en sluiten*.

18.2.3.3 Web Intelligence-instellingen beheren

U kunt voor Web Intelligence-documenten bepalen tot welke functies uw gebruikers toegang hebben door eigenschappen in te stellen voor de Web Intelligence-toepassing.

18.2.3.3.1 Weergave-instellingen voor Web Intelligence wijzigen

1. Ga naar het gebied *Toepassingen* in de CMC en selecteer *Web Intelligence*.
2. Klik op *Beheren* > *Eigenschappen.*
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
3. Definieer een of meer van de volgende weergaveopties.

Optie	Beschrijving
Gewijzigde opties voor gegevensweergave > *Dimensies en details*	Met de opties in dit gebied geeft u aan hoe toegevoegde gegevens moeten worden weergegeven in rapporten en kunt u de letterstijl, tekstkleur en achtergrondkleur wijzigen. Uw wijzigingen worden automatisch weergegeven in een voorbeeldweergave van een cel. Klik tot slot op *OK*.
Gewijzigde opties voor gegevensweergave > *Fluctuerende meetwaarden (numerieke meetwaarden)*	Met de opties in dit gebied kunt u de paginakoptekst wijzigen en opmaken, en de letterstijl, tekstkleur en achtergrondkleur wijzigen. Uw wijzigingen worden automatisch weergegeven in een voorbeeldweergave van een cel. Klik tot slot op *OK*.
Eigenschappen van ingesloten afbeelding	Voer de maximumgrootte van de ingesloten afbeelding in.
Ondersteuning voor landkaarten	Schakel de ondersteuning voor landkaarten in Web Intelligence in of uit.
Eigenschappen van modus Snelle weergave	Geef in de daarvoor bestemde velden het maximum aantal verticale records, het maximum aantal horizontale records, de maximale paginabreedte, de minimale paginahoogte, een waarde voor Rechts opvullen en een waarde Onder opvullen op.
Instellingen voor Automatisch opslaan	Stel het interval in waarmee documenten automatisch worden opgeslagen. Dit interval wordt opnieuw ingesteld wanneer een document handmatig of automatisch wordt opgeslagen. Het document dat automatisch is opgeslagen, wordt ook verwijderd wanneer u een document handmatig sluit.
Automatisch vernieuwen	Hiermee worden Web Intelligence-documenten automatisch vernieuwd wanneer de Web Intelligence-documenteigenschap *Automatisch vernieuwen* is geselecteerd. Raadpleeg de *Gebruikershandleiding voor SAP BusinessObjects Web Intelligence* voor meer informatie.
Automatisch samenvoegen	Hiermee worden dimensies automatisch samengevoegd wanneer de Web Intelligence-documenteigenschap *Dimensies automatisch samenvoegen* is geselecteerd. Raadpleeg de *Gebruikershandleiding voor SAP BusinessObjects Web Intelligence* voor meer informatie.
Document automatisch vernieuwen bij het openen van instellingen voor beveiligingsrecht	Wis deze optie om Web Intelligence in staat te stellen om documenten bij het openen automatisch te vernieuwen, zonder de optie *Vernieuwen bij openen* in de Web Intelligence-documenteigenschappen in te schakelen. Wanneer u deze optie selecteert, wordt het beveiligingsrecht *Documenten - automatisch vernieuwen bij openen uitschakelen* geselecteerd.
Slimme weergave	Deze optie bepaalt welke documentversie wordt weergegeven wanneer gebruikers documenten openen in Web Intelligence. • Nieuwste exemplaar weergeven Het nieuwste exemplaar van het object wordt geopend. Als een document bijvoorbeeld elk uur moet worden vernieuwd en het document is vijf uur geleden voor het laatst opgeslagen en gesloten, wordt het nieuwste exemplaar geopend. • Object weergeven Het document wordt geopend in dezelfde status die het had toen het voor het laatst werd opgeslagen, ongeacht geplande vernieuwingen die mogelijk zijn uitgevoerd.

Optie	Beschrijving
JavaScript	Hier selecteert u dat cellen worden weergegeven met Inhoud lezen als HTML of Inhoud lezen als hyperlink in Web Intelligence-documenten: • *JavaScript uitschakelen, en hyperlinks en enkel de HTML-elementen die door Web Intelligence worden gebruikt, inschakelen* Met deze standaardoptie worden hyperlinks en de beperkte set HTML-elementen die vereist zijn voor Web Intelligence-functies, ingeschakeld. JavaScript en de andere HTML-elementen uit de documenten worden verwijderd. • *Enkel op de pagina Geautoriseerde HTML-elementen gedefinieerde HTML-elementen inschakelen* Met deze optie worden enkel de HTML-elementen en attributen ingeschakeld die u opgeeft op de pagina *Geautoriseerde HTML-elementen*. • *JavaScript, HTML-elementen en hyperlinks inschakelen* Met deze optie schakelt u alle JavaScript, HTML-elementen en hyperlinks in. Wanneer u de optie wijzigt, meld u dan eerst af en weer aan bij de toepassing om de wijzigingen in Web Intelligence te zien. ⚠ Let op • Dankzij de mogelijkheden voor formules biedt Web Intelligence ingesloten JavaScript/HTML-code in documentcellen. Deze code kan worden ingeschakeld of uitgeschakeld in de Central Management Console. Door JavaScript, HTML's en hyperlinks te autoriseren, erkent u echter het risico dat u wordt blootgesteld aan cross-site scripting. Met cross-site scripting kunnen aanvallers websites aanpassen of codes uitvoeren op andere systemen. Deze kwetsbaarheid heeft invloed op producten zoals internetbrowsers wanneer ze scripts uitvoeren. In de meeste gevallen zijn cross-site scripting-aanvallen het gevolg van onbeveiligd programmeren op het doelsysteem. • De code kan worden afgestemd door HTML-codes en -attributen in *BI-beheerderstudio* > *Toepassingen* > *HTML-elementen* te autoriseren. SAP is echter niet verantwoordelijk voor de compatibiliteit van deze code en de mogelijke neveneffecten. Uw code kan bijvoorbeeld mogelijk enkele aanpassingen vereisen vanwege browserupdates, ondersteuning voor de JavaScript-code of de manier waarop de code dynamisch wordt ingesloten op de webpagina. De code vereist mogelijk enkele aanpassingen om in die nieuwe context te worden uitgevoerd.
Inhoud uitlijnen voor nieuwe documenten	Gebruik deze opties om te definiëren of de inhoud van een nieuw document van rechts naar links of van links naar rechts moet worden uitgelijnd, of dat het moet afhangen van de voorkeurslandinstelling voor weergave en/of landinstelling van het product van de gebruiker.
Feature Toggle	Gebruik dit tekstveld om schakelopties in te voeren om voorbeeldfuncties in te schakelen. Deze schakelopties kunnen ook worden gebruikt in SAP Notes om standaardgedrag aan te passen. Deze lijst met schakelopties moet worden ingevoerd als een lijst in de JSON-indeling.

4. Klik op *Opslaan en sluiten*.

> **Opmerking**
>
> als u de selectie wilt terugzetten naar de standaardvariabelen voor weergave, klikt u op *Opnieuw instellen*.

18.2.3.3.2 Services met aangepaste elementen

Aangepaste elementen zijn visualisaties waarvan het genereren van de weergave is gedelegeerd aan externe services van derden door Web Intelligence.

In Web Intelligence-documenten worden aangepaste elementen geïntegreerd en weergegeven, zoals elk ander rapportelement (diagrammen, tabellen, enz.) Services met aangepaste elementen moeten eerst in de CMC worden geconfigureerd, zodat eindgebruikers aangepaste elementen in Web Intelligence-documenten kunnen visualiseren.

Aangezien uw gegevens worden overgedragen tussen de BOE-server en de server voor aangepaste elementen van een derde partij, is het aan te bevelen de server voor aangepaste elementen op uw intranet te implementeren. Als dit niet mogelijk is, raden we aan uitsluitend HTTPS te gebruiken voor toegang tot de server voor aangepaste elementen.

> **Let op**
>
> De door u geïmplementeerde service Aangepaste elementen voegt code toe aan Web Intelligence en kan potentiële beveiligingsproblemen zoals cross-site scripting genereren. Met cross-site scripting kunnen aanvallers code en scripts uitvoeren op computers van andere gebruikers. Een beveiligingingswaarschuwing vraagt uw expliciete toestemming voordat u de service Aangepaste elementen implementeert. Uw toestemming is verplicht om de service Aangepaste elementen te implementeren.

Migratie

Wanneer u een Web Intelligence-document van de ene CMS naar de andere migreert, moet de service met aangepaste elementen waarmee de inhoud in dit document is gecreëerd opnieuw worden gecreëerd in de nieuwe CMS, met dezelfde naam. Als de service met aangepaste elementen niet opnieuw (met dezelfde naam) wordt gecreëerd in de nieuwe CMS, kunnen de aangepaste elementen in het gemigreerde document niet langer worden gewijzigd.

18.2.3.3.2.1 Een service met aangepaste elementen toevoegen

U moet als beheerder eerst de externe service opgeven die de weergave afhandelt voordat eindgebruikers aangepaste elementen kunnen gebruiken. Standaard is er geen service met aangepaste elementen geactiveerd. Deze instelling is optioneel en moet worden ingeschakeld in de CMC.

U hebt de URL van de service met aangepaste elementen toegevoegd aan de lijst met vertrouwde URL's. Raadpleeg de sectie Vertrouwde URL's toevoegen aan de lijst met geautoriseerde URL's [pagina 717] als u dit niet hebt gedaan.

1. Open de CMC (Central Management Console).
2. Klik op *Applicaties*.
3. Klik met de rechtermuisknop op *Web Intelligence*.
4. Klik op *Eigenschappen*.
5. Klik op *Aangepaste elementen*.
6. Klik op *Service toevoegen*.
7. Geef de service een naam.

   > ⚠ Let op
   >
   > De naam van de service wordt ongewijzigd weergegeven in Web Intelligence-clients en moet uniek zijn. U kunt een servicenaam die al bestaat niet opnieuw gebruiken. Als u de naam van een service wijzigt, is het niet meer mogelijk om de aangepaste elementen te wijzigen die met deze service in Web Intelligence-documenten zijn gemaakt.

8. Voer een URL met het poortnummer in.
9. Klik op *Testen*.
10. Selecteer een *Mediatype*.

    Web Intelligence kan de mediatypen HTML of bitmap gebruiken. Het voorkeursmediatype is HTML (tekst/html) dat interactiviteit in Web Intelligence-clients en een betere gebruikerservaring mogelijk maakt. Bitmapmediatypen kunnen .PNG (afbeelding/png), .JPG (afbeelding/JPG) of .GIF (afbeelding/gif) zijn.
11. Voer de *DPI van afbeelding* in.

    > ⓘ Opmerking
    >
    > Dit is de resolutie van de bitmapafbeeldingen die door de service zijn gegenereerd. Voor de publicatie van Web Intelligence-rapporten als PDF- of Excel-bestanden is een bitmapindeling noodzakelijk terwijl aangepaste elementen worden weergegeven als afbeeldingen. Zonder bitmapindeling wordt in deze publicaties een leeg blok weergegeven in plaats van het verwachte aangepaste element.

12. Klik op *OK*.

    > ⓘ Opmerking
    >
    > U kunt verschillende services met aangepaste elementen tegelijkertijd gebruiken. Eén service kan meerdere aangepaste elementen leveren.

Verwante informatie

URL's autoriseren [pagina 716]

18.2.3.3.3 Parallelle vernieuwing gegevensprovider

Met 'Parallelle vernieuwing gegevensprovider' worden de prestaties van gegevensvernieuwing verbeterd in Web Intelligence-documenten die meerdere gegevensproviders bevatten.

Om query's tegelijk te vernieuwen, verspreidt Web Intelligence alle gegevensproviders over meerdere threads. Deze functie is standaard geactiveerd en Web Intelligence kan tot 64 query's tegelijk vernieuwen. Gegevensproviders op basis van relationele, OLAP- en BICS-verbindingen, en persoonlijke-gegevensproviders (tekstbestanden, FHSQL) worden ondersteund.

> **⚠ Beperking**
>
> Excel-gegevensproviders worden niet ondersteund.

U kunt deze waarde in de Central Management Console verlagen als de hardware waarop Web Intelligence wordt uitgevoerd een dergelijke werkbelasting niet ondersteunt. Zorg ervoor dat uw hardware over voldoende kernen beschikt om optimale prestaties te kunnen garanderen.

Er zijn twee globale parameters beschikbaar in de Central Management Console:

- *Maximumaantal parallelle query's per document*: stel het maximumaantal gegevensproviders in dat Web Intelligence per document tegelijkertijd kan vernieuwen. De standaardwaarde is 64.
- *Parallelle query's voor planning inschakelen*: schakel de parallelle queryverwerking in of uit bij het plannen van documenten. Deze optie is standaard ingeschakeld.

We raden u tevens aan om elke databaseverbinding te verfijnen met een parameter waarmee u het aantal query's kunt instellen dat tegelijkertijd kan worden uitgevoerd. Deze parameter heet 'Maximumaantal parallelle query's' en is beschikbaar:

- In de Central Management Console of het hulpprogramma voor informatieontwerp voor OLAP- en BICS-verbindingen.
- In het hulpprogramma voor informatieontwerp of het hulpprogramma voor universeontwerp voor relationele verbindingen.

Voor elke verbinding is het aantal gegevensproviders dat tegelijkertijd kan worden vernieuwd standaard ingesteld op 4. De databasebeheerder kan deze waarde aanpassen in overeenstemming met de hardware van de database. Voor tekstbestanden is de standaardwaarde ingesteld op 1.

Voorbeeld

In dit voorbeeld zijn alle standaardwaarden behouden en ondersteunt elke verbinding een maximumaantal van 4 parallelle vernieuwingstaken.

Verbinding	Aantal te vernieuwen gegevensproviders
2 OLAP-verbindingen	6 (5 op Verbinding 1, 1 op Verbinding 2)
1 Relationele verbinding	2
1 BICS-verbinding	2

Verbinding	Aantal te vernieuwen gegevensproviders
Excelbestanden uit een persoonlijke gegevensprovider	2

Beide Excelbestanden worden na elkaar vernieuwd omdat ze niet worden ondersteund door de functie 'Parallelle vernieuwing gegevensprovider' .

Vier van de gegevensproviders van de eerste OLAP-verbinding worden gelijktijdig vernieuwd op threads 1, 2, 3 en 4. De vijfde wordt in de wachtrij geplaatst en zal worden verwerkt zodra één van de gegevensproviders (van eender welke verbinding) is vernieuwd. De gegevensprovider van de tweede OLAP-verbinding wordt vernieuwd op thread 5, omdat deze van een andere verbinding is.

De vier gegevensproviders van de relationele en de BICS-verbinding worden gelijktijdig vernieuwd op threads 5, 6, 7 en 8.

> **Opmerking**
>
> Telkens wanneer er meer gegevensproviders van hetzelfde type zijn dan de opgegeven waarde, worden ze in de wachtrij geplaatst om te wachten totdat andere gegevensproviders zijn voltooid.

Verwante informatie

Aantal gegevensproviders dat parallel vernieuwd wordt per document wijzigen [pagina 714]
Aantal gegevensproviders dat parallel vernieuwd wordt voor een specifieke OLAP-verbinding wijzigen [pagina 715]

18.2.3.3.3.1 Aantal gegevensproviders dat parallel vernieuwd wordt per document wijzigen

1. Klik in het startscherm van de CMC op *Servers*.
2. Klik op *Web Intelligence-services*.
3. Klik met de rechtermuisknop op *Web Intelligence-verwerkingsserver* en klik op *Eigenschappen*.
4. Voer in het invoerveld *Maximumaantal parallelle query's* een aantal in.

   De mogelijke waarden hebben een bereik van 0 tot 64.

   > **Opmerking**
   >
   > Als u 0 invoert, schakelt u de functie voor het vernieuwen van gegevensproviders uit.

18.2.3.3.3.2 Parallelle queryverwerking voor planning uitschakelen

1. Klik in het startscherm van de CMC op *Servers*.
2. Klik op *Web Intelligence-services*.
3. Klik met de rechtermuisknop op *Web Intelligence-verwerkingsserver* en klik op *Eigenschappen*.
4. Schakel *Parallelle query's voor planning inschakelen* uit.

18.2.3.3.3.3 Aantal gegevensproviders dat parallel vernieuwd wordt voor een specifieke OLAP-verbinding wijzigen

1. Klik op het startscherm op *OLAP verbindingen*.
2. Blader naar de verbinding die u wilt configureren en klik met de rechtermuisknop erop.
3. Selecteer *Ordenen* > *Bewerken*.
4. Voer in het invoerveld *Maximumaantal parallelle query's* een aantal in.

   De mogelijke waarden hebben een bereik van 1 tot 64.

   > **Opmerking**
   >
   > Als u 1 invoert, worden gegevensproviders sequentieel vernieuwd.

18.2.3.3.4 Beveiliging voor CSV-exports

Web Intelligence biedt een beveiligingsmaatregel ter voorkoming van opdrachtinjectie wanneer gebruikers een CSV-bestand openen dat is gegenereerd op basis van een document in Microsoft Excel. U kunt deze beveiliging voor CSV-exports uitschakelen.

Standaard voegt Web Intelligence bij het exporteren naar CSV of een CSV-archief een spatie toe voorafgaand aan de volgende tekens:

- = (gelijk aan)
- + (plus)
- - (minus)
- @ (at)

De extra spatie zorgt ervoor dat waarden met deze tekens niet worden uitgevoerd als opdracht, wat een beveiligingsprobleem in uw systeem zou kunnen veroorzaken.

Verwante informatie

Beveiliging uitschakelen voor CSV-exporten [pagina 716]

18.2.3.3.4.1 Beveiliging uitschakelen voor CSV-exporten

Als u de standaardbeveiligingsmaatregel in Web Intelligence wilt uitschakelen waarmee opdrachtinjectie wordt voorkomen wanneer gebruikers een geëxporteerd CSV-bestand openen in Microsoft Excel, wijzigt u de bijbehorende registersleutel.

Stel de waarde van de registersleutel `EscapeCharactersForCSVExport` in op 'false' om de beveiligingsmaatregel uit te schakelen. Standaard is de registersleutel niet aanwezig en is de waarde ingesteld op 'true'. Mogelijk moet u de sleutel dus maken om de waarde op 'false' te kunnen instellen.

De wijziging gaat in nadat Web Intelligence-gebruikers de toepassing hebben gesloten en opnieuw hebben geopend.

Wijzig de registersleutel als volgt:

- Stel in Windows de registersleutel in op 'false' op de server- en clientcomputers: `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.
- Stel in UNIX op de servercomputers in `$installdir/setup/boconfig.cfg` de registerdeclaratiesleutel in op 'false' `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.

18.2.3.3.5 URL's autoriseren

Web Intelligence gebruikt URL's voor:

- Hyperlinks in het document
- Hyperlinks in aanwijzingen
- Achtergrondafbeelding
- OData-gegevensbron
- Aangepaste elementen of externe uitbreidingen

Deze URL's kunnen mogelijk beveiligingsbedreigingen veroorzaken.

Als beheerder moet u in de Central Management Console een lijst met vertrouwde URL's maken die gebruikers kunnen gebruiken. Deze lijst bepaalt het gebruik van deze URL's in Web Intelligence.

18.2.3.3.5.1 Vertrouwde URL's toevoegen aan de lijst met geautoriseerde URL's

Wanneer u een URL in Web Intelligence wilt gebruiken als hyperlink in het document of een aanwijzingshint, een achtergrondafbeelding, een OData-gegevensbron, of een nieuwe aangepaste service of externe uitbreiding, moet u deze eerst autoriseren.

1. Klik op het startscherm van de Central Management Console op *Toepassingen*.
2. Selecteer *Web Intelligence*.
3. Selecteer in het contextmenu de optie *Eigenschappen*.
4. Selecteer de sectie *Categorie geautoriseerde URL's*.
5. Klik op de knop *Nieuwe URL toevoegen* om een nieuwe vertrouwde URL toe te voegen.
6. Geef in het veld *Geautoriseerde URL* een unieke URL op, met protocol, hostnaam en poort.

   > → Tip
   >
   > U kunt het teken * typen om elke URL voor een hyperlink of achtergrondafbeelding of OData-gegevensbron te autoriseren. Vervolgens moet u op het selectievakje *Ik accepteer het risico* klikken om te bevestigen dat u het mogelijke risico van het inschakelen van alle URL's begrijpt.

7. Als de ingevoerde URL een URL is naar een uitbreiding of service voor aangepaste elementen die toegankelijk is via een proxy, kunt u het selectievakje *Als deze URL wordt gebruikt voor een aangepast element of een uitbreiding waarvoor een proxy is vereist, voer dan de server en poort ervan in* inschakelen om deze proxyserver en poort in te stellen.
8. Klik op *OK*.

18.2.3.4 Crystal Reports-instellingen beheren

18.2.3.4.1 Slimme weergave inschakelen in Crystal Reports

1. Ga naar het gebied *Toepassingen* in de CMC en selecteer *Crystal Reports*.
2. Kies *Eigenschappen* > *beheren*
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
3. Kies *BI-startpunt*.
4. Definieer de volgende weergaveoptie:

Optie	Beschrijving
Slimme weergave	Deze optie bepaalt welke documentversie wordt weergegeven wanneer gebruikers een Crystal Report openen. • Nieuwste exemplaar weergeven Het nieuwste geslaagde exemplaar van het object wordt geopend. Als een document bijvoorbeeld elk uur moet worden vernieuwd en het document vijf uur geleden voor het laatst is opgeslagen en gesloten, wordt het nieuwste geslaagde exemplaar geopend. • Object weergeven Het document wordt geopend in dezelfde status die het had toen het voor het laatst werd opgeslagen, ongeacht geplande vernieuwingen die mogelijk zijn uitgevoerd.

18.2.3.4.2 Ja-bibliotheek voor gebruikersfuncties inschakelen voor Crystal Reports voor Enterprise

U kunt het rapport weergeven dat de Java-UFL (User Function Library, bibliotheek voor gebruikersfuncties) bevat. Volg de onderstaande stappen:

1. Meld u aan bij de CMC.
2. Kies *Toepassingen* in de vervolgkeuzelijst.
3. Kies *Crystal Reports-configuratie*.
4. Selecteer op het linkerpaneel onder *Eigenschappen* de optie *Crystal Reports voor Enterprise*.
5. Kies de optie *Nieuwe toevoegen* en voer de volgende eigenschappen in:

Eigenschap	Waarde	Aanvullende informatie
classpath	Het klassepad naar de Java-UFL's.	• Gebruik een puntkomma als scheidingsteken voor meerdere JAR-bestanden. • Gebruik een dubbele backslash (\\) of gebruik in plaats daarvan een forwardslash (/). • Voorbeeld: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\java\\lib\\MyFirstUFL.jar
ExternalFunctionLibraryClassNames.classname	De volledig gekwalificeerde naam van de UFL.	Voorbeeld: samples.ufl.InternationalizationLibrary

6. Start aan Crystal Reports gerelateerde services opnieuw.
   U kunt nu de werkstromen voor weergave en planning uitvoeren.

18.2.3.4.3 .NET/.COM-bibliotheek voor gebruikersfuncties inschakelen voor Crystal Reports voor Enterprise

U kunt het rapport weergeven dat de .NET/.COM-UFL (User Function Library, bibliotheek voor gebruikersfuncties) bevat. Volg de onderstaande stappen:

1. Kopieer de 64-bits versie van .Net-UFL naar `<Installatiemap>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

   > **Opmerking**
   >
   > SAP Crystal Reports for Enterprise Designer is 64-bits; er is dus een 64-bits .NET-UFL voor nodig. SAP Crystal Reports for Enterprise-services op Business Intelligence-platform daarentegen is 64-bits; hiervoor is een 64-bits .NET-UFL nodig.

2. Registreer en GAC de 64-bits dll via “regasm <dll> en “gacutil /if <dll>”.
3. Meld u aan bij de CMC.
4. Kies *Toepassingen* in de vervolgkeuzelijst.
5. Kies *Crystal Reports-configuratie*.
6. Selecteer op het linkerpaneel onder *Eigenschappen* de optie *Crystal Reports voor Enterprise*.
7. Kies de optie *Nieuwe toevoegen* en voer de volgende eigenschap in:

Categorie	Eigenschap	Waarde
Laat deze kolom leeg.	NonJavaExternalFunctionLibraries.managerDirectory	Pad naar 64-bits UFL-bestand • Gebruik een dubbele backslash (\\) of gebruik in plaats daarvan een forwardslash (/). • Voorbeeld: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\win64_x64).

8. Start de aan Crystal Reports gerelateerde services opnieuw.
   U kunt nu de werkstromen voor weergave en planning uitvoeren.

18.2.3.5 Meldingsinstellingen beheren

In het gebied *Toepassingen* van de CMC in het BI-platform kunt u op systeemniveau instellingen opgeven voor meldingen.

U kunt voor de toepassing *Signalering* bepalen en definiëren hoe systeemgebruikers toegang hebben tot signalen door:

- De map *Mijn signalen* in te schakelen voor de abonnees op signalen.
- Signaalberichten die via e-mail worden verzonden in te schakelen en op te maken.
- Een limiet in te stellen voor het aantal signalen in het systeem.
- Een vervalperiode in te stellen voor signaalberichten.

Verwante informatie

Gebruikersrechten instellen voor toepassingen [pagina 693]

18.2.3.5.1 Eigenschappen voor meldingsdoelen wijzigen

1. Dubbelklik in het gebied *Toepassingen* van de CMC op *Meldingstoepassing*.
2. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Meldingen* wordt weergegeven.
3. (Vereist) Voer een van de volgende acties uit:
   - Selecteer *Mijn meldingen inschakelen* om meldingsabonnees in te schakelen zodat ze meldingen ontvangen onder *Mijn meldingen* in BI-startpunt.
   - Selecteer *E-mail inschakelen* om meldingsabonnees in te schakelen zodat ze meldingen via e-mail ontvangen.
     Er worden algemene e-mailopties voor meldingen weergegeven.
4. Als u *E-mail inschakelen* hebt geselecteerd, voert u de volgende acties uit:
   - Voer in het vakje *Van* het e-mailadres in dat wordt gebruikt om meldingen te versturen.
     Abonnees ontvangen e-mailmeldingen vanaf dit e-mailadres. Gebruik een geldig e-mailadres dat door uw systeem wordt herkend.
   - Voer in het vakje *Aan* het e-mailadres van de meldingsabonnee in.
     Alle systeemmeldingen worden standaard naar dit e-mailadres gestuurd.

     > → Tip
     >
     > Geef geen e-mailadres of ontvanger op. Gebruik de tijdelijke aanduiding *%SI_EMAIL_ADDRESS%*.
   - Voer in het vakje *CC* het e-mailadres in van alle ontvangers die een CC van meldingen moeten ontvangen.
   - Voer in het vakje *Onderwerp* een standaardonderwerptitel in die moet worden gebruikt in e-mails met meldingen.
   - Voer in het vakje *Bericht* een standaardbericht in dat moet worden opgenomen in e-mails met meldingen.
   - Selecteer *Bijlage toevoegen* zodat bijlagen standaard worden opgenomen in e-mails met meldingen.
     Selecteer bijvoorbeeld deze optie om bijbehorende Crystal Reports-rapport met geactiveerde meldingen op te nemen.
   - Als u *Bijlage toevoegen* hebt geselecteerd, selecteert u in *Bestandsnaam* de optie *Automatisch gegenereerd* of *Specifieke naam* om aan te geven hoe bijlagen in e-mails een naam moeten krijgen.

5. Klik op *Opslaan en sluiten*.

Verwante informatie

Gebruikersrechten instellen voor toepassingen [pagina 693]
Meldingsinstellingen beheren [pagina 719]

18.2.3.5.2 Standaardeigenschappen van Signalering wijzigen

1. Ga naar het gebied *Toepassingen* in de CMC en selecteer *Meldingstoepassing*.
2. Klik op *Beheren* > *Eigenschappen* > *Standaardinstellingen*.
3. Stel de toepasselijke waarden in voor de volgende eigenschappen.

Optie	Beschrijving
Vervalperiode	Hiermee geeft u aan hoe lang signalen in het systeem blijven voordat deze worden verwijderd.
Maximumaantal meldingen	Hiermee wordt het maximumaantal meldingen opgegeven dat door het systeem wordt ondersteund. Wanneer de drempel wordt bereikt, verwijdert het systeem 20% van de meldingen, te beginnen met de oudste berichten.

4. Klik op *Opslaan en sluiten*.

Verwante informatie

Meldingsinstellingen beheren [pagina 719]

18.2.3.6 Toepassingsinstellingen beheer BI Commentary

BI Commentary is een toepassing die is geïntroduceerd in de CMC. Hiermee kunnen documentgebruikers samenwerken door opmerkingen te plaatsen bij beschikbare gegevens/statistieken in een bepaald document.

Met BI Commentary kunnen gebruikers can opmerkingen plaatsen bij gegevens/statistieken in de rapporten.

> → Aanbeveling
>
> In BI Commentary worden tabellen standaard gemaakt en verzorgd in de controledatabase.

> **Opmerking**
>
> Voor het gebruik van BI-commentaar met de controledatabase op een niet-Windows-platform, zie de Handleiding voor gegevenstoegang om ODBC stuurprogramma's te configureren.

SAP raadt echter aan om een nieuwe database te configureren waarin opmerkingen uit de toepassing BI-commentaar kunnen worden opgeslagen. Databases met ondersteuning voor BI-commentaar zijn dezelfde als die met ondersteuning voor controle. De ondersteunde databases en corresponderende gecertificeerde JDBC-jar-bestanden voor VI-commentaar omvatten:

- IBM DB2 Workgroup Edition - db2jcc4.jar
- Microsoft SQL Server - sqljdbc4.jar
- MySQL - com.mysql.jdbc_5.1.5.jar
- Oracle - ojdbc6.jar
- SAP HANA - ngdbc.jar
- Sybase Adaptive Server Enterprise - jconn4.jar
- Sybase SQL Anywhere - jconn4.jar

> **Opmerking**
>
> Ongeacht of u BI-commentaar met de controledatabase of een andere ondersteunde database configureert, kan BI-commentaar alleen met de MySQL-database werken als u de MySQL-JDBC-JAR op de volgende locatie plaatst: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.
>
> Als u BI-commentaar configureert met IBM DB2, hebt u in uw systeem een tijdelijke paginagrootte voor tabelruimte nodig van 8K, 16K of 32K. De grootte van de pagina is standaard 4K.

> **Opmerking**
>
> Als de controledatabase niet standaard is geconfigureerd/ingeschakeld, werkt BI Commentary niet tenzij u handmatig een nieuwe database voor BI Commentary configureert.
>
> Als u BI Commentary met controledatabase configureert en u verwijdert de controledatabase, worden alle in de controledatabase opgeslagen opmerkingen ook verwijderd.
>
> De controledatabase gebruikt ODBC of eigen typen databasestuurprogramma's. Voor het configureren van een nieuwe BI Commentary-database hebt u een JDBC-stuurprogramma nodig.

> **Opmerking**
>
> De maximumgrootte van een opmerking is 2000 UTF-8 tekenbytes of 666 UTF-16 tekenbytes.

> **Opmerking**
>
> U kunt opmerkingen niet met het Data Federator-hulpprogramma migreren.

> **Opmerking**
>
> BI-commnetaar wordt niet ondersteund voor MaxDB-verbindingen.

> **Opmerking**
>
> Om commentaargegevens te verwijderen die door de gebruiker zijn gemaakt, gebruikt u de volgende query:
>
> `DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'`

18.2.3.6.1 Nieuwe BI-commentaardatabase configureren

U hebt een JDBC-verbinding gemaakt.

> **Opmerking**
>
> Als u een nieuwe BI-commentaardatabase configureert, is de Commentaar-service in de Adaptive Processing Server verantwoordelijk voor het schrijven van Commentaar-informatie naar de database. De volgende stappen moeten worden genomen op elke computer in de cluster waar de Commentaar-service actief is.

Voer de volgende stappen uit om een JDBC-verbinding te maken:

1. Plaats de JDBC-stuurprogrammacontainer voor de database die u wilt configureren op de volgende locatie: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > **Opmerking**
   >
   > Als u een upgrade uitvoert naar SAP BusinessObjects Business Intelligence Platform 4.2 Support Package 2, en in eerdere versies al een nieuwe database voor BI-commentaar had geconfigureerd, moet u het bestand van het databasestuurprogramma van de 'jdbc'-map verplaatsen naar `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` to `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

2. Start SIA opnieuw.

Ga als volgt te werk om een nieuwe database voor BI-commentaar te configureren:

1. Meld u aan bij de CMC.
2. Selecteer *Toepassingen* in het vervolgkeuzemenu op de CMC-startpagina.
3. Selecteer in de lijst met *toepassingsnamen Toepassing BI-commentaar*.

   Het dialoogvenster *BI-commentaar* wordt weergegeven. Standaard wordt het keuzerondje *Controledatabase gebruiken* geselecteerd.
4. Selecteer het keuzerondje *Andere ondersteunde database gebruiken*.
5. Voer het *type*, de *databasenaam*, de *host*, de *poort*, de *gebruikersnaam* en het *wachtwoord* in het deelvenster *Commentaardatabase configureren* in.
6. Kies *Opslaan en sluiten*.
7. Start APS opnieuw op.

   Wijzigingen in de configuratie van de database van BI-commentaar worden pas doorgevoerd nadat u de Adaptive Processing Server (APS) opnieuw hebt opgestart.

U kunt uw verbinding valideren door *Verbinding testen* te kiezen

> **Opmerking**
>
> Als u een upgrade uitvoert naar SAP BusinessObjects Business Intelligence-platform 4.3 ondersteuningspakket 3 en al een database voor BI-commentaar voor JDBC op basis van de eerdere versies had geconfigureerd, wordt het wachtwoordveld nu leeg wanneer u *Verbinding testen*, *Opslaan en sluiten* of *Opslaan* selecteert.

U kunt oudere opmerkingen verwijderen of opschonen door het selectievakje *Alle opmerkingen verwijderen die ouder zijn dan* in te schakelen en het aantal dagen op te geven.

> **Opmerking**
>
> Om de wijzigingen van kracht te laten worden, moet u alle APS-servers die de service BI-commentaar hosten opnieuw starten.

U hebt nu een nieuwe database geconfigureerd waarin commentaar uit de BI-commentaartoepassing kan worden opgeslagen.

18.2.3.7 Instellingen voor de toepassing BI-beheerderstudio beheren

> **Opmerking**
>
> U hebt alleen toegang tot BI-beheerderstudio als u deel uitmaakt van de Administrator-groep.

Als u specifieke toegangsrechten weigert, zoals: *Toegang tot Cockpit BI-beheerder toestaan*, *Toegang tot Toezicht toestaan* en *Toegang tot Visueel verschil toestaan*, hebt u mogelijk geen toegang tot de specifieke toepassing in BI-beheerderstudio.

Specific Rights for BI Admin Studio	Implicit Value					
Allow access to BI Admin Cockpit	Granted					
Allow access to Monitoring	Granted					
Allow access to Visual Difference	Granted					
Visual Difference - Create comparison	Granted					
Visual Difference - Delete comparison	Granted					
Visual Difference - Rerun comparison	Granted					
Visual Difference - View comparison	Granted					

Als de rechten *Visueel verschil* zijn geweigerd, kunt u ook het gebruik van de toepassing Visueel verschil beperken.

18.2.3.8 Integratie van samenwerkingstoepassingen beheren

Deze handleiding is bedoeld voor beheerders van het BI-platform die het BI-platform integreren met een samenwerkingstoepassing van SAP Jam.

Gebruik het gebied *Toepassingen* van de CMC (Central Management Console) in het BI-platform om samenwerking in te schakelen en te configureren.

De volgende aanvullende configuratie is vereist in de Enterprise-agent van de samenwerkingstoepassing:

- Een HTTPS-verbinding met een serviceprovider tot stand brengen
- Voldoen aan vereisten voor verificatie

Wanneer SAP Jam is geconfigureerd, zijn feeds van de samenwerkingstoepassing beschikbaar in het BI-startpunt.

SAP Jam biedt geen ondersteuning voor Microsoft Internet Explorer 11.

18.2.3.8.1 Vereisten voor samenwerking

Aan de vereisten voor samenwerking moet worden voldaan voordat u het BI-platform integreert met een samenwerkingstoepassing.

- Het BI-platform moet met ten minste één CMS (Central Management Server) worden geïnstalleerd.
- De samenwerkingstoepassing (SAP Jam) moet zijn geconfigureerd in de CMC (Central Management Console).
- Er moet een Enterprise-organisatie voor de samenwerkingstoepassing (SAP Jam) worden gedefinieerd.
- SAP Jam-gebruikers moeten tot de Enterprise-organisatie behoren.
- Een SAP Jam-Enterprise-agent is vereist voor het toewijzen van gebruikers via een lokale LDAP-/AD-directoryservice.

18.2.3.8.2 BI-platformconfiguratie

18.2.3.8.2.1 Opties voor samenwerkingsconfiguratie

Samenwerkingsopties worden weergegeven in het dialoogvenster *Eigenschappen:Samenwerking* in de CMC (Central Management Console) in het BI-platform.

Als u het dialoogvenster *Eigenschappen:Samenwerking* wilt openen, klikt u op het tabblad *Toepassingen* in de CMC op *Samenwerking* en selecteert u *Beheren* > *Eigenschappen*.

Optie	Beschrijving
Samenwerking inschakelen	Schakel dit selectievakje in en selecteer *SAP Jam*.
Verbindings-URL	Voer de URL naar de samenwerkingstoepassing in.
Id voor provider unieke identiteit	Voer een unieke waarde voor uw implementatie van het BI-platform in. De waarde moet worden gekoppeld aan het certificaat dat gebruikt wordt om integratie met de beheerconsole van de samenwerkingstoepassing te configureren. De toepassing die een identiteit voor eenmalige aanmelding bevestigt moet als OAuth-beheertoepassing zijn geconfigureerd.

Optie	Beschrijving
Base64-certificaat van identiteitsprovider	Als u op *Genereren* klikt, wordt een certificaat in dit vak gecreëerd. Gebruik dit certificaat in de beheerconsole van de samenwerkingstoepassing om een OAuth-consumentensleutel te genereren. Het certificaat brengt de vertrouwensrelatie tussen de samenwerkingstoepassing en het BI-platform tot stand. De externe identiteitsprovider wordt zelf geïdentificeerd met een X509-certificaat, waarmee alle identiteitsbevestigingen worden ondertekend. Het certificaat moet van Base64-codering zijn voorzien.
OAuth-consumentensleutel	Voer de OAuth-consumentensleutel in die vanuit de beheerconsole van de samenwerkingstoepassing is gegenereerd.
Verbinding maken met proxy	Selecteer dit selectievakje in om een verbinding via proxy in te schakelen en informatie over de proxyhost in de vakken *Host van HTTP-proxy* en *Poort* in te voeren. Als u inkomende verbindingen vanaf samenwerkingstoepassingsservers naar uw bedrijfsnetwerk wilt toestaan, moet er een omgekeerde proxy aanwezig zijn in de DMZ. Als u een vertrouwd certificaat van een SSL-certificaataanbieder aan uw omgekeerde proxy wilt toevoegen, moet uw omgekeerde proxy een domein- of subdomeinnaam hebben.
	Host van HTTP-proxy — In de configuratie van de omgekeerde proxy voert u een extern adres in dat toegankelijk is voor de samenwerkingstoepassing. Gebruik bijvoorbeeld `https://<ReverseProxy>/`; hierbij is `<ReverseProxy>` de domein- of subdomeinnaam van uw omgekeerde proxy. De samenwerkingstoepassing gebruikt dit adres om informatie naar het BI-platform te sturen. De omgekeerde proxy gebruikt dit adres om gegevens die vanaf de samenwerkingstoepassing zijn ontvangen, door te sturen naar de computer met de Enterprise-agent van de samenwerkingstoepassing.
	Poort — De Enterprise-agent van de samenwerkingstoepassing is geconfigureerd om te luisteren naar poort 8443.

18.2.3.8.2.2 Samenwerking inschakelen en configureren in de CMC

Voor deze taak is een geldige verbinding met de beheerconsole van de samenwerkingstoepassing (SAP Jam) vereist. U moet beveiligingsgegevens van de console doorgeven en ophalen.

Om veiligheidsredenen kunnen de volgende standaardaccounts geen inhoud naar SAP Jam verzenden of plannen:

- Gast
- SMAdmin
- Beheerder
- WaaWSServletPrincipal

1. Ga in de CMC (Central Management Console) in het BI-platform naar het gebied *Toepassingen* en dubbelklik op *Samenwerking*.

2. Schakel in het dialoogvenster *Eigenschappen:Samenwerking* het selectievakje *Samenwerking inschakelen* in en selecteer *SAP Jam*.
3. Voer in het vak *Verbindings-URL* de URL naar de samenwerkingstoepassing in.
4. Voer in het vak *Id voor provider unieke identiteit* een waarde voor de unieke identiteitsprovider in voor uw BI-platformimplementatie.

   Maak een aantekening van de waarde van de identiteitsprovider; u hebt deze nodig wanneer u de toepassingssamenwerking configureert.
5. Klik op *Genereren* (of *Opnieuw genereren* als er al eerder een certificaat is gegenereerd).
   In het vak *Base64-certificaat van identiteitsprovider* wordt het certificaat weergegeven. U gebruikt het certificaat om de samenwerkingstoepassing te configureren.
6. Voer in het vak *OAuth-consumentensleutel* de OAuth-consumentensleutel in.
7. Voer u de volgende acties uit als u via proxy verbinding maakt met de server waarop SAP Jam wordt uitgevoerd:
   a. Schakel het selectievakje *Verbinding maken met proxy* in.
   b. Voer in het vak *Host van HTTP-proxy* de proxyhostnaam van de server in.
   c. Voer in het vak *Poort* het poortnummer van de server in.
8. Klik op *Opslaan en sluiten*.

18.2.3.8.3 SAP Jam-configuratie

18.2.3.8.3.1 Een nieuwe, door SAML vertrouwde IDP voor SAP registreren

U moet iedere gebruiker registreren met een uniek e-mailadres dat overeenkomt met het Enterprise-e-mailadres van de gebruiker in het BI-startpunt. De e-mailadressen worden toegewezen tussen het BI-platform en SAP.

Voordat u een nieuwe SAML-vertrouwde IDP kunt registreren:

- Uw bedrijf moet toegevoegd zijn aan en geconfigureerd zijn in SAP.
- U moet een geldige SAP-gebruikersaccount hebben die aan uw bedrijf in SAP is gekoppeld.
- U moet bedrijfsbeheerrechten hebben voor uw bedrijf in SAP en volledige beheerdersrechten in het BI-platform en BI-startpunt.
- BI-startpunt moet zijn geregistreerd als een OAuth-client die fungeert als vertegenwoordiger van het startpunt binnen SAP.

SAP Jam biedt geen ondersteuning voor Microsoft Internet Explorer 11.

1. Selecteer in de rechterbovenhoek van de Central Management Console (CMC) in het BI-platform de optie *Beheerder* en daarna *Beheer*.
   Informatie over uw bedrijf wordt weergegeven, inclusief uw licenties voor SAP. Noteer of onthoud de informatie.
2. Selecteer uit het menu *Beheer* de optie *Door SAML vertrouwde ID's* en klik op *Registreer uw identiteitsprovider*.

   U moet de IDP registreren die u in het BI-startpunt hebt gemaakt.

3. Voer in het vak *IDP ID* de waarde van de unieke identiteitsprovider in die is gemaakt toen SAP werd geconfigureerd in het BI-platform.

   Als u de waarde niet hebt, neemt u contact op met de beheerder van uw externe toepassing.

   Bijvoorbeeld: voer **`<Bedrijfsnaam>_<Systeem-ID>_<Client>`** in.
4. Voer in het vak *URL voor eenmalige aanmelding* de URL in waarmee SAP rechtstreeks wordt opgeroepen.

   SAP gebruikt deze URL voor eenmalige aanmelding met de unieke identiteitsprovider.
5. Voer in het vak *URL voor eenmalige afmelding* de URL in die moet worden weergegeven nadat is afgemeld bij SAP.

   SAP gebruikt deze URL voor eenmalige afmelding bij de unieke identiteitsprovider.
6. Voer in het vakje *Default Name ID Format* (Standaardnotatie van naam-id) de notatie van de naam-id die in verificatieverzoeken moet worden gebruikt.
7. Voer in het vakje *Default Name ID Policy SP Name Qualifier* (Standaardbeleid voor naam-id Kwalificatie van SP-naam) de kwalificatie van de SP-naam in die in verificatieverzoeken moet worden gebruikt.
8. Selecteer in de lijst *Allowed Assertion Scope* (Toegestaan bevestigingsbereik) de optie *Users in my company* (Gebruikers in mijn bedrijf).

   Deze optie geeft de reeks gebruikers op waarvoor SAP bevestigingen van de IDP accepteert.
9. Voer in het vakje *X509-certificaat (Base64)* de waarde van het Base64-certificaat in die is gegenereerd toen SAP in het BI-platform is geconfigureerd.

   Als u de waarde niet hebt, neemt u contact op met de beheerder van uw externe toepassing.
10. Klik op *Register*.

18.2.3.8.3.2 Een OAuth-client voor SAP Jam maken

Voordat u een OAuth-consumentensleutel kunt maken:

- Uw bedrijf moet toegevoegd zijn aan en geconfigureerd zijn in SAP Jam.
- U moet een geldige SAP Jam-gebruikersaccount hebben die aan uw bedrijf in SAP Jam is gekoppeld.
- U moet bedrijfsbeheerrechten hebben voor uw bedrijf in SAP Jam en volledige beheerdersrechten in het BI-platform en BI-startpunt.
- BI-startpunt moet zijn geregistreerd bij SAP Jam als een OAuth-client die fungeert als vertegenwoordiger van het startpunt binnen SAP Jam.
- Iedere gebruiker moet in SAP Jam zijn geregistreerd met een uniek e-mailadres dat overeenkomt met het Enterprise-emailadres van de gebruiker in het BI-startpunt. De e-mailadressen worden toegewezen tussen het BI-platform en SAP Jam.

SAP Jam biedt geen ondersteuning voor Microsoft Internet Explorer 11.

1. Selecteer in SAP Jam in het menu *Administrator* (Beheerder) in de rechterbovenhoek de optie *Admin* (Beheer).
   Informatie over uw bedrijf wordt weergegeven, inclusief uw licenties voor SAP Jam.
2. In het menu *Beheer* selecteert u *OAuth-clients* en klikt u op *OAuth-client toevoegen*.
3. Voer in het dialoogvenster *Een nieuwe OAuth-client registreren* in het vakje *Naam* de waarde van de unieke identiteitsprovider in die is gemaakt toen SAP Jam in het BI-platform werd geconfigureerd.

   Als u de waarde niet hebt, neemt u contact op met de beheerder van uw externe toepassing.

SAP Jam geeft de naam van de toepassing weer als een hyperlink (naar de ingevoerde URL) wanneer actie wordt genomen uit naam van een gebruiker.

Bijvoorbeeld: voer **`<Bedrijfsnaam>_<Systeem-ID>_<Client>_<Toepassing>`** in.

4. Voer in het vak *Integratie-URL* de URL voor het BI-startpunt in.

   SAP Jam geeft de naam van de toepassing weer als een hyperlink naar de URL wanneer actie wordt genomen uit naam van een gebruiker.

5. Voer in het vakje *X509-certificaat (Base64)* de waarde van het Base64-certificaat in die is gegenereerd toen SAP Jam in het BI-platform is geconfigureerd.

   Als u de waarde niet hebt, neemt u contact op met de beheerder van uw externe toepassing.

   Als u dit vakje leeglaat, levert SAP Jam een consumentengeheim.

6. Klik op *Opslaan*.

De OAuth-consumentensleutel wordt gegenereerd. Maak een aantekening van de OAuth-consumentensleutelwaarde zodat de BI-platformbeheerder deze kan gebruiken.

18.2.3.9 Pushberichtgevingsservice in SAP BusinessObjects Mobile beheren

SAP BusinessObjects Mobile-server stuurt berichtgeving naar iOS-apparaten van SAP BusinessObjects Mobile-toepassingsgebruikers. Berichtgeving wordt gepusht in de volgende scenario's:

- wanneer op het apparaat van een gebruiker gedownloade BI-documenten een update of nieuw exemplaar beschikbaar hebben op de server.
- wanneer een nieuw document wordt ontvangen in Postvak In van BI van een gebruiker.
- wanneer het BI-platform of de BOE-beheerder een bericht uitzendt.

Berichtgeving wordt automatisch naar het apparaat gepusht vanaf Mobile Server via Apple Push Notification Server (APNS). Gebruikers hoeven niet op de server zijn aangesloten om pushberichtgeving te ontvangen. Gebruikers kunnen zelfs pushberichtgeving ontvangen wanneer de app niet actief is op het systeem. "Instellingen voor berichtgeving" moeten in de toepassing zijn ingeschakeld. Zie voor meer informatie over het configureren van pushberichtgeving de *Handleiding voor implementatie en configuratie van Mobile Server* voor Mobile Server 4.2.

> **Opmerking**
>
> Om pushberichtgeving op uw mobiele apparaat in te schakelen, moet BIMobileService in de APS worden uitgevoerd.
>
> Aangezien BIMobileService niet veel geheugen inneemt, kunt u het uitvoeren naast andere services in de APS.

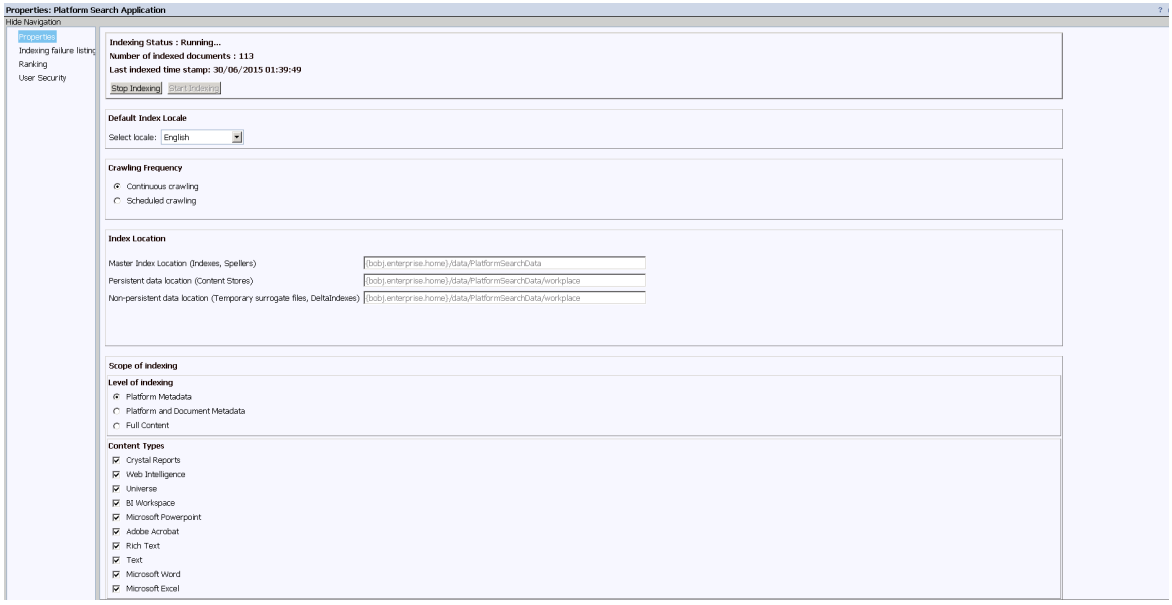
18.2.3.10 Instellingen voor Platform zoeken beheren

In het gebied *Toepassingen* van de CMC in het BI-platform kunt u op systeemniveau instellingen opgeven voor de toepassing Platform zoeken.

18.2.3.10.1 Toepassingseigenschappen configureren in de CMC

Voer de volgende stappen uit om de toepassingseigenschappen van Platform zoeken te configureren:

1. Ga naar het beheergebied *Toepassingen* in de CMC.
2. Selecteer de *toepassing Platform zoeken*.
3. Klik op *Beheren* > *Eigenschappen*. Het dialoogvenster *Eigenschappen* wordt weergegeven.



4. Configureer de instellingen voor Platform zoeken:

Optie	Beschrijving
Zoekstatistieken	Platform zoeken biedt de volgende zoekstatistieken: • Indexeringsstatus: hiermee wordt de status van het indexeringsproces weergegeven. • Aantal geïndexeerde documenten: hiermee wordt het aantal documenten weergegeven dat is geïndexeerd. • Laatst geïndexeerde tijdstempel: hiermee wordt de tijdstempel weergegeven waarmee het document voor het laatst is geïndexeerd.

Optie	Beschrijving
Indexeren stoppen/starten	Met de opties voor het starten of stoppen van de indexering kunt u het indexeringsproces starten of stoppen wanneer u wilt omschakelen van continu naar gepland verkennen, of voor onderhoudsdoeleinden. Klik op *Indexering stoppen* om het indexeren te stoppen.
Standaardindex van de landinstelling	Platform zoeken maakt gebruik van de landinstelling die in de CMC is opgegeven voor indexering van alle niet-gelokaliseerde BI-documenten. Nadat het document is gelokaliseerd, wordt de toepasselijke taalanalyse gebruikt voor indexering. Zoekopdrachten zijn gebaseerd op de productlandinstelling van de client, en het gewicht dat de productlandinstelling van de client heeft. U kunt het gewicht aanpassen in de eigenschappen van de CMC-configuratie.
Frequentie voor verkennen	U kunt de volledige BI-platformgegevensopslagruimte indexeren aan de hand van de volgende opties: • Continu verkennen: met deze optie is indexering een continu proces waarbij de gegevensopslagruimte wordt geïndexeerd wanneer er een object wordt toegevoegd, gewijzigd of verwijderd. Zo kunt u de meest up-to-date inhoud van BI-platform bekijken en ermee werken. Met continu verkennen wordt de gegevensopslagruimte voortdurend bijgewerkt met de acties die u uitvoert. Deze optie is standaard ingesteld. Continu verkennen werkt zonder tussenkomst van de gebruiker en beperkt de tijd die het indexeren van een document in beslag neemt. • Gepland verkennen: met deze optie is indexering gebaseerd op een planning die is ingesteld met de opties in Planning. Voor meer informatie over het plannen van een object raadpleegt u de sectie *Een object plannen* van Platform zoeken in de *online-Help voor SAP BusinessObjects Business Intelligence-platform CMC*. **Opmerking** • Als u *Gepland verkennen* selecteert en het *Terugkeerpatroon* instelt op een andere optie dan *Nu*, geeft Platform zoeken de datum- en tijdstempel weer waarop het document wordt gepland om opnieuw te indexeren. • Als u *Gepland verkennen* selecteert, is de knop *Indexeren starten* ingeschakeld en de knop *Indexeren stoppen* uitgeschakeld. • Nadat de planning voltooid is, wordt de knop *Indexeren stoppen* ingeschakeld.

Optie	Beschrijving
Indexlocatie	De indexen worden opgeslagen in gedeelde mappen op de volgende locaties: • Hoofdindexlocatie (indexen en speller): de hoofd- en spellerindexen zijn opgeslagen op deze locatie. Tijdens een zoekactie worden de eerste resultaten opgehaald met de hoofdindex en worden de spellerindexen gebruikt om suggesties op te halen. In een geclusterde implementatie van BI-platform moet deze locatie een gedeelde bestandssysteem zijn dat toegankelijk is vanuit alle knoppunten in het cluster. • Permanente gegevenslocatie (inhoudsopslag): de inhoudsopslag bevindt zich op deze locatie. Deze is gemaakt op basis van de hoofdindexlocatie en blijft ermee gesynchroniseerd. De inhoudsopslag wordt gebruikt om facetten te genereren en de eerste treffers te verwerken die via de locatie van de hoofdindex zijn gegenereerd. In een geclusterde BI-platformimplementatie wordt bij elk knooppunt een inhoudsopslag gegenereerd. De permanente gegevenslocatie is de enige indexlocatie waar de geclusterde omgeving invloed op heeft, omdat de inhoudsopslagmappen zich hier bevinden. Als een computer één zoekservice heeft, is er ook maar één locatie voor inhoudsopslag. Bijvoorbeeld {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam>\ContentStores. Als een geclusterde omgeving echter meerdere zoekservices bevat, heeft elke zoekservice één eigen locatie voor inhoudsopslag. Als er bijvoorbeeld twee exemplaren van een server worden uitgevoerd, zijn de locaties van de inhoudsopslag als volgt: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam 1>\ContentStores. • Niet-permanente gegevenslocatie (tijdelijke bestanden, delta-indexen): op deze locatie worden delta-indexen gemaakt en tijdelijk opgeslagen voordat deze worden samengevoegd met de hoofdindex. De indexen op deze locatie worden verwijderd wanneer ze zijn samengevoegd met de hoofdindex. Daarnaast worden surrogaatbestanden (uitvoer van de extractors) op deze locatie gemaakt en tijdelijk opgeslagen totdat ze geconverteerd worden in delta-indexen. **Opmerking** • Hoofdindexlocatie moet een gedeelde locatie zijn. • U moet op *Indexeren stoppen* klikken om de indexlocatie aan te passen. • Als u een indexlocatie aanpast, kopieert u de inhoud naar een nieuwe locatie, omdat de indexeringsgegevens anders verloren gaan. • De indexbestanden kunnen mogelijk persoonlijke en vertrouwelijke informatie opslaan, met name wanneer u ervoor kiest om documentinhoud te indexeren. U moet alleen een systeemgebruiker toestemming geven voor toegang tot de gedeelde map en u moet de gedeelde mappen in een versleutelde omgeving opslaan om diefstal van gegevens te vermijden.

Optie	Beschrijving

Indexeringsniveau	U kunt op de volgende manieren de inhoud die u wilt zoeken, afstemmen op het indexeringsniveau:
	• Metagegevens van platform: er wordt alleen een index gemaakt van de metagegevens van het platform, zoals titels, trefwoorden en beschrijvingen van documenten. Standaard is deze optie geselecteerd.
	• Metagegevens van platform en documenten: in deze index zijn de metagegevens van platform en documenten inbegrepen. De metagegevens van het document bestaan onder meer uit de aanmaakdatum, de wijzigingsdatum en de naam van de auteur.
	• Volledige inhoud: in deze index zijn de metagegevens van platform en documenten inbegrepen, evenals andere inhoud zoals:
	  • De eigenlijke inhoud van het document
	  • De inhoud van aanwijzingen en zoeklijsten
	  • Diagrammen, grafieken en labels
	Opmerking
	Volledig indexeren van de inhoud wordt niet ondersteund voor Analysis Office- en Lumira-documenten. Alleen het indexeren van de metagegevens wordt ondersteund voor Analysis Office- en Lumira-documenten.
	Opmerking
	Wanneer u het indexeringsniveau aanpast, wordt de indexering geïnitialiseerd om de volledige BI-platformgegevensopslagruimte te vernieuwen.

Optie	Beschrijving
Inhoudstypen	U kunt de volgende inhoudstypen selecteren voor indexering: • Crystal Reports • Web Intelligence • Universe • BI-werkruimte • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • RTF-tekst • Tekst • Microsoft Word • Microsoft Excel Het inhoudtypefilter is niet van toepassing op indexering van platformmetagegevens. Onafhankelijk van de inhoudtypen die u selecteert, vindt het indexeren van platformmetagegevens plaats voor alle ondersteunde objecttypen, en de zoekresultaten in BI-startpunt geven alle objecten voor het trefwoord gerelateerd aan platformmetagegevens als resultaat. Het inhoudstypefilter is relevant voor het indexeren van documentmetagegevens (documentauteur, documentkoptekst, documentvoettekst enz.) en het indexeren van inhoud (grafieken, diagrammen, tabel bij een rapport). Op basis van het indexeerniveau en de inhoudstypen die u selecteert, worden de documentmetagegevens en de inhoud voor de geselecteerde objecttypen uit de gegevensopslagruimte door platform zoeken geïndexeerd. Alleen die objecten worden in de zoekresultaten van het BI-startpunt weergegeven bij het zoeken naar het trefwoord gerelateerd aan documentmetagegevens en -inhoud.
Index opnieuw maken	Met deze optie wordt de bestaande index verwijderd en wordt de gehele gegevensopslagruimte opnieuw geïndexeerd. U kunt de optie *Index opnieuw maken* selecteren ongeacht of indexering actief is of is gestopt. De bestaande index wordt verwijderd wanneer u u wijzigingen op de eigenschappenpagina opslaat. Als indexering momenteel is gestopt, begint het opnieuw maken van de index pas wanneer u indexering opnieuw start. Als u niet wilt dat Platform zoeken de documenten opnieuw indexeert, moet u de selectie van *Index opnieuw maken* opheffen voordat u op de knop *Indexering starten* klikt.

Optie	Beschrijving
Documenten die zijn uitgesloten van indexering	De optie *Documenten die zijn uitgesloten van indexering* sluit documenten van indexering uit. U wilt bijvoorbeeld niet dat zeer grote Crystal Reports-rapporten doorzoekbaar worden gemaakt, omdat de resources van de Report Application Server anders overbelast raken. Zo wilt u waarschijnlijk ook niet dat publicaties met honderden aangepaste rapporten worden geïndexeerd. Door bepaalde documenten uit te sluiten, kunt u voorkomen dat ze worden geopend door Platform zoeken. Vergeet niet dat een document dat al geïndexeerd is voordat het in deze groep werd geplaatst, mogelijk nog steeds doorzocht kan worden. U moet de index opnieuw maken om ervoor te zorgen dat documenten in de groep *Documenten die zijn uitgesloten van indexering* niet doorzocht kunnen worden. Alleen de beheerdersaccount heeft standaard volledige toegang tot de optie *Documenten die zijn uitgesloten van indexering*. Andere gebruikers met de volgende rechten kunnen alleen documenten toevoegen aan de groep *Documenten die zijn uitgesloten van indexering*: • Weergave- en bewerkingsrechten voor de categorie • Het document rechtstreeks bewerken
Andere configuratie - exemplaar overslaan	Exemplaren van documenten worden standaard geselecteerd voor indexering. Dit zorgt voor een grotere index, die meer schijfruimte gebruikt. De map "Lucene-indexengine" in de map PlatformSearchData wordt enorm groot door de indexering van een zeer groot aantal exemplaren in de gegevensopslagruimte. Als er miljoenen (of meer) documenten zijn en veel van deze documenten ook nog eens een groot aantal bestaande exemplaren hebben (naast geplande exemplaren die regelmatig worden gegenereerd) in het systeem, wordt de map "Lucene-indexengine" te groot, zelfs als het indexeringsniveau wordt ingesteld op "Metagegevens platform". Met de functie Exemplaar overslaan bij zoeken platform kunt u de indexering van exemplaren besturen door via het selectievakje onder 'Andere configuratie - exemplaar overslaan' op de pagina Eigenschappen zoektoepassing platform in CMC in- of uit te schakelen. **Opmerking** • Als u Exemplaar overslaan in- of uitschakelt, moet u de Adaptive Processing Server voor zoeken platform opnieuw starten. Deze wijziging beïnvloedt alle indexeringsniveaus. • Als u Exemplaar overslaan wijzigt en de wijzigingen wilt toepassen op alle bestaande exemplaren (d.w.z. selecteren voor indexering), moet u de index opnieuw maken.

Optie	Beschrijving
Objecten die zijn uitgesloten van indexering	De optie *Objecten die zijn uitgesloten van indexering* sluit objecten van indexering uit. U wilt bijvoorbeeld niet dat bepaalde objecten doorzoekbaar worden gemaakt, omdat de resources van de Report Application Server anders overbelast raken. Door bepaalde objecten uit te sluiten, kunt u voorkomen dat ze worden geopend door Platform zoeken. Vergeet niet dat een object dat al geïndexeerd is voordat het in deze groep werd geplaatst, mogelijk nog steeds doorzocht kan worden. U moet de index opnieuw maken om ervoor te zorgen dat objecten in de groep *Objecten die zijn uitgesloten van indexering* niet doorzocht kunnen worden. Lijst met objecten die kunnen worden uitgesloten van indexering: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profiel • Gebeurtenis • Discussies • InformationDesigner • MDAnalysis • Publicatie • Niet-specifiek • Analytisch • Hyperlink • Programma • pQuery • DSL.MetaDataFile • Sneltoets • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

Optie	Beschrijving
	• VISI.Lums • VISILums • Gebruiker • Gebruikersgroep

5. Klik op *Opslaan en sluiten*.

> **Opmerking**
>
> Als een gebruiker de optie *Index opnieuw maken* niet selecteert en het indexeringsniveau wijzigt of extractors selecteert of deselecteert, wordt de index incrementeel bijgewerkt zonder de bestaande index te verwijderen.

18.2.3.11 BEx-webintegratie configureren

BEx-webtoepassingen zijn webgebaseerde toepassingen uit Business Explorer (BEx) van SAP Business Warehouse (BW) voor gegevensanalyse, rapportage en analytische toepassingen op het web.

De Business Explorer is de SAP NetWeaver Business Intelligence-suite, die flexibele rapportage- en analysehulpmiddelen biedt voor strategische analyse en ondersteuning bij besluitvorming. Deze hulpmiddelen omvatten query-, rapportage- en analysefuncties. Als werknemer met toegangsrechten kunt u historische of actuele gegevens op verschillende detailniveaus en vanuit verschillende perspectieven evalueren, zowel op het web als in Microsoft Excel.

Gebruikers roepen de gegevens op vanuit het SAP NetWeaver-portaal of vanuit het BI-startpunt van SAP BI-platform. Auteurs van BEx-webtoepassingen kunnen de webtoepassingen direct uitvoeren in het BI-startpunt vanuit BEx Web Application Designer.

Voer de volgende configuratiestappen uit om BEx-webtoepassingen in het BI-platform te integreren:

1. Stel een server in voor de BEx-webtoepassingen in de Central Management Console (CMC).

   U kunt een algemene of zelstandige server voor de BEx-webtoepassingen gebruiken.

   > **→ Tip**
   >
   > Het is raadzaam een zelfstandige server voor de BEx-webtoepassingen in te stellen, aangezien de algemene server doorgaans door vele andere services wordt gebruikt.

2. Configureer de serverinstellingen.
3. Controleer de verbinding met het BW-systeem.
4. Om ervoor te zorgen dat auteurs BEx-webtoepassingen direct in het BI-startpunt kunnen uitvoeren vanuit BEx Web Application Designer, moet u de relevante instellingen maken in de tabel *Verbonden portalen* (**RSPOR_T_PORTAL**) in het BW-systeem.

Na de configuratie van de BI-platformserver kunnen gebruikers BEx-webtoepassingen in het BI-startpunt openen. Ze kunnen hier door de gegevens navigeren en de BEx-webtoepassingen als bladwijzers opslaan in de favorieten van de webbrowser.

⚠ Beperking

Integratie wordt ondersteund vanaf de volgende SAP NetWeaver-releases:

SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
SAP NetWeaver 7.3 Support Package Stack 1

Aangezien de SAP NetWeaver Java-stack niet vereist is voor deze integratie, gelden de volgende beperkingen:

Het uitzenden van informatie wordt niet ondersteund.
Aangezien de portal en Knowledge Management van SAP NetWeaver niet nodig zijn, wordt documentintegratie en het gebruik van portaalmotieven niet ondersteund in de BEx-webtoepassingen.
Het webitem *Rapportage* wordt niet ondersteund. Het is raadzaam dat u SAP Crystal Reports gebruikt voor rapportage met opmaak.
De exportbibliotheek voor SAP Business Explorer wordt gebruikt om afgedrukte versies van BEx-webtoepassingen te maken. Adobe Document Services (ADS) zijn niet beschikbaar.
De BEx-webtoepassingen die in het BI-platform zijn geïntegreerd, kunnen alleen gegevensbronnen bevatten die zijn opgeslagen in het BW-hoofdsysteem. In de systeemadministratie definieert u welk systeem geconfigureerd wordt als het BW-hoofdsysteem in het BI-platform.
Eenmalige aanmelding tussen het BI-platform en het SAP NetWeaver BW-systeem is niet ingeschakeld. Voor elke BI-platformsessie worden de gebruikers van de BEx-webtoepassingen gevraagd zich aan te melden bij het relevante BW-hoofdsysteem.
De rapportinterface rapporteren van en naar BEx-webtoepassingen wordt niet ondersteund. Overeenkomstige opdrachten worden niet uitgevoerd.
Dashboards die zijn gebaseerd op BEx-query's of queryweergaven en die zijn gemaakt met SAP BusinessObjects Dashboards, worden niet ondersteund.

Voor meer informatie over de functies van BEx-webtoepassingen raadpleegt u de SAP Help Portal op http://help.sap.com: *SAP NetWeaver 7.3* > *SAP NetWeaver Library: Function-Oriented View* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Analysis & Reporting: BEx Web Applications*.

Voor meer informatie over het oproepen en opslaan van BEx-webtoepassingen in het BI-startpunt raadpleegt u de gebruikershandleiding voor het *BI-startpunt* op http://help.sap.com.

Verwante informatie

Een server starten voor BEx-webtoepassingen [pagina 738]
Een zelfstandige server starten voor BEx-webtoepassingen [pagina 739]
Serverinstellingen configureren [pagina 739]
Verbinding met BW-systeem controleren [pagina 740]
Een verbinding tussen BEx Web Application Designer en het BI-platform configureren [pagina 741]

18.2.3.11.1 Een server starten voor BEx-webtoepassingen

Voordat u deze taak kunt uitvoeren, moet de Adaptive Processing Server gestopt zijn.

1. Meld u aan bij de CMC (Central Management Console).
2. Kies *Servers*.
3. Vouw het knooppunt *Servicecategorieën* uit en kies *Analysis-services*.
4. Selecteer *Adaptive Processing Server* en kies *Services selecteren* in het snelmenu.
5. Verplaats *BEx-webtoepassingsservice* uit de lijst *Beschikbare services* naar de lijst Services aan de rechterkant.
6. Start de BEx-webtoepassingsservice opnieuw door de Adaptive Processing Server opnieuw te starten.

18.2.3.11.2 Een zelfstandige server starten voor BEx-webtoepassingen

1. Meld u aan bij de CMC (Central Management Console).
2. Kies *Servers*.
3. Vouw het knooppunt *Servicecategorieën* uit en kies *Analysis-services*.
4. Selecteer *Adaptive Processing Server* en kies *Server klonen* in het snelmenu.
5. Voer een naam in voor de server (bijvoorbeeld **`AdaptiveProcessingServer`**) en selecteer het gewenste knooppunt in het vak *Klonen naar knooppunt*.
6. Selecteer de gekloonde server en kies *Services selecteren* in het snelmenu.
7. Selecteer *BEx-webtoepassingsservice* in de lijst *Beschikbare services* en verplaats de service naar de lijst Services aan de rechterkant.
8. Start de BEx-webtoepassingsservice door de nieuwe Adaptive Processing Server te starten.

18.2.3.11.3 Serverinstellingen configureren

1. Meld u aan bij de CMC (Central Management Console).
2. Kies *Servers*.
3. Vouw het knooppunt *Servicecategorieën* uit en kies *Analysis-services*.
4. Selecteer de server die de BEx-webtoepassingsservice host en kies *Eigenschappen* in het snelmenu.
5. Onder de *Configuratie van de BEx-webtoepassingsservice* in het gebied *BEx-webtoepassingenservice* configureert u de volgende instellingen:
   a. Controleer (en wijzig indien nodig) het maximumaantal clientsessies.
   b. Onder *SAP BW Master System* voert u de naam in van de OLAP-verbinding met het BW-systeem dat u gemaakt hebt in het BI-platform. De standaardnaam is *SAP_BW*.
   c. Voer de naam in van het *JCo Server RFC-doel* dat u ingevoerd hebt in het BW-systeem onder *Configuratie van RFC-verbindingen* (transactiecode **`sm59`**).
   d. Voer de naam in van de *JCo Server Gateway-host* dat u vastgesteld hebt in het BW-systeem onder *Configuratie van RFC-verbindingen* (transactiecode **`sm59`**).
   e. Voer de naam in van de *JCo Server Gateway-service* dat u vastgesteld hebt in het BW-systeem onder *Configuratie van RFC-verbindingen* (transactiecode **`sm59`**).
   f. Controleer (en wijzig indien nodig) het *Verbindingsaantal van JCo-server*.

6. Kies *Opslaan en sluiten*.
7. Selecteer de server die de BEx-webtoepassingsservice host en kies *Server opnieuw starten* in het snelmenu.

   Als u de geselecteerde instellingen wilt toepassen, moet u de server opnieuw starten.

   > ⓘ Opmerking
   >
   > Voordat u de server opnieuw start, moet de RFC-doel in het ABAP-systeem zijn ingesteld.

Verwante informatie

Aanmaken van een RFC-doel in het ABAP-systeem [pagina 741]

18.2.3.11.4 Verbinding met BW-systeem controleren

1. Meld u aan bij de CMC (Central Management Console).
2. Kies *OLAP-verbindingen*.
3. Controleer of een verbinding gemaakt is met het BW-systeem. Zo niet, dan klikt u op de knop *Nieuwe verbinding* om een verbinding tot stand te brengen. De standaardnaam van de verbinding is **SAP_BW**. U kunt tevens een andere naam invoeren.
4. Zorg ervoor dat u *Vooraf gedefinieerd* geselecteerd hebt onder *Verificatie* en de verplichte ingangen voor gebruiker en wachtwoord hebt ingevoerd.

   > ⓘ Opmerking
   >
   > Deze gebruikersaccount is verplicht voor het RFC-doel van de JCo-server dat de integratie van BEx Web Application Designer, het BW-systeem en het BI-platform mogelijk maakt.

   > → Tip
   >
   > Voor het veilig maken van de verbinding dient u ervoor te zorgen dat alleen beheerders toegangsrechten hiervoor hebben.
   > 1. Hiertoe klikt u met de rechtermuisknop op de verbinding met het BW-systeem (standaardnaam **SAP_BW**) en kiest u *Gebruikersbeveiliging*.
   > 2. Maak de verplichte beveiligingsinstellingen en geef indien mogelijk alleen toegangsrechten aan beheerders.

18.2.3.11.5 Een verbinding tussen BEx Web Application Designer en het BI-platform configureren

Om ervoor te zorgen dat auteurs BEx-webtoepassingen direct in het BI-startpunt kunnen uitvoeren vanuit BEx Web Application Designer, moet u de relevante instellingen maken in de tabel *Verbonden portalen* (**RSPOR_T_PORTAL**) in het BW-systeem.

1. In het BW-systeem roept u de transactie **SM30** (*Onderhoud tabelweergave*) op.
2. Onder *Tabel/weergave* voert u **RSPOR_T_PORTAL** in.
3. Kies *Onderhouden*.
4. Voor het maken van een nieuwe vermelding kiest u *Nieuwe vermeldingen*.
5. Maak de volgende instellingen:
   a. Voor integratie tussen het BW-systeem en het BI-platform moet u een RFC-bestemming maken in transactie **SM59**. Voer deze RFC-bestemming in onder *Bestemming*.
   b. Selecteer *Standaardportal*. Dit zorgt ervoor dat webtoepassingen in Web Application Designer altijd opgeroepen worden in het BI-platform.
   c. Voer onder *URL-prefix* de URL in naar de Web Application Container Server (WACS) van BI-platform, inclusief het protocol, de hostnaam en poort, bijvoorbeeld **http://<wacs><domein>:<poort>**.
   d. Onder *Platform* selecteert u *BOE*.
   e. Selecteer *SAP Export Lib (PDF) gebruiken* als u de exportbibliotheek voor SAP Business Explorer wilt activeren, waarbij het mogelijk wordt om PDF-, PostScript- en PCL-bestanden te exporteren vanuit BEx-webtoepassingen.
6. Uw vermeldingen opslaan.

Verwante informatie

Aanmaken van een RFC-doel in het ABAP-systeem [pagina 741]

18.2.3.11.5.1 Aanmaken van een RFC-doel in het ABAP-systeem

Voor integratie van het BW-systeem met het BI-platform hebt u een RFC-doel nodig. Dit RFC-doel maakt het mogelijk dat het BW-systeem en het BI-platform met elkaar communiceren.

1. Roep *Configuratie van RFC-verbindingen* op (transactiecode**SM59**).
2. Kies *Aanmaken*.
3. Onderhoud het RFC-doel:
   a. Voer een naam in voor het RFC-doel.
   b. Selecteer *T voor TCP/IP-verbinding* als verbindingstype.
   c. Typ een beschrijving.

      U kunt de omschrijving van het RFC-doel taalafhankelijk onderhouden.

d. Onder *Technische instellingen* selecteert u *Geregistreerd serverprogramma* als activeringstype.
e. Onder *Technische instellingen* voert u de programma-id in.

   De programma-id moet identiek zijn aan de programma-id (JCo Server RFC-doel) die u hebt opgegeven bij het maken van het doel voor dit BW-systeem in de BI-platformserver.
f. Onder *Technische instellingen* voert u onder *Gateway-opties* de gateway-host en de gateway-service in die de BI-platformserver gebruikt om te communiceren met het BW-systeem.

4. Op de tabpagina *Aanmelden en beveiliging* activeert u de optie *SAP-aanmeldticket verzenden*.
5. Uw vermeldingen opslaan.

Verwante informatie

Serverinstellingen configureren [pagina 739]

18.2.3.12 Eenmalige aanmelding voor SAP HANA configureren

In het gebied *Toepassingen* van de CMC in het BI-platform kunt u eenmalige aanmelding of SSO (Single Sign-On) configureren voor SAP HANA-databaseverbindingen. Eenmalige aanmelding wordt geïmplementeerd door middel van SAML (Security Assertion Markup Language).

Wanneer u een BI-platformsessie tot stand hebt gebrachct, kunt u een SAML-ticket genereren die kan worden gebruikt voor aanmelding bij SAP HANA zonder dat de gebruiker een wachtwoord hoeft op te geven.

Dit is de basiswerkstroom voor het verbinden van SAP HANA-gegevensbronnen:

1. Een beheerder configureert een vertrouwensrelatie tussen SAP HANA en het BI-platform in de CMC.
2. Een gebruiker meldt zich aan bij het BI-platform met een van de ondersteunde verificatieproviders.
3. Mits de gebruikers-id's van SAP HANA en het BI-platform overeenkomen, kan het BI-platform een SAML-verklaring genereren die SAP HANA kan accepteren om een verbinding voor de huidige gebruiker tot stand te brengen. De gebruikers-id die aan SAP HANA wordt doorgegeven, is de gebruikers-id van het BI-platform voor de gebruiker die zich heeft aangemeld.
4. Een BI-platformclienttoepassing maakt een SAP HANA-verbinding.

> **Opmerking**
>
> Voordat u SAP HANA SSO met SAML configureert, moet u SSL configureren op de SAP HANA-computer. Raadpleeg de SAP HANA-documentatie voor details.

18.2.3.12.1 SAP HANA-verbindingsinstellingen

De onderstaande tabel bevat een overzicht van de instellingen die in de CMC beschikbaar zijn voor configuratie van SAP HANA-verbindingen.

Instelling	Beschrijving
HANA-hostnaam	Geef de naam van uw SAP HANA-host op.
HANA-poort	Geef het poortnummer van uw SAP HANA-host op.
Id voor provider unieke identiteit	Een unieke naam binnen een bepaalde HANA-installatie. De HANA-installatie accepteert juist ondertekende tickets van de naam van deze identiteitsprovider voor aanmeldingen.
Base64-certificaat van identiteitsprovider	Wanneer u op *Genereren* klikt, wordt er een certificaat gemaakt in het veld *Base64-certificaat van identiteitsprovider*. Kopieer dit certificaat naar het bestand `trust.pem` in uw SAP HANA-implementatie. Dit certificaat brengt de vertrouwensrelatie tussen SAP HANA en het BI-platform tot stand. De externe identiteitsprovider wordt zelf geïdentificeerd met een X509-certificaat, waarmee alle identiteitsbevestigingen worden ondertekend. Het certificaat moet van Base64-codering zijn voorzien.
SAP HANA-exemplaarnummer	Geef het instancenummer van uw SAP HANA-database op.
SAP HANA-tenantdatabase	Geef de naam van uw SAP HANA-tenantdatabase op.

18.2.3.12.2 Een SAP HANA-verbinding maken

1. Haal de relevante SAP HANA-databaseparameters op.
   a. Open de SAP HANA Studio-toepassing.
   b. Open de eigenschappenpagina voor uw systeem en zoek naar de URL voor de databaseverbinding.
   c. Leg de naam van de hostmachine, het poortnummer, het instancenummer en de naam van de tenantdatabase vast.

      U hebt deze informatie nodig in stap 2.
2. Configureer een SAP HANA-verbinding in het BI-platform.
   a. Ga naar het gebied *Toepassingen* in de CMC en dubbelklik op *HANA-verificatie*.
   b. Klik in het dialoogvenster *HANA-verificatie* op de knop *Een verbinding maken*.
      Het dialoogvenster *Verbinding voor HANA-verificatie maken* wordt geopend.
   c. Selecteer een *Verbindingstype*.

      > **Opmerking**
      >
      > Selecteer *SAP HANA* voor een JDBC-verbinding en *SAP HANA HTTP* voor een HTTP-verbinding.

   d. Voer het poortnummer, de naam van de hostmachine, het instancenummer en de naam van de tenantdatabase in die u in stap 1 hebt vastgelegd.
   e. Geef in het veld *Uniek id van identiteitsprovider* een waarde op die voor uw implementatie van het BI-platform moet worden gebruikt.
   f. Voer *Serviceprovidernaam* in.

      > **Opmerking**
      >
      > U kunt de configuratie van Serviceprovidernaam in SAP HANA controleren door te navigeren naar `indexserver.ini -> Verificatie -> saml_service_provider_name`. U kunt de waarde in SAP HANA ook wijzigen door de hieronder vermelde code in te voeren: `ALTER SYSTEM ALTER CONFIGURATION (‘indexserver.ini’, ‘SYSTEM’) SET (‘authentication’,`

> `‘saml_service_provider_name’) = ‘DEV00’ WITH RECONFIGURE;` In de code is DEV 00 de naam van de serviceprovider en u kunt het naar uw wens invoeren. De aanbevolen procedure om de serviceprovider een naam te geven is het combineren van de systeem-id (DEV) en het exemplaarnummer (00).

g. Selecteer *Veilige verbinding*.

> **Opmerking**
>
> Selecteer *Veilige verbinding* om een veilige JDBC- of HTTPS-verbinding tot stand te brengen
>
> - Selecteer *SAP HANA HTTP* als *verbindingstype* om een HTTPS-verbinding tot stand te brengen en selecteer vervolgens *Veilige verbinding*.
> - Selecteer *SAP HANA* als *verbindingstype* om een veilige JDBC-verbinding tot stand te brengen en selecteer vervolgens *Veilige verbinding*.

h. Klik op *Genereren.*
In het vak *Base64-certificaat van identiteitsprovider* wordt een certificaat aangemaakt.

3. Configureer uw SAP HANA-implementatie.
   a. Meld u aan bij het SAP HANA-systeem.
   b. Vouw *SSL- en vertrouwensconfiguratie* uit en selecteer *PSE-beheer*.
   c. Selecteer het PSE-bestand uit de vervolgkeuzelijst *PSE beheren*.
   d. Selecteer *Certificaten importeren*.
   e. Plak het certificaat dat in de eerdere stap is gegenereerd in het BI-platform.
   f. Selecteer *Importeren*.
   g. Start SAP HANA-studio.
   h. Vouw in de weergave *Systemen* uw SAP HANA-systeem uit. Zie SAP HANA ONE-beheerdershandleiding.
   i. Open (Beveiligingseditor) uit de map Beveiliging.
   j. Selecteer (SAML-identiteitsprovider voor certificaatbestand importeren).
   k. Selecteer uw identiteitsprovider uit de lijst *SAML-identiteitsprovider*.
   l. Selecteer (implementeren).
   m. Navigeer naar de SAP HANA-gebruiker in de weergave *Systemen*.
   n. Open de SAP HANA-gebruiker in het editorgebied.
   o. Controleer in het tabblad *Gebruiker SAML* als de verificatie en selecteer *Configureren*.
   p. Selecteer *Toevoegen* in de wizard *Externe SAML-identiteiten configureren*.
   q. Selecteer uw identiteitsprovider.
   r. Selecteer OK.
   s. Selecteer uw identiteitsprovider en voer de gebruikersnaam van het BI-platform in die is toegewezen aan de SAP HANA-gebruiker.
   t. Selecteer OK.
   u. Selecteer (implementeren).
   v. Start het SAP HANA-systeem opnieuw.
      1. Open het contextmenu van uw SAP HANA-systeem.
      2. Selecteer *Configuratie en toezicht*.
      3. Selecteer *Systeem opnieuw starten*.
4. Test de SAP HANA-configuratie.

a. Ga naar het gebied *Toepassingen* in de CMC en dubbelklik op *HANA-verificatie*.
b. Open in het dialoogvenster *HANA-verificatie* de verbinding die u in stap 2 hebt gemaakt.
   Het dialoogvenster *Verbinding voor HANA-verificatie bewerken* wordt geopend.
c. Voer onder *Test de verbinding voor deze gebruiker* een gebruikersnaam in en klik op de knop *Verbinding testen* om te verifiëren dat uw verbindingsinstellingen geldig zijn.

   Voer bijvoorbeeld de gebruikersnaam **`Beheerder`** in. Als de instellingen niet geldig zijn, wordt een foutbericht weergegeven. U kunt de volgende stappen voor probleemoplossing proberen:

   - Zorg dat geen ander certificaat in het bestand `trust.pem` een Onderwerp of Uitgever met dezelfde CN-eigenschapswaarde bevat. Als u de onderdelen van het certificaat wilt zien, zoekt u op internet naar "x509 certificate decoder" om een toepassing voor certificaatdecodering te vinden.
   - Probeer de volgende opdrachten om de configuratie aan HANA-zijde te testen:

     ```
     select * from "SAML_PROVIDERS"
     select user_name, is_saml_enabled from users where user_name =
     '<UserName>'
     select * from "PUBLIC"."SAML_USER_MAPPINGS"
     ```

   - Als er een SAML-verificatiefout wordt weergegeven tijdens configuratie van SSO in SAP HANA, volgt u de volgende stappen:
     1. Stel in het bestand `indexserver.ini` de parameter `sslCreateSelfSignedCertificate` in op **`false`**.
     2. Stel in hetzelfde bestand de parameters `sslKeyStore` en `sslTrustStore` in op absolute paden.
     3. Genereer de bestanden `key.pem` en `trust.pem` opnieuw.

Als het bestand `key.pem` niet bestaat in de map `.ssl`, is SAP HANA niet goed geconfigureerd om SSL te gebruiken.

18.2.3.12.3 SAP HANA HTTPS-verbinding configureren

De configuratie van SAP HANA HTTPS omvat toevoeging van het HANA-server- en HANA-server CA-certificaat in TrustStore of een locatie van uw keuze.

> **Opmerking**
>
> U moet het SAP HANA-servercertificaat uit het SAP HANA-systeem exporteren voordat u het certificaat in TrustStore of in een andere locatie toevoegt.

Het certificaat in Truststore toevoegen

1. Ga naar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
2. Voer de volgende opdracht uit: `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.

3. Het HANA-server- en HANA server CA-certificaat worden opgeslagen in TrustStore.

> **Opmerking**
>
> Als het keystorebestand zich in de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security` bevindt, gaan de wijzigingen die zijn aangebracht in het keystorebestand verloren na een upgrade van SAP Business Intelligence Platform Support Package 4 naar Support Package 5. Daarom wordt het aanbevolen om het certificaat in een andere locatie toe te voegen.

Het certificaat in een andere locatie toevoegen

1. Ga naar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Voer de volgende opdracht uit: `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Opmerking**
   >
   > De hierboven gedefinieerde locatie is maar een voorbeeld. U kunt elke locatie van uw keuze toevoegen.

3. Voer de volgende opdracht uit zodat de APS-server de bestandslocatie kan identificeren:

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Opmerking**
   >
   > cacerts_PATH en Password zijn maar een voorbeeld van het keystorepad en wachtwoord voor het certificaat. U kunt elk pad en wachtwoord van uw keuze toevoegen.

18.2.3.13 Instellingen voor SAP Lumira beheren

Vanuit het gebied "Toepassingen" van CMC kunt u rechten beheren die gerelateerd zijn aan de functionaliteit voor gegevens verzamelen en content delen van SAP Lumira voor elke gebruiker of gebruikersgroep.

Voer de volgende stappen uit om rechten voor SAP Lumira te beheren:

1. Selecteer vanuit de startpagina van CMC *Toepassingen* > *SAP Lumira* > *Gebruikersbeveiliging*.
2. Selecteer de gebruiker groep waarvoor u rechten wilt instellen.
3. Selecteer *Beveiliging toewijzen*.
4. Selecteer *Geavanceerd*.
5. Selecteer *Rechten toevoegen/verwijderen*.
6. Definieer de rechten die de gebruiker voor SAP Lumira moet hebben.
7. Klik op *Toepassen*.

18.2.3.14 Instellingen voor SAP Analytics Cloud beheren

18.2.3.14.1 Hubobjecten doorgeven aan SAP Analytics Hub

U kunt BI-assets doorgeven aan een nieuwe categorie *Hubobject* en dezelfde BI-assets openen via SAP Analytics Hub.

Maak een *OAuth-client* in SAP Analytics Cloud en noteer de waarden voor parameters zoals *Tenant-URL SAP Analytics Cloud*, *Token-URL*, *OAuth-client-ID* en *Geheim*. Raadpleeg het onderwerp *OAuth-client beheren* in SAP Analytics Cloud Help in de SAP Help Portal voor meer informatie over het maken van een OAuth-client.

SAP Analytics Hub biedt u toegang tot uw on-premises en cloudgebaseerde BI-assets via één platform. U moet vertrouwen configureren tussen het BI-platform en SAP Analytics Cloud, die als een identiteitsprovider voor SAP Analytics Hub fungeert, om het BI-platform toe te staan om BI-assets te uploaden naar SAP Analytics Hub.

> **Opmerking**
>
> Publicaties worden niet ondersteund in de categorie *Hubobject*.

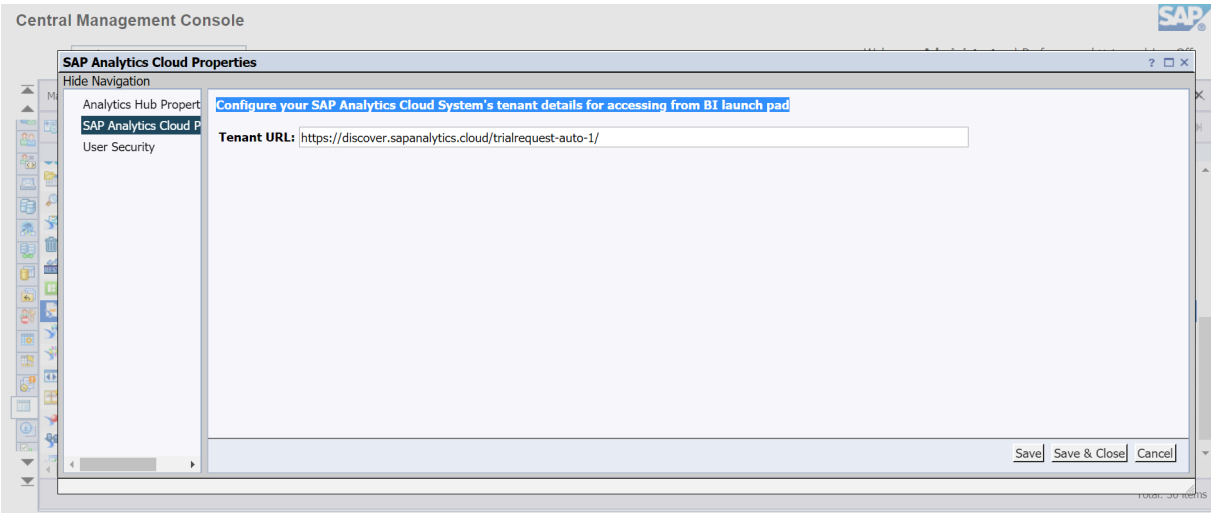
1. Meld u aan bij CMC en navigeer naar *Toepassingen* > *SAP Analytics Cloud*.
2. Selecteer *BI-platform toestaan om BI-assets door te geven aan SAP Analytics Hub*.
3. Voer de volgende parameters in:
   - *Tenant-URL SAP Analytics Cloud*
   - *Token-URL*
   - *OAuth-client-ID*
   - *Geheim*
4. Selecteer *Opslaan en sluiten*.

U hebt SAP Analytics Cloud-instellingen in het BI-platform geconfigureerd om de BI-assets in *Hubobject* naar SAP Analytics Hub te uploaden.

18.2.3.14.2 De instellingen voor Tenant-URL SAP Analytics Cloud configureren

U kunt nu de tenantgegevens van het SAP Analytics Cloud-systeem configureren om er toegang toe te krijgen via de SAC-tegel in de toepassingen van het BI-startpunt.

> **Opmerking**
>
> Standaard is de URL geconfigureerd voor de URL voor de proefversie van SAP Analytics.



18.2.3.15 Configuratie verificatieserver

Via de toepassing Configuratie verificatieserver hebben databasebronnen toegang tot het mechanisme of protocol van de verificatieserver.

End-to-end SSO OAuth-ondersteuning - enkelvoudige en meervoudige OAuth-serverondersteuning

In de Central Management Console biedt de toepassing *Configuratie verificatieserver* u de mogelijkheid om verificatieservers te configureren en te beheren op het BI-platform. Binnen de toepassing is de beheerder verantwoordelijk voor het registreren en beheren van de configuratie via de verificatieverwijzingsobjecten. Elke verificatieserverconfiguratie bevat een verificatieverwijzingsobject. U kunt verificatieserverconfiguraties maken voor niet-specifieke, Google Drive-, Microsoft Drive- of OData-bronnen.

Vul de verplichte velden onder *Voer configuratie-informatie in voor een verificatieserver* in om een verificatieserverconfiguratie te maken.

De *Verificatiescope* kan worden gebaseerd op uw behoeften voor het beheren waar eindgebruikers toegang toe hebben, online of offline.

18.2.3.15.1 Een verificatieserver configureren

U kunt een verificatieserver configureren.

1. Start de Central Management Console en meld u als beheerder aan.
2. Selecteer op de startpagina de optie *Toepassingen* onder de kolom *Beheren*.
3. Dubbelklik in de pagina *Toepassingen* op *Configuratie verificatieserver*.

4. Voer in het venster *Configuratie verificatieserver* een van de volgende handelingen uit:
   - Selecteer *Beheren* > *Nieuwe configuratie verificatieserver*
   - Selecteer het werkbalkpictogram *Een nieuwe verificatieserverconfiguratie maken*
5. Vul de volgende parameers in het dialoogvenster *Een nieuwe verificatieserverconfiguratie maken* in:
   - *Verwijzingsnaam*
     Kies een unieke willekeurige tekenreeks en voer dezelfde in om de configuratie te identificeren, om de configuratie in verschillende workflows te herkennen en te kiezen om op verificatie gebaseerde SSO te verkrijgen.
   - *Beschrijving* (optioneel)
     Voer een toelichting of trefwoord in om de configuratie op de lijst met beschikbare configuraties te beschrijven en eenvoudig te herkennen.
   - **Velden die specifiek zijn voor OpenID Connect**
     De volgende velden zijn specifiek voor OpenID Connect-verificatie en zijn niet vereist voor op verificatie gebaseerde SSO:
     - Selectievakje *Ingeschakeld voor "OpenID Connect"-verificatie*
     - *Uitgever-URI*
     - *URI JSON Web Key-sets (jwks_uri)*
     - *ID tokensigneeralgoritme*
   - *Verificatie-eindpunt*
     Voer de URL van de verificatieserver in, waarmee u de verificatie kunt verkrijgen.
   - *Tokeneindpunt*
     Voer de URL van de verificatieserver in, waarmee u een toegangstoken kunt aanvragen door de verificatiecode uit te wisselen.
   - *Client-id*
     Voer de naam in van de toepassing die wordt gebruikt om de BI-omgeving bij de verificatieserver te registreren.
   - *Clientgeheim*
     Voer de specifieke geheime code in die overeenkomt met de toepassing die wordt gebruikt bij het registreren van de BI-omgeving bij de verificatieserver.
   - *Omleidings-URL*
     Voer de URL in van het eindpunt van de BI-omgeving waarnaar de verificatiecode moet worden verzonden door de verificatieserver na de succesvolle validatie van de verificatie.
   - *Herroepingseindpunt* (optioneel)
     Voer de URL van de verificatieserver in, waarmee de toepassing de herroeping van alle eerder uitgegeven toegangstokens kan aanvragen via een specifiek vernieuwingstoken.
   - *Verificatiescope*
     Voer de ondersteunde verificatiescopes van de verificatieserver in om de limieten te definiëren voor de toegang van de toepassing (BI-landschap) tot verschillende beschikbare API-bronnen.

     > **Opmerking**
     >
     > BI-platformimplementatie van OAuth SSO is gebaseerd op offline toegang. Als uw doel voor de configuratie van de verificatieserver op het BI-platform is om gegevens te vernieuwen of toegang te krijgen tot bronnen zonder telkens opnieuw om de validatie van de verificatie te worden gevraagd, moet u dit veld configureren met de vereiste scope-parameter samen met één

> verplichte parameter (bijvoorbeeld refresh_token of offline_access op basis van de leverancier van de verificatietieserver).

- *Type bron*
  Kies het gewenste brontype uit de beschikbare lijst met brontypen die door het BI-platform worden ondersteund. Hieronder volgt de huidige lijst met brontypen die op het BI-platform worden ondersteund voor configuratie en toegang via de bijbehorende verificatieserver:
  - *Niet-specifiek* (standaardwaarde)
    Niet-specifiek voor een leverancier of protocol, om elke bron aan te geven die kan worden geopend na succesvolle verificatie door een verificatieserver.
  - *GoogleDrive*
    Om aan te geven dat de configuratie van een Google-verificatieserver is die kan worden gebruikt voor toegang van Google Drive tot verschillende BI-platformscenario's. Op enig moment kan er slechts één configuratie van het type GoogleDrive in het systeem bestaan.
  - *Microsoft Drive*
    Om aan te geven dat de configuratie van een Microsoft-verificatieserver is die kan worden gebruikt voor toegang van Microsoft Drive tot verschillende BI-platformscenario's. Op enig moment kan er slechts één configuratie van het type Microsoft Drive in het systeem bestaan.
  - *OData*
    Niet specifiek voor een leverancier, maar om aan te geven dat de configuratie gerelateerd is aan een bron die toegankelijk is via het OData-protocol met verificatie door een verificatieserver. Net als bij GoogleDrive kan er op enig moment slechts één configuratie van het type OData in het systeem bestaan.

> **Opmerking**
>
> De parameter *Type bron* heeft niets te maken met de OAuth 2.0-standaard. Deze wordt echter geïntroduceerd in de configuratie om eventuele dubbelzinnigheden bij het identificeren van bepaalde bronnen op het BI-platform te voorkomen. Daarom kunnen de bijbehorende configuraties eenvoudig worden geselecteerd en gebruikt in bepaalde scenario's om verificatie te verkrijgen.

- *Toegangstype*
  Deze parameter is specifiek voor de verificatieconfiguratie van het type *GoogleDrive*. Deze wordt automatisch ingevuld als de waarde voor het veld *Type bron* is ingesteld op *GoogleDrive*.
- *Aangepaste parameters* (optioneel)
  Voer eventuele aangepaste parameters in die nodig zijn om te verzenden tijdens het aanvragen van de verificatie. Dit is gebaseerd op eventuele aangepaste vereisten (indien nodig) van de verificatieserver die wordt geconfigureerd.

> **Opmerking**
>
> De naam van de aangepaste parameter moet uniek zijn in de configuratie.
>
> In elke verificatieconfiguratie mogen maximaal vijf aangepaste parameters worden geconfigureerd.

6. Selecteer nadat u alle vereiste parameters hebt ingevuld *OK* om de details te valideren en de configuratie op te slaan.

   De configuratie wordt opgeslagen als een systeemobject in de gegevensopslagruimte van het type *Verificatieverwijzing*. U kunt in alle ondersteunde scenario's naar de configuratie verwijzen met de bijbehorende *Verwijzingsnaam*.

18.2.3.15.2 De configuratie van de verificatieserver testen

U kunt de configuratie van uw verificatieserver testen.

1. Nadat u de configuratie van de verificatieserver hebt opgeslagen, start u het BI-startpunt en meldt u zich aan om uw configuratie te testen.

   > ⓘ Opmerking
   >
   > Het is momenteel niet mogelijk om de configuratie te testen via de CMC.
   >
   > Meld u aan als beheerder of met een gebruikersaccount van het BI-platform, die niet is beperkt tot het gebruik van de hierboven opgeslagen verificatieconfiguratie.
   >
   > Gebruik de huidige aanmeldingsmethode die is geconfigureerd voor het BI-startpunt (bijvoorbeeld Enterprise of een willekeurige verificatiemethode).

2. Selecteer het gebruikerspictogram.
3. Selecteer *Instellingen* in het vervolgkeuzemenu dat wordt weergegeven.
4. Selecteer in het dialoogvenster *Instellingen* de optie *Verificatietokens* in de sectie *Gebruikersaccount*.
5. Selecteer *Genereren* in de kolom *Tokens beheren*.
6. Volgens het beleid van uw organisatie, gebaseerd op de verificatieconfiguratie op uw verificatieserver, vindt ofwel de accountvalidatie plaats op basis van de certificaten die in het systeem zijn geconfigureerd, ofwel wordt u gevraagd naar de gebruikersnaam, het wachtwoord en/of verificatie op basis van de configuratie-instellingen.
7. Zodra de referenties of het certificaat met succes zijn gevalideerd, moet het BI-platform het vernieuwingstoken hebben ontvangen. Het moet veilig zijn opgeslagen in de gegevensopslagruimte van het BI-platform. Als dit is gelukt, ziet u de volgende wijzigingen op het tabblad *Verificatietokens*:
   - In de kolom *Verloopt op* moet u de vervalwaarde zien voor het token dat is uitgegeven door de verificatieserver. Als de verificatieserver een token zonder vervaldatum uitgeeft, wordt de kolomwaarde bijgewerkt als *Verloopt niet*.
   - Onder de kolom *Tokens beheren* moet u de knop *Verwijderen* zien naast de knop *Genereren*.
     - Met de knop *Verwijderen* verwijdert u het token dat is uitgegeven door de verificatieserver. Deze verwijdering is niet alleen beperkt tot het verwijderen van het token uit de gegevensopslagruimte van het BI-platform. Deze kan ook afhankelijk van de configuratie en ondersteuning worden doorgegeven aan de verificatieserver.
     - Als voor de optionele parameter *Herroepingseindpunt* de juiste URL is ingevuld op basis van de ondersteuning van uw verificatieserver hiervoor, wordt het uitgegeven token ook ingetrokken op het niveau van de verificatieserver, en wordt het token uit de gegevensopslagruimte van het BI-platform verwijderd.
8. Als het token wordt uitgegeven en de kolom *Verloopt op* wordt bijgewerkt op basis van het verlopen van het token dat is uitgegeven, werkt de configuratie met succes en is deze gereed voor gebruik door BI-ontwikkelaars en BI-eindgebruikers.

18.2.3.16 Configuratie informatieclassificatie

In het BI-platform kunt u de Azure-beleidsserver van uw organisatie configureren om de mogelijkheid om BI-inhoud te classificeren in te schakelen voor uw BI-landschap. Deze classificatiemogelijkheden kunnen worden toegepast via vertrouwelijkheidslabels die zijn gedefinieerd door de beheerder van de Azure-beleidsserver van uw organisatie.

> **Opmerking**
>
> Deze integratieoptie voor het configureren van de beleidsserver wordt alleen ondersteund voor Microsoft Azure Information Protection Platform.
>
> De SP04-release van SAP BusinessObjects BI 4.3 omvat een integratieoptie voor het Microsoft Azure Information Protection Platform. Houd er echter rekening mee dat de applicatie voor het configureren van de Azure-beleidsserverdetails in het BI-platform niet standaard is ingeschakeld, maar wordt geleverd als verborgen functie. Zie 3409349 voor meer informatie over het zichtbaar maken van deze verborgen functie.

Deze functie is alleen beschikbaar op het Windows-platform.

18.2.3.16.1 Informatieclassificatie configureren

1. Meld u als beheerder aan bij de *Central Management Console*.
2. Navigeer naar *Toepassingen*.
3. Rechtsklik op de applicatie *Configuratie Informatieclassificatie*.
4. Selecteer *Configuratie voor informatieclassificatie*.
5. Selecteer het aankruisvakje *Informatieclassificatie inschakelen* om de configuratie en velden in te schakelen.
6. Voer de token-URL van de Azure-beleidsserver van uw organisatie in het veld *Beleidsserver-URL* in.
   De URL-notatie moet `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token` zijn.
7. Voer de waarden van de *Client-ID* en het *Clientgeheim* van uw clientapplicatie op Azure in.
   Deze zijn ingeschakeld voor de verificatieflowmodus 'clientaanmeldingsgegevens' voor toegang tot de Azure-beleidsserver van uw organisatie.
8. Klik op *Configuratie opslaan en testen* om de verbinding te testen.
9. Is de configuratietest geslaagd, klik dan op *Opslaan* of *Opslaan en sluiten*.

> **Opmerking**
>
> Vink het aankruisvakje voor *Ingeschakeld voor certificaatverificatie* niet aan, omdat deze verificatieconfiguratiemodus niet wordt ondersteund.

18.3 Toepassingen beheren via Semantic Layer-eigenschappen

Configuratieopties in de DSL-bibliotheek (Dimensional Semantic Layer) kunnen worden ingesteld tijdens runtime om het gedrag te wijzigen van HANA Direct Access en BW Direct Access via BICS-verbindingen in BI-hulpprogramma's, zoals Web Intelligence, het hulpprogramma voor informatieontwerp, Dashboards en Crystal Reports for Enterprise. Deze opties worden opgegeven via Java-opdrachtregelopties in de vorm:

-DoptionName=optionValue

Het kan lastig zijn om deze instellingen te onderhouden en wijzigen:

- De opdrachtregelopties moeten worden opgegeven voor elk afzonderlijk Java-proces dat DSL uitvoert. Er is geen gemeenschappelijke locatie waar wijzigingen kunnen worden aangebracht.
- Elk DSL Java-proces afzonderlijk moet opnieuw worden opgestart om de herziene instellingen in te laten gaan. Wijzigingen worden niet direct van kracht.

Om de administratieve taak van het onderhouden van DSL-BICS-configuratieopties te vereenvoudigen, is een nieuw mechanisme geïntroduceerd, waarbij de opties in een bestand kunnen worden opgeslagen. Wijzigingen van het bestand zullen de nieuwe optie-instellingen doorvoeren in alle DSL-processen die het bestand lezen.

De naam en waarde van de optie worden in een bestand opgeslagen als geldige XML voor java.util.Propertes zoals gedefinieerd door http://java.sun.com/dtd/properties.dtd

Wanneer u dit nieuwe mechanisme voor het eerst gebruikt door DSL uit te voeren, worden de volgende twee bestanden automatisch gegenereerd:

- DSLBICSConfiguration.xml of DSLConfiguration.xml - dit bestand bevat alle beschikbare opties en hun standaardwaarden. Dit bestand mag niet worden gewijzigd.
- DSLBICSConfiguration_custom.xml of DSLConfiguration_custom.xml - dit bestand bevat alle opties met door de beheerder opgegeven waarden.

> **Opmerking**
>
> - DSLBICSConfiguration.xml- en DSLBICSConfiguration_custom.xml-bestanden worden gebruikt om het gedrag te beheren van BW Direct Access via BICS-verbindingen.
> - DSLConfiguration.xml en DSLconfiguration_custom.xml-bestanden worden gebruikt om het gedrag te beheren van HANA Direct Access.

Het gegenereerde bestand `DSLBICSConfiguration_custom.xml` en `DSLConfiguration_custom.xml` bevatten alle optie-instellingen die zijn opgegeven via de opdrachtregel en standaardinstellingen voor andere opties. Nadat ze voor het eerst zijn gegenereerd, kunnen de bestanden `DSLBICSConfiguration_custom.xml` en `DSLConfiguration.xml` worden gewijzigd voor het aanpassen of toevoegen van optiewaarden. Dit bestand wordt niet door het mechanisme bijgewerkt nadat het voor het eerst is gegenereerd. Het bestand `DSLBICSConfiguration.xml` wordt door het mechanisme bijgewerkt met nieuwe beschikbare opties, of als er een standaardwaarde is gewijzigd.

Wilt u de standaardeigenschappen wijzigen, gebruik dan het bestand voor aangepaste configuratie om nieuwe instellingen voor algemene of toepassingsspecifieke eigenschappen op te slaan. De bestanden bevinden zich standaard in: `SAP BusinessObjects Enterprise XI 4.0\java\lib`

Wijzig de eigenschappen in het standaardconfiguratiebestand niet.

18.4 Toepassingen beheren via BOE.war-eigenschappen

18.4.1 Het BOE.war-bestand

U kunt instellingen voor webtoepassingen van BI-platform wijzigen door standaardeigenschappen voor het BOE.war-bestand te overschrijven. Dit bestand wordt geïmplementeerd op de computer die de webtoepassingsserver host. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u meer wilt weten over hoe het bestand wordt geïmplementeerd.

De eigenschappen in het BOE.war-bestand beheren specificaties voor standaardaanmeldingsgedrag, standaardverificatiemethoden en instellingen voor eenmalige aanmelding. U kunt twee typen eigenschappen opgeven:

- Algemene eigenschappen: deze eigenschappen hebben invloed op alle webtoepassingen in het BOE.war-bestand.
- Toepassingsspecifieke eigenschappen: eigenschapsinstellingen die alleen invloed hebben op een specifieke webtoepassing.

Wilt u de standaardeigenschappen wijzigen, gebruik dan de map voor aangepaste configuratie om nieuwe instellingen voor algemene of toepassingsspecifieke eigenschappen op te slaan. Deze map bevindt zich standaard in: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Wijzig de eigenschappen in de map `config\default` niet.

> **Opmerking**
>
> Op sommige webtoepassingsservers zoals de Tomcat-versie die is gebundeld met het BI-platform, kunt u het BOE.war-bestand rechtstreeks openen. In dit geval kunt u rechtstreeks aangepaste instellingen configureren, zonder de implementatie van het WAR-bestand te verwijderen. Als u de geïmplementeerde webtoepassingen niet rechtstreeks kunt openen, moet u de implementatie van het bestand verwijderen, het bestand aanpassen en vervolgens opnieuw implementeren. Zie de *Implementatiehandleiding voor het SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u meer informatie wilt.

18.4.1.1 Globale BOE.war-eigenschappen

'In de volgende tabel staan de instellingen die zijn opgenomen in het standaardbestand `global.properties` voor BOE.war.

Creëer een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om deze instellingen te overschrijven.

Instelling	Standaardwaarden	Beschrijving
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Hiermee worden permanente cookies op de aanmeldingspagina van de webtoepassing in- of uitgeschakeld.

Instelling	Standaardwaarden	Beschrijving
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Geeft aan welke verificatiemethode moet worden gebruikt bij SiteMinder. De enige opties zijn secLDAP en secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Hiermee wordt verificatie voor SiteMinder in- en uitgeschakeld.
`sso.enabled`	`sso.enabled=false`	Hiermee schakelt u eenmalige aanmelding bij BI-platform in of uit.
`sso.sap.primary`	`sso.sap.primary=false`	Stel in op `true` als u SAP SSO wilt gebruiken als de primaire methode voor eenmalige aanmelding bij de toepassing. Alleen van toepassing op gevallen waarbij zowel SAP als SiteMinder SSO worden gebruikt.
`max.tree.children.threshold`	`max.tree.children.threshold=200`	Hiermee wordt de drempel opgegeven waarbij het besturingselement van de structuurlijst niet alle knooppunten weergeeft, maar alleen het bericht Te veel onderliggende elementen.
`trusted.auth.shared.secret`	Geen	Geeft de naam van de sessievariabele aan die wordt gebruikt om het geheim voor Vertrouwde verificatie op te halen. Alleen van toepassing als de websessie wordt gebruikt om het gedeelde geheim door te geven.
`trusted.auth.user.param`	Geen	Geeft de naam van de variabele aan die wordt gebruikt om de gebruikersnaam voor Vertrouwde verificatie op te halen en kan op een van de volgende waarden worden ingesteld: • `Header` • `URL Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	Geen	Geeft de naam van de methode aan die wordt gebruikt om de gebruikersnaam voor Vertrouwde verificatie op te halen en kan op een van de volgende waarden worden ingesteld: • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` Laat deze optie leeg om Vertrouwde verificatie uit te schakelen.
`trusted.auth.user.namespace.enabled`	`trusted.auth.user.namespace.enabled=false`	Hiermee wordt dynamische binding van aliassen aan bestaande gebruikersaccounts in- en uitgeschakeld. Als de eigenschap is ingesteld op `true`, gebruikt Vertrouwde verificatie aliasbinding

Instelling	Standaardwaarden	Beschrijving
		om gebruikers van het BI platform te verifiëren. Met aliasbinding werkt uw toepassingsserver als een SAML-serviceprovider. Hierdoor biedt Vertrouwde verificatie eenmalige aanmelding van SAML bij het systeem. Als Vertrouwde verificatie is ingesteld op `false`, wordt het koppelen van namen gebruikt om gebruikers te verifiëren.

`vintela.enabled`	`vintela.enabled=false`
	`idm.realm=YOUR_REALM`
	`idm.princ=YOUR_PRINCIPAL`
	`idm.allowUnsecured=true`
	`idm.allowNTLM=false`
	`idm.logger.name=simple`
	`idm.logger.props=error-log.properties`
		Wordt gebruikt om Vintela-instellingen voor Windows AD-verificatie in of uit te schakelen.

`pinger.showWarningDialog.cmc`	`pinger.showWarningDialog.cmc=true`	Geeft aan of het waarschuwingsvenster wordt weergegeven met het bericht dat de huidige sessie in de CMC binnenkort verloopt.
`pinger.showWarningDialog.bilaunchpad`	`pinger.showWarningDialog.bilaunchpad=true`	Geeft aan of het waarschuwingsvenster wordt weergegeven met het bericht dat de huidige sessie in het BI-startpunt binnenkort verloopt.
`pinger.warningPeriod.pingIncrementsInSeconds`	`pinger.warningPeriod.pingIncrementsInSeconds=15`	Geeft aan hoe vaak een aanvraag van de webserver moet worden verzonden terwijl het waarschuwingsbericht over de verlopen sessie wordt weergegeven. Dit is van belang voor de synchronisatie van het waarschuwingsvenster in toepassingen.
`pinger.warningPeriod.lengthInMinutes`	`pinger.warningPeriod.lengthInMinutes=5`	Geeft aan hoe lang voordat de sessie verloopt, de waarschuwing moet worden weergegeven.
`logoff.on.websession.expiry`	`logoff.on.websession.expiry=true`	Geeft aan of alle toepassingssessies worden afgemeld als de websessie verloopt.
`pinger.enabled`	`pinger.enabled=true`	Hiermee worden de waarschuwingsberichten voor verlopen sessies in- of uitgeschakeld.
`system.com.sap.bip.jcomanager.destinations.maxsize`	`system.com.sap.bip.jcomanager.destinations.maxsize=1000`	Geeft het maximumaantal Java-verbindingen in de cache aan.
`httpproxy.username`	`httpproxy.username=myusername`	Geeft de gebruikersnaam voor aanmelding bij de HTTP-proxyserver aan.
`httpproxy.password`	`httpproxy.password=mypassword`	Geeft het wachtwoord voor aanmelding bij de HTTP-proxyserver aan.
`logon.embed.secret`	Geen	Een gedeeld geheim tussen een portal waarin BI-platformtoepassingen en de BI-platformtoepassingsserver zijn ingesloten. Het

Instelling	Standaardwaarden	Beschrijving
		geheim wordt gebruikt om te bepalen of BI-platformtoepassingen veilig in andere pagina's kunnen worden ingesloten.
`logon.embed.timeout`	`logon.embed.timeout=300`	Het aantal seconden waarna BI-platformtoepassingen zoals BI-startpunt niet langer in een portal worden ingesloten. Zorg dat de systeemklokken op de computers van de BI-platformwebserver en de portalserver binnen dit aantal seconden vallen.
`iview.autologoff`	`iview.autologoff=true`	Stel deze waarde in op `true` voor onmiddellijke automatische afmelding voor iViews in technologieplatform SAP NetWeaver.
`pinger.showWarningDialog`	`pinger.showWarningDialog=true`	Geeft aan of het waarschuwingsvenster wordt weergegeven met het bericht dat de huidige sessie binnenkort verloopt. Niet van toepassing op de CMC en BI-startpunt.
`ure.request.queue.timeout.seconds`	`ure.request.queue.timeout.seconds=20`	Het aantal seconden dat een aanvraag wacht op verwachte vorige aanvragen voordat deze een time-out geeft. Wanneer gebruikers navigatie of mapuitbreidingsacties in het besturingselement van de structuurlijst in het BI-startpunt uitvoeren, worden voor die acties AJAX-aanvragen in de wachtrij geplaatst. De gebruikersinterface wacht totdat deze aanvragen zijn voltooid voordat de besturing weer aan de gebruiker wordt gegeven. Deze instelling bepaalt het aantal seconden dat de gebruikersinterface op elke aanvraag wacht indien onverwachte vertragingen in de back-endquery optreden.
`enable.safe.html`	`enable.safe.html=true`	Activeert gebruik van veilige webpagina-URL's in de webpaginamodule-URL's voor BI-werkruimte.
`upload.file.maxsize.in MB`	`upload.file.maxsize.in MB = 0`	Hiermee wordt de maximale bestandsgrootte voor het uploaden van bestanden in megabytes opgegeven. Als de standaardwaarde 0 is ingesteld, kunnen bestanden van willekeurige grootte worden geüpload.
`upload.file.allowed.formats`	Geen	Hiermee worden de toegestane bestandsindelingen voor het uploaden van bestanden opgegeven. Zie 2296060 voor meer informatie.

Instelling	Standaardwaarden	Beschrijving
`upload.file.maxsize.in MB=0`	Geen	Maximale bestandsgrootte voor het uploaden van lokale documenten in megabytes. Dit moet een geheel getal zijn, bijvoorbeeld: 10, enz.
`upload.file.allowed.fo rmats=`	Geen	Deze eigenschap wordt gebruikt om verschillende bestandstypen te beheren die zijn toegestaan voor het uploaden van een lokaal document. Zie SAP Note 2296060 voor een lijst met ondersteunde bestandsindelingen. Als u meerdere indelingen definieert, moet u de bestandsindelingen van elkaar scheiden door een komma, zoals txt,doc,xls.
`offlinehelp.enabled=fa lse`	Geen	Stel de vlag offlineHelp in op 'true' om de offline Help in te schakelen. De standaardwaarde is ingesteld op 'false'.
`offlinehelp.url=`	Geen	De offlinehelp.url wordt weergegeven als de gebruiker de vlag 'offline' op 'true' heeft ingesteld.

18.4.1.2 Eigenschappen van BI-startpunt

In de volgende tabel staan de instellingen die zijn opgenomen in het standaardbestand `bilaunchpad.properties` voor het BOE.war-bestand. Maak een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om deze instellingen te overschrijven.

Instelling	Beschrijving
`app.name`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name=BI launch pad`
`app.name.short`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name.short=BI launch pad`
`app.url.name`	Geeft de URL-naam van de toepassing aan, voorafgegaan door het teken "/". Standaard: `app.url.name=/BI`
`authentication.default`	Geeft de standaardverificatiemethode aan die wordt gebruikt om gebruikers in de toepassing te verifiëren. U kunt een van de volgende mogelijkheden gebruiken voor deze instelling: **Verificatie** — **Waarde instelling** Enterprise — `secEnterprise`

Instelling	Beschrijving
	<table><tr><th>Verificatie</th><th>Waarde instelling</th></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> Standaard: authentication.default=secEnterprise
authentication.visible	Geeft aan of gebruikers die zich aanmelden bij het BI-startpunt, de mogelijkheid hebben om de verificatiemethode weer te geven en te wijzigen. Standaard: authentication.visible=false
Authentication.VisibleList	Geeft de zichtbaarheid aan van de lijst met beschikbare verificatietypen in het aanmeldingsscherm. Hieronder wordt de lijst met beschikbare verificatietypen weergegevens: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7. In de lijst kunt u ervoor kiezen om verificatietypen in of uit te schakelen door de gewenste verificatietypen op te nemen in of uit te sluiten van de Authentication.VisibleList. Standaard: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7
sap.system.client.visible authentication.sapSystem authentication.sapClient	Geeft de zichtbaarheid aan van de velden *SAP-systeem* en *SAP-client* wanneer u 'SAP' als verificatietype kiest. Standaard: sap.system.client.visible=true. Wanneer sap.system.client.visible is ingesteld op sap.system.client.visible=false, kunt u de waarden opgeven voor het SAP-systeem en de SAP-client in het eigenschappenbestand met respectievelijk de parameter authentication.sapSystem en authentication.sapClient.
cms.default	Geeft de standaardnaam van de CMS aan. Standaard: cms.default=[name of host machine]
cms.visible	Geeft aan of gebruikers die zich aanmelden bij het BI-startpunt, de mogelijkheid hebben om de CMS-naam weer te geven en te wijzigen. Standaard: cms.visible=true

Instelling	Beschrijving
`dialogue.prompt.enabled`	Geeft aan of gebruikers moeten worden gewaarschuwd als ze een invoerpagina in een dialoogvenster verlaten. Standaard: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Geeft aan of het maken van tokens wel of niet wordt ingeschakeld voor de sessie nadat een gebruiker zich aanmeldt bij het BI-startpunt. De token wordt opgeslagen in een cookie. Standaard: `logontoken.enabled=false`
`SMTPFrom`	Hiermee wordt het veld *Van* in- of uitgeschakeld wanneer een object naar een doel wordt gepland. Standaard: `SMTPFrom=true` Als de waarde is ingesteld op `false`, wordt het veld *Van* niet weergegeven en probeert het systeem de e-mailwaarde *Van* op te halen in de onderstaande volgorde: 1. Als eerste uit de standaardwaarde voor rapporten van een rapportobject. 2. Als tweede uit het e-mailadres in het gebruikersprofiel van de gebruiker die is aangemeld. 3. Als laatste uit de standaardwaarde voor de Job Server.
`url.exit`	Geeft aan naar welke URL gebruikers worden verwezen nadat ze hun BI-startpuntsessie hebben beëindigd. Deze instelling is alleen van toepassing op gebruikers die zich hebben aangemeld bij de toepassing via een extern verificatieproces.
`disable.locale.preference`	Geeft aan of gebruikers de voorkeurslandinstellingen voor weergave in het BI-startpunt kunnen weergeven en dus wijzigen. Standaard: `disable.locale.preference=false`
`extlogon.allow.logoff`	Hiermee wordt het automatisch afmelden van gebruikerssessies in- of uitgeschakeld als gebruikers eenmaal hun BI-startpuntsessie hebben afgesloten. Stel de waarde in op false als u niet wilt dat gebruikerssessies automatisch worden beëindigd wanneer gebruikers zich afmelden van het BI-startpunt. Standaard: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Hiermee wordt opgegeven of andere pagina's moeten worden toegestaan om deze toepassing (als frame) in te sluiten zonder een geldig insluitingstoken door te geven. Standaard: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Hiermee wordt een door komma's gescheiden lijst met SSO-typen opgegeven die moeten worden ingeschakeld, evenals de volgorde waarin ze worden uitgevoerd. Een lege lijst geeft aan dat de verouderde volgorde moet worden gebruikt.

Instelling	Beschrijving
	Als de lijst wordt opgegeven, worden de verouderde opties genegeerd. Geldige opties: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` en `siteminder`. Als u geen van deze opties wilt gebruiken, kiest u: `none`
`allowed.cms`	Om veilige aanmelding te garanderen en SSRF (Server-Side Request Forgery) te voorkomen, kunt u een witte lijst maken met geldige CMS-namen of IP's, in combinatie met de poortnummers. U wordt alleen bij de toepassing aangemeld als de waarde die tijdens aanmelding wordt ingevoerd exact overeenkomt met de waarde op de witte lijst. Voer de lijst met CMS-namen of IP's in combinatie met het poortnummer in de eigenschap allowed.cms in. Bijvoorbeeld `allowed.cms =<cms name or IP>:<port number>.` Als u meerdere CMS'en hebt waarmee u verbinding wilt maken, voert u de waarden gescheiden door een komma (,) in, zoals hieronder te zien is: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Opmerking** • Als u wilt aanmelden met de CMS-naam of de IP, voegt u beide toe aan de eigenschap `allowed.cms`. • Omdat het poortnummer optioneel is in het aanmeldingsscherm, kunt u ervoor kiezen om het weg te laten op de witte lijst. U wordt dan aangemeld bij de standaardpoort. Als het poortnummer echter wel op de witte lijst staat en niet wordt ingevoerd tijdens aanmelding, mislukt de aanmelding. Hieronder volgen de scenario's waarvoor het gebruik van een witte lijst niet vereist is. • Als de waarde van `cms.visible` is ingesteld op false en er een CMS is ingesteld voor `cms.default` • Als de CMS is geclusterd en u zich aanmeldt met de clusternaam. Als u zich probeert aan te melden

Instelling	Beschrijving
	bij een specifieke cluster (CMS), moet de CMS-naam aanwezig zijn in de eigenschap `allowed.cms`. • Als eenmalige aanmelding wordt gebruikt voor aanmelding.

18.4.1.3 Eigenschappen van het Fiorified BI-startpunt

In de volgende tabel staan de instellingen die zijn opgenomen in het standaardbestand `FioriBI.properties` voor het BOE.war-bestand. Maak een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om deze instellingen te overschrijven.

> **Opmerking**
>
> In BI 4.2 SP5 wordt de naam van bestand “Bing.properties” gewijzigd in bestand “FioriBI.properties”. Wanneer u een oudere versie bijwerkt of een upgrade uitvoert naar BI 4.2 SP5, moet u de naam van het eigenschappenbestand van het Fiorified BI-startpunt handmatig wijzigen van “Bing.properties” in “FioriBI.properties” om de bestaande configuraties voor het Fiorified BI-startpunt te behouden.

Instelling	Beschrijving
`app.name`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name=BI launch pad`
`app.name.short`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name.short=BI launch pad`
`app.url.name`	Geeft de URL-naam van de toepassing aan, voorafgegaan door het teken “/”. Standaard: `app.url.name=/BILaunchpad`
`authentication.default`	Geeft de standaardverificatiemethode aan die wordt gebruikt om gebruikers in de toepassing te verifiëren. U kunt een van de volgende mogelijkheden gebruiken voor deze instelling: **Verificatie** — **Waarde instelling** Enterprise — `secEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3`

Instelling	Beschrijving
	<table><tr><th>Verificatie</th><th>Waarde instelling</th></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> Standaard: authentication.default=secEnterprise
authentication.visible	Geeft aan of gebruikers die zich aanmelden bij het Fiorified BI-startpunt, de mogelijkheid hebben om de verificatiemethode weer te geven en te wijzigen. Standaard: authentication.visible=false
Authentication.VisibleList	Geeft de zichtbaarheid aan van de lijst met beschikbare verificatietypen in het aanmeldingsscherm. Hieronder wordt de lijst met beschikbare verificatietypen weergegevens: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7. In de lijst kunt u ervoor kiezen om verificatietypen in of uit te schakelen door de gewenste verificatietypen op te nemen in of uit te sluiten van de Authentication.VisibleList. Standaard: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7
sap.system.client.visible authentication.sapSystem authentication.sapClient	Geeft de zichtbaarheid aan van de velden *SAP-systeem* en *SAP-client* wanneer u 'SAP' als verificatietype kiest. Standaard: sap.system.client.visible=true. Wanneer sap.system.client.visible is ingesteld op sap.system.client.visible=false, kunt u de waarden opgeven voor het SAP-systeem en de SAP-client in het eigenschappenbestand met respectievelijk de parameter authentication.sapSystem= en authentication.sapClient=.
cms.default	Geeft de standaardnaam van de CMS aan. Standaard: cms.default=[name of host machine]
cms.visible	Geeft aan of gebruikers die zich aanmelden bij het Fiorified BI-startpunt, de mogelijkheid hebben om de CMS-naam weer te geven en te wijzigen. Standaard: cms.visible=true
dialogue.prompt.enabled	Geeft aan of gebruikers moeten worden gewaarschuwd als ze een invoerpagina in een dialoogvenster verlaten. Standaard: dialogue.prompt.enabled=false

Instelling	Beschrijving
`logontoken.enabled`	Geeft aan of het maken van tokens wel of niet wordt ingeschakeld voor de sessie nadat een gebruiker zich aanmeldt bij het BI-startpunt. De token wordt opgeslagen in een cookie. Standaard: `logontoken.enabled=false`
`SMTPFrom`	Hiermee wordt het veld *Van* in- of uitgeschakeld wanneer een object naar een doel wordt gepland. Standaard: `SMTPFrom=true` Als de waarde is ingesteld op `false`, wordt het veld *Van* niet weergegeven en probeert het systeem de e-mailwaarde *Van* op te halen in de onderstaande volgorde: 1. Als eerste uit de standaardwaarde voor rapporten van een rapportobject. 2. Als tweede uit het e-mailadres in het gebruikersprofiel van de gebruiker die is aangemeld. 3. Als laatste uit de standaardwaarde voor de Job Server.
`url.exit`	Geeft aan naar welke URL gebruikers worden verwezen nadat ze hun Fiorified BI-startpuntsessie hebben beëindigd. Deze instelling is alleen van toepassing op gebruikers die zich hebben aangemeld bij de toepassing via een extern verificatieproces.
`disable.locale.preference`	Geeft aan of gebruikers de voorkeurslandinstellingen voor weergave in het Fiorified BI-startpunt kunnen weergeven en dus wijzigen. Standaard: `disable.locale.preference=false`
`extlogon.allow.logoff`	Hiermee wordt het automatisch afmelden van gebruikerssessies in- of uitgeschakeld als gebruikers eenmaal hun Fiorified BI-startpuntsessie hebben afgesloten. Stel de waarde in op false als u niet wilt dat gebruikerssessies automatisch worden beëindigd wanneer gebruikers zich afmelden van het BI-startpunt. Standaard: `extlogon.allow.logoff=true`
`logon.allowInsecureEmbedding`	Hiermee wordt opgegeven of andere pagina's moeten worden toegestaan om deze toepassing (als frame) in te sluiten zonder een geldig insluitingstoken door te geven. Standaard: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Hiermee wordt een door komma's gescheiden lijst met SSO-typen opgegeven die moeten worden ingeschakeld, evenals de volgorde waarin ze worden uitgevoerd. Een lege lijst geeft aan dat de verouderde volgorde moet worden gebruikt. Als de lijst wordt opgegeven, worden de verouderde opties genegeerd.

Instelling	Beschrijving
	Geldige opties: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO` en `siteminder`. Als u geen van deze opties wilt gebruiken, kiest u: `none`
`allowed.cms`	Om veilige aanmelding te garanderen en SSRF (Server-Side Request Forgery) te voorkomen, kunt u een witte lijst maken met geldige CMS-namen of IP's, in combinatie met de poortnummers. U wordt alleen bij de toepassing aangemeld als de waarde die tijdens aanmelding wordt ingevoerd exact overeenkomt met de waarde op de witte lijst. Voer de lijst met CMS-namen of IP's in combinatie met het poortnummer in de eigenschap allowed.cms in. Bijvoorbeeld `allowed.cms =<cms name or IP>:<port number>.` Als u meerdere CMS-en hebt waarmee u verbinding wilt maken, voert u de waarden gescheiden door een komma (,) in, zoals hieronder te zien is: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Opmerking** • Als u wilt aanmelden met de CMS-naam of de IP, voegt u beide toe aan de eigenschap `allowed.cms`. • Omdat het poortnummer optioneel is in het aanmeldingsscherm, kunt u ervoor kiezen om het weg te laten op de witte lijst. U wordt dan aangemeld bij de standaardpoort. Als het poortnummer echter wel op de witte lijst staat en niet wordt ingevoerd tijdens aanmelding, mislukt de aanmelding. Hieronder volgen de scenario's waarvoor het gebruik van een witte lijst niet vereist is. • Als de waarde van `cms.visible` is ingesteld op false en er een CMS is ingesteld voor `cms.default` • Als de CMS is geclusterd en u zich aanmeldt met de clusternaam. Als u zich probeert aan te melden bij een specifieke cluster (CMS), moet de CMS-naam aanwezig zijn in de eigenschap `allowed.cms`.

Instelling	Beschrijving
	• Als eenmalige aanmelding wordt gebruikt voor aanmelding.
upload.file.maxsize.inMB=0	Maximale bestandsgrootte voor het uploaden van lokale documenten in megabytes. Dit moet een geheel getal zijn, bijvoorbeeld: 10, enz.
upload.file.allowed.formats=	Deze eigenschap wordt gebruikt om verschillende bestandstypen te beheren die zijn toegestaan voor het uploaden van een lokaal document. Zie SAP Note 2296060 voor een lijst met ondersteunde bestandsindelingen. Als u meerdere indelingen definieert, moet u de bestandsindelingen van elkaar scheiden door een komma, zoals txt,doc,xls.
app.custom.banner.message	Geeft het bannerbericht in het BI-startpunt aan.
logon.webssoauthnetication.framework=None	Deze eigenschap wordt gebruikt om de workflow Web SSO-verificatie in te schakelen. De mogelijke waarden zijn Geen, OpenId en SAML.
openid.restful.url=	Deze eigenschap wordt gebruikt om de Restful-URL in te stellen, die wordt opgegeven in CMC. Bijvoorbeeld: `http://<hostname>:<portNo>/biprws`

18.4.1.4 OpenDocument-eigenschappen

In de volgende tabel staan de instellingen die zijn opgenomen in het standaardbestand `opendocument.properties` voor het BOE.war-bestand. Maak een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om deze instellingen te overschrijven.

Instelling	Beschrijving
`app.name`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name=SAP BusinessObjects OpenDocument`
`app.name.short`	Geeft de weergavenaam van de toepassing aan. De naam wordt weergegeven op de titelpagina en het aanmeldingsscherm van de webtoepassing. Standaard: `app.name.short=OpenDocument`
`authentication.default`	Geeft de standaardverificatiemethode aan die wordt gebruikt om gebruikers in de toepassing te verifiëren. U

Instelling	Beschrijving
	kunt een van de volgende mogelijkheden gebruiken voor deze instelling: **Verificatie** / **Waarde instelling** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracles EBS: `secOraApps` Standaard: `authentication.default=secEnterprise`
`authentication.visible`	Geeft aan of gebruikers die zich aanmelden bij OpenDocument, de mogelijkheid hebben om de verificatiemethode weer te geven en te wijzigen. Standaard: `authentication.visible=false`
`Authentication.VisibleList`	Geeft de zichtbaarheid aan van de lijst met beschikbare verificatietypen in het aanmeldingsscherm. Hieronder wordt de lijst met beschikbare verificatietypen weergegevens: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. In de lijst kunt u ervoor kiezen om verificatietypen in of uit te schakelen door de gewenste verificatietypen op te nemen in of uit te sluiten van de `Authentication.VisibleList`. Standaard: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
 	
`authentication.sapSystem`
 	
`authentication.sapClient`
	Geeft de zichtbaarheid aan van de velden *SAP-systeem* en *SAP-client* wanneer u 'SAP' als verificatietype kiest. Standaard: `sap.system.client.visible=true`. Wanneer `sap.system.client.visible` is ingesteld op `sap.system.client.visible=false`, kunt u de waarden opgeven voor het SAP-systeem en de SAP-client in het eigenschappenbestand met respectievelijk de parameter `authentication.sapSystem=` en `authentication.sapClient=`.

`cms.default`	Geeft de standaardnaam van de CMS aan. Standaard: `cms.default=[name of host machine]`

Instelling	Beschrijving
`cms.visible`	Geeft aan of gebruikers die zich aanmelden bij OpenDocument, de mogelijkheid hebben om de CMS-naam weer te geven en te wijzigen. Standaard: `cms.visible=true`
`logontoken.enabled`	Geeft aan of het maken van tokens wel of niet wordt ingeschakeld voor de sessie nadat een gebruiker zich aanmeldt bij OpenDocument. De token wordt opgeslagen in een cookie. Standaard: `logontoken.enabled=false`
`extlogon.allow.logoff`	Hiermee wordt het automatisch afmelden van gebruikerssessies in- of uitgeschakeld als gebruikers eenmaal hun OpenDocument-sessie hebben afgesloten. Stel de waarde in op False als u niet wilt dat gebruikerssessies automatisch worden beëindigd wanneer gebruikers zich afmelden van OpenDocument. Standaard: `extlogon.allow.logoff=true`
`SAPLogonToken.enabled`	Hiermee wordt opgegeven of SAP-aanmeldingstokens van de RESTful-webservice zijn toegestaan voor verificatie bij het BI-platform. De SAP-aanmeldingstoken wordt opgegeven door de waarde van de X-SAP-LogonToken in de aanvraagheader na een geslaagde aanmelding bij de URL van de RESTful-webservice. Standaard: `SAPLogonToken.enabled=true`
`logon.allowInsecureEmbedding=false`	Hiermee wordt opgegeven of andere pagina's moeten worden toegestaan om deze toepassing (als frame) in te sluiten zonder een geldig insluitingstoken door te geven. Standaard: `logon.allowInsecureEmbedding=false`
`sso.types.and.order`	Hiermee wordt een door komma's gescheiden lijst met SSO-typen opgegeven die moeten worden ingeschakeld, evenals de volgorde waarin ze worden uitgevoerd. Een lege lijst geeft aan dat de verouderde volgorde moet worden gebruikt. Als de lijst wordt opgegeven, worden de verouderde opties genegeerd. Geldige opties: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO` en `siteminder`. Als u geen van deze opties wilt gebruiken, kiest u: `none`
`allowed.cms`	Om veilige aanmelding te garanderen en SSRF (Server-Side Request Forgery) te voorkomen, kunt u een witte lijst maken met geldige CMS-namen of IP's, in combinatie met de poortnummers. U wordt alleen bij de toepassing aangemeld

Instelling	Beschrijving
	als de waarde die tijdens aanmelding wordt ingevoerd exact overeenkomt met de waarde op de witte lijst. Voer de lijst met CMS-namen of IP's in combinatie met het poortnummer in de eigenschap allowed.cms in. Bijvoorbeeld `allowed.cms =<cms name or IP>:<port number>.` Als u meerdere CMS'en hebt waarmee u verbinding wilt maken, voert u de waarden gescheiden door een komma (,) in, zoals hieronder te zien is: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **Opmerking** • Als u wilt aanmelden met de CMS-naam of de IP, voegt u beide toe aan de eigenschap `allowed.cms`. • Omdat het poortnummer optioneel is in het aanmeldingsscherm, kunt u ervoor kiezen om het weg te laten op de witte lijst. U wordt dan aangemeld bij de standaardpoort. Als het poortnummer echter wel op de witte lijst staat en niet wordt ingevoerd tijdens aanmelding, mislukt de aanmelding. Hieronder volgen de scenario's waarvoor het gebruik van een witte lijst niet vereist is. • Als de waarde van `cms.visible` is ingesteld op false en er een CMS is ingesteld voor `cms.default` • Als de CMS is geclusterd en u zich aanmeldt met de clusternaam. Als u zich probeert aan te melden bij een specifieke cluster (CMS), moet de CMS-naam aanwezig zijn in de eigenschap `allowed.cms`. • Als eenmalige aanmelding wordt gebruikt voor aanmelding.

18.4.1.5 CMC-eigenschappen

In de volgende tabel staan de instellingen die zijn opgenomen in het standaardbestand `cmc.properties` voor BOE.war. Maak een nieuw bestand in `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` om deze instellingen te overschrijven.

Instelling	Beschrijving
`app.url.name`	Geeft de URL-naam van de toepassing aan, voorafgegaan door het teken "/". Standaard: `app.url.name=/CMC`
`authentication.default`	Geeft de standaardverificatiemethode aan die wordt gebruikt om gebruikers in de toepassing te verifiëren. U kunt een van de volgende mogelijkheden gebruiken voor deze instelling: **Verificatie** / **Waarde instelling** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracles EBS: `secOraApps` Standaard: `authentication.default=secEnterprise`
`authentication.visible`	Geeft aan of gebruikers die zich aanmelden bij de CMC, de mogelijkheid hebben om de verificatiemethode weer te geven en te wijzigen. Standaard: `authentication.visible=false`
`Authentication.VisibleList`	Geeft de zichtbaarheid aan van de lijst met beschikbare verificatietypen in het aanmeldingsscherm. Hieronder wordt de lijst met beschikbare verificatietypen weergegevens: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. In de lijst kunt u ervoor kiezen om verificatietypen in of uit te schakelen door de gewenste verificatietypen op te nemen in of uit te sluiten van de `Authentication.VisibleList`. Standaard: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

`sap.system.client.visible`
 	
`authentication.sapSystem`
 	
`authentication.sapClient`
	Geeft de zichtbaarheid aan van de velden *SAP-systeem* en *SAP-client* wanneer u 'SAP' als verificatietype kiest. Standaard: `sap.system.client.visible=true`. Wanneer `sap.system.client.visible` is ingesteld op `sap.system.client.visible=false`, kunt u de waarden opgeven voor het SAP-systeem en de SAP-client in het eigenschappenbestand met respectievelijk de parameter `authentication.sapSystem=` en `authentication.sapClient=`.

Instelling	Beschrijving
`cms.default`	Geeft de standaardnaam van de CMS aan. Standaard: `cms.default=[name of host machine]`
`cms.visible`	Geeft aan of gebruikers die zich aanmelden bij de CMC, de mogelijkheid hebben om de CMS-naam weer te geven en te wijzigen. Standaard: `cms.visible=true`
`dialogue.prompt.enabled`	Geeft aan of gebruikers moeten worden gewaarschuwd als ze een invoerpagina in een dialoogvenster verlaten. Standaard: `dialogue.prompt.enabled=false`
`logontoken.enabled`	Geeft aan of het maken van tokens wel of niet wordt ingeschakeld voor de sessie nadat een gebruiker zich aanmeldt bij de CMC. De token wordt opgeslagen in een cookie. Standaard: `logontoken.enabled=false`
`SMTPFrom`	Hiermee wordt het veld *Van* in- of uitgeschakeld wanneer een object naar een doel wordt gepland. Standaard: `SMTPFrom=true` Als de waarde is ingesteld op `false`, wordt het veld *Van* niet weergegeven en probeert het systeem de e-mailwaarde *Van* op te halen in de onderstaande volgorde: 1. Als eerste uit de standaardwaarde voor rapporten van een rapportobject. 2. Als tweede uit het e-mailadres in het gebruikersprofiel van de gebruiker die is aangemeld. 3. Als laatste uit de standaardwaarde voor de Job Server.
`ulr.exit`	Geeft de URL aan waarmee gebruikers worden doorverwezen nadat ze hun CMC-sessie hebben beëindigd. Deze instelling is alleen van toepassing op gebruikers die zich hebben aangemeld bij de toepassing via een extern verificatieproces.
`allowed.cms`	Om veilige aanmelding te garanderen en SSRF (Server-Side Request Forgery) te voorkomen, kunt u een witte lijst maken met geldige CMS-namen of IP's, in combinatie met de poortnummers. U wordt alleen bij de toepassing aangemeld als de waarde die tijdens aanmelding wordt ingevoerd exact overeenkomt met de waarde op de witte lijst. Voer de lijst met CMS-namen of IP's in combinatie met het poortnummer in de eigenschap allowed.cms in. Bijvoorbeeld `allowed.cms =<cms name or IP>:<port number>.` Als u meerdere CMS'en hebt waarmee u verbinding wilt maken, voert u de waarden gescheiden door een komma (,) in, zoals hieronder te zien is: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`

Instelling	Beschrijving
	Opmerking • Als u wilt aanmelden met de CMS-naam of de IP, voegt u beide toe aan de eigenschap `allowed.cms`. • Omdat het poortnummer optioneel is in het aanmeldingsscherm, kunt u ervoor kiezen om het weg te laten op de witte lijst. U wordt dan aangemeld bij de standaardpoort. Als het poortnummer echter wel op de witte lijst staat en niet wordt ingevoerd tijdens aanmelding, mislukt de aanmelding. Hieronder volgen de scenario's waarvoor het gebruik van een witte lijst niet vereist is. • Als de waarde van `cms.visible` is ingesteld op false en er een CMS is ingesteld voor `cms.default` • Als de CMS is geclusterd en u zich aanmeldt met de clusternaam. Als u zich probeert aan te melden bij een specifieke cluster (CMS), moet de CMS-naam aanwezig zijn in de eigenschap `allowed.cms`. • Als eenmalige aanmelding wordt gebruikt voor aanmelding.

18.5 Ingangspunten voor aanmelding bij BI-startpunt en OpenDocument aanpassen

U kunt de aanmeldingspagina voor het BI-startpunt en OpenDocument-webtoepassingen aanpassen. U kunt bijvoorbeeld de aanmeldingspagina aanpassen om een bedrijfslogo of -opmaakmodel te gebruiken, of u kunt een aangepaste aanmeldingspagina maken die vertrouwde verificatie inschakelt.

Wilt u de aanmeldingspagina aanpassen, dan wijzigt u het bestand `custom.jsp` dat is opgeslagen in de toepassingsgebieden BI-startpunt en OpenDocument van de `BOE.war`-webtoepassing, en vervolgens implementeert u de `BOE.war`-webtoepassing opnieuw op uw BI-platformsysteem. Gebruikers hebben toegang tot het ingangspunt voor aanmelding door naar een unieke URL te navigeren.

U moet bekend zijn met het implementeren van webtoepassingen van BI-platform om met deze voorbeelden te werken. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie.

18.5.1 Bestandslocaties van het BI-startpunt en OpenDocument

De webtoepassingen BI-startpunt en OpenDocument zijn gebundeld in het `BOE.war`-webarchiefbestand. De locatie van het `BOE.war`-archief is gedefinieerd in het bestand `BOE.properties`.

Op Windows-systemen vindt u het bestand `BOE.properties` hier:

- `<BOE_INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

Op UNIX-systemen vindt u het bestand `BOE.properties` hier:

- `<BOE_INSTALLATIEMAP>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

De volgende tabellen definiëren de locatie van algemene bestanden in het `BOE.war`-webarchiefbestand voor de toepassingen BI-startpunt en OpenDocument.

Bestandslocaties voor BI-startpunt

> **Opmerking**
>
> De webtoepassing BI-startpunt heette voorheen InfoView.

Type bestand	Locatie
Aangepast aanmeldings-script	`WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`
Map voor extra bestanden	`WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`
Aangepaste aanmeldings-URL	`http://<servernaam>:<poort>/BOE/BI/custom.jsp`

Bestandslocaties voor OpenDocument

Type bestand	Locatie
Aangepast aanmeldings-script	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp`
Map voor extra bestanden	`WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources`
Aangepaste aanmeldings-URL	`http://<servernaam>:<poort>/BOE/OpenDocument/opendoc/custom.jsp`

18.5.2 Een aangepaste aanmeldingspagina definiëren

U kunt de aanmeldingspagina voor BI-platform aanpassen. U kunt bijvoorbeeld een aangepaste aanmeldingspagina maken die een bedrijfslogo weergeeft en een bedrijfsopmaakmodel gebruikt.

Bewerk het bestand `custom.jsp` om de aanmelding voor uw gebruikers aan te passen, en plaats ondersteuningsbestanden in de map `noCacheCustomResources`.

In dit voorbeeld wordt weergegeven hoe u een aangepaste aanmeldingspagina maakt die de gebruiker doorverwijst naar de standaardaanmeldingspagina.

1. Maak een bestand dat uw aangepaste aanmeldingscode bevat, en sla het op als `custom.js` in de map `noCacheCustomResources`.

   In dit voorbeeld wordt een functie gedefinieerd die de gebruiker doorverwijst naar de standaardaanmeldingspagina `logon.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. Bewerk het bestand `custom.jsp` om de aanmeldingspagina aan te passen.

   In dit voorbeeld wordt een welkomstbericht en een hyperlink weergegeven die de methode `load` aanroept die is gedefinieerd in het bestand `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. Implementeer de `BOE.war`-webtoepassing opnieuw, en start de webserver opnieuw.

18.5.3 Vertrouwde verificatie toevoegen bij aanmelding

Wilt u vertrouwde verificatie inschakelen, dan stelt u de vertrouwde gebruiker in als een sessie-attribuut in het bestand `custom.jsp`, en wijzigt u de verificatie-instellingen in een kopie van het bestand `global.properties`. De waarden van de aangepaste kopie van het bestand `global.properties` overschrijven de standaardwaarden.

> **Opmerking**
>
> Om veiligheidsredenen mag vertrouwde verificatie alleen worden ingeschakeld met HTTPS. Als u vertrouwde verificatie zonder HTTPS hebt ingeschakeld, wordt dit als een inbreuk op de beveiliging beschouwd omdat de URL voor onbevoegde gebruikers wordt weergegeven. Om een inbreuk op de beveiliging te voorkomen, kunnen de gebruikersgegevens worden gevalideerd met een geldig certificaat. Zie 1388240 voor meer informatie.

1. Bewerk het bestand `custom.jsp` om een sessie-attribuut in te stellen dat de vertrouwde gebruiker definieert.

   ```
   request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
   ```

2. Maak een aangepaste kopie van het bestand `global.properties` door `WEB-INF\config\default\global.properties` te kopiëren naar `WEB-INF\config\custom\global.properties`.
3. Wijzig `WEB-INF\config\custom\global.properties` om eenmalige aanmelding in te schakelen.

   ```
   sso.enabled=true
   ```

4. Wijzig `WEB-INF\config\custom\global.properties` om parameters voor vertrouwde verificatie in te stellen, waaronder de sessievariabele voor de vertrouwde gebruiker en het gedeelde geheim.

   Vervang `"..."` door het gedeelde geheim voor uw systeem.

   ```
   trusted.auth.user.param=TrustedUserAttribute
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.shared.secret="..."
   ```

   Voor meer informatie leest u het verwante onderwerp over configuratie van vertrouwde verificatie voor webtoepassingen.
5. Implementeer uw webtoepassing opnieuw, en start de webserver opnieuw.
6. Activeer vertrouwde verificatie in de CMC.

   Dubbelklik op het tabblad *Verificatie* op *Enterprise* en schakel het selectievakje *Vertrouwde verificatie is ingeschakeld* in.

Verwante informatie

Vertrouwde verificatie inschakelen [pagina 256]
Vertrouwde verificatie voor de webtoepassing configureren [pagina 263]

18.6 Gebruikersinterfaces toepassing aanpassen

Bepaalde gebruikersinterfaces van toepassingen kunnen worden aangepast via de CMC.

In de Central Management Console kunt u de vormgeving van bepaalde toepassingen aanpassen. Bijvoorbeeld: u kunt gebruikersinterface-elementen in-/uitschakelen.

18.6.1 Web Intelligence

18.6.1.1 Interface-elementen van Web Intelligence aanpassen per gebruikersgroepen en mappen

Door middel van aanpassing kunt u meerdere interface-elementen verbergen om de manier waarop eindgebruikers interactie hebben met de toepassing te vereenvoudigen, afhankelijk van gebruikersgroepen en mappen die Web Intelligence-documenten bevatten. U kunt typen gegevensbronnen verwerken, de bewerkingsmodus in-/uitschakelen, de automatische vernieuwingsfunctie uitschakelen, en nog veel meer.

Standaard is elk interface-element ingeschakeld. Als u deze wilt verbergen, kunt u dit doen in de Central Management Console. In de onderstaande tabel worden de gebruikersinterface-elementen vermeld die u kunt verbergen.

Functielijst	Beschrijving
Modus	Verbergt de beschikbare modi waartoe de gebruiker toegang heeft via de vervolgkeuzeknop. • Lezen Om de leesmodus te verbergen in de vervolgkeuzeknop. • Ontwerpen Om ontwerp- en structuurmodi te verbergen in de vervolgkeuzeknop. • Gegevens Om de modus Gegevens te verbergen in de vervolgkeuzeknop. Als alle modi zijn uitgeschakeld, kunnen documenten alleen worden geopend in de modus Lezen.
Locatie	Verbergt een gehele categorie gegevensbronnen. U kunt de volgende categorieën uitschakelen: • Gegevensopslagruimte BI-platform • Lokaal (alleen beschikbaar in Rich CLient) • Webservices • Google Drive • Microsoft OneDrive

Functielijst	Beschrijving
Gegevensbron	In de modus Ontwerp kunt u de gegevensbronnen beperken die beschikbaar zijn in de dialoogvensters *Een gegevensbron selecteren* en *Bron wijzigen*. U kunt de volgende gegevensbronnen uitschakelen: • Universes • Web Intelligence-documenten • Excel-bestanden • Tekstbestanden • SAP BW • SAP HANA-weergaven • Vrije SQL-query's • OData • Google-werkblad
Query	• Vernieuwen Verbergt in de leesmodus de sectie *Gegevens* in de werkbalk. Verbergt in de ontwerpmodus het vervolgkeuzemenu *Vernieuwen*, de opdracht *Alles vernieuwen*, de knop *Uitvoeren* en het bijbehorende vervolgkeuzemenu in het queryvenster. • Geavanceerd vernieuwen Verbergt in de ontwerpmodus de opdracht *Geavanceerd* vernieuwen in het vervolgkeuzemenu *Vernieuwen*. • Automatisch vernieuwen Verbergt de optie *Automatisch vernieuwen* in de presentatiemodus. • Bron wijzigen Verbergt in de modus Ontwerp de mogelijkheid om de gegevensbronnen van het document te wijzigen.
Gegevens	Verbergt de functies Kubussen combineren in de modus Gegevens.
Analyse	• Analyseren Verbergt in zowel de leesmodus als de ontwerpmodus het selectievakje *Analyseren* in de sectie Analyseren van de werkbalk en analysefilters in de *Filterbalk*. Ook worden in het rapport waarden die niet kunnen worden geanalyseerd niet weergegeven als hyperlinks en zijn de analyseacties en -pictogrammen die beschikbaar zijn voor deze waarden verborgen. Verbergt in de modus Ontwerpen de analysefilters in het venster *Maken*, onder *Gegevensfilters*. • Gegevenswijzigingen bijhouden In de modus Lezen en Ontwerp verbergt u *Gegevenswijzigingen bijhouden* en *Wijzigingen weergeven* uit de werkbalk.

Functielijst	Beschrijving
Documenten	• *Nieuw*, *Openen*, *Opslaan*, *Favorieten*, *Presentatiemodus*. Verbergt de bijhorende knoppen uit de werkbalk. • Opmerkingen Verbergt in zowel de leesmodus als de ontwerpmodus het tabblad *Opmerkingen* in het zijvenster en de opdracht *Opmerkingen* in het contextmenu. • Gedeelde elementen Verbergt in de ontwerpmodus het tabblad *Gedeelde elementen* in het zijvenster en de opdracht *Gedeelde elementen* in de sectie *Invoegen* van de werkbalk.
Exporteren naar	Verbergt in elke modus de mogelijkheid om documentrapporten en kubussen te exporteren naar: • Excel • PDF • HTML • TXT • CSV
Koppeling genereren	Verbergt in de modus Ontwerp de mogelijkheid uit om een OpenDocument-koppeling te maken en OData-koppelingen te genereren voor query's en afzonderlijke rapportelementen van contextmenu's.
Plannen en publiceren	Verbergt de mogelijkheid om documenten te plannen en te publiceren in TXT, XLS, PDF, HTML, MHTML en CSV.

18.6.1.1.1 Aanpassingsinterface

U kunt afzonderlijke mappen selecteren, zodat de aanpassing automatisch wordt toegepast op de documenten die deze bevatten. Selecteer een of meer mappen in het gebied *Aangepaste mappen* en ga naar het tabblad *Functies* om te beginnen met aanpassen. Standaard wordt de aanpassing toegepast op elk document in de map die u hebt geselecteerd.

Op het tabblad *Functies* worden alle functies vermeld die u kunt inschakelen of uitschakelen. Gebruik de relevante selectievakjes om ze in- of uit te schakelen.

18.6.1.1.2 Aanpassingsregels

De volgende regels worden gebruikt om het toepassen van aanpassingen op een gebruiker te definiëren:

- Als de gebruiker bij verschillende groepen hoort, is alleen de aanpassing van toepassing die is gedefinieerd voor de groep waarvan de ID lager is. De aanpassing die voor de andere groepen waarvan de gebruiker deel uitmaakt, is niet van toepassing.

- Voor een structuur met geneste mappen worden aanpassingen voor het document voor elementen van de gebruikersinterface, voor functies en voor uitbreidingsmodules gedefinieerd door de onmiddellijk bovenliggende map van het document dat in de lijst met aangepaste mappen is toegevoegd.
- De aanpassing die voor Standaardmappen is gedefinieerd, is van toepassing op de documenten die in Persoonlijke documenten en Postvakken IN zijn opgeslagen, en voor documenten waarvoor de bovenliggende map niet is aangepast.
- De aanpassing die voor elementen van de gebruikersinterface is gedefinieerd, heeft voorrang boven de aanpassing die voor functies is gedefinieerd, aangezien functies slechts een snelkoppeling zijn om alle elementen van de gebruikersinterface in te schakelen.
- Scenario: Wanneer de aanpassingselementen worden weergegeven als een structuurlijst en u een knooppunt op een systeem uitschakelt. Als u dit systeem bijwerkt met een nieuwere versie van het product met nieuwe items in de knooppunten, worden deze items standaard geactiveerd, zelfs als het bovenste knooppunt is uitgeschakeld.

18.6.1.1.3 De weergave van de Web Intelligence-interface aanpassen

U kunt de weergave van de Web Intelligence-gebruikersinterface aanpassen door menu-items, subitems en functies te verbergen voor een geselecteerde gebruikersgroep en documentmap.

1. Meld u als beheerder aan bij de CMC.
2. Selecteer in de lijst *Ordenen* de optie *Gebruikers en groepen*.
3. Selecteer een gebruikersgroep in de lijst *Groepshiërarchie*.
4. Klik in de lijst *Acties* op *Aanpassing*.
5. Voer een van de volgende handelingen uit op in de sectie *Aangepaste mappen*:

Optie	Beschrijving
Een standaardaanpassing definiëren	1. Selecteer *Standaardmappen* in het gebied *Aangepaste mappen*.
De documentmappen toevoegen waarop u aanpassing wilt toepassen voor de geselecteerde gebruikersgroep	1. Klik op *Map toevoegen*. 2. Selecteer de mappen. De mappen worden in het gebied *Aangepaste mappen* weergegeven.
Het opnieuw definiëren van dezelfde aanpassing voor andere mappen voorkomen	1. Selecteer in het gebied *Aangepaste mappen* de map van waaruit u de aanpassing wilt kopiëren. 2. Klik in de vervolgkeuzelijst op *Aanpassing dupliceren*. 3. Selecteer de map waarvoor u de aanpassing wilt definiëren. 4. Klik op *Aanpassing plakken*. 5. Ga naar stap 7.
De aanpassing voor een bepaalde map verwijderen	1. Selecteer de map in het gebied *Aangepaste mappen*. 2. Klik in de vervolgkeuzelijst op *Map verwijderen*. 3. Ga naar stap 7.

Optie	Beschrijving
	ⓘ Opmerking U kunt *Standaardmappen* niet verwijderen.

6. Selecteer of deselecteer elementen op het tabblad *Functies* om deze weer te geven of te verbergen in Web Intelligence.

   Als u alle onderliggende elementen van een bovenliggend element deselecteert, wordt het bovenliggende element ook gedeselecteerd en verborgen in Web Intelligence. Zie Interface-elementen van Web Intelligence aanpassen per gebruikersgroepen en mappen [pagina 776] voor meer informatie.
7. Klik op *Opslaan en sluiten*.

Wanneer u de aanpassing opslaat, zien alle gebruikers van de geselecteerde groep deze wijzigingen wanneer ze zich de volgende keer aanmelden bij BI-startpunt en Web Intelligence openen.

> ⓘ Opmerking
>
> Het is raadzaam u aan te melden bij BI-startpunt als gebruiker van de groep die u zojuist hebt aangepast, Web Intelligence te starten en te verifiëren dat de interface overeenkomt met uw aanpassingsinstellingen.

18.6.1.2 Web Intelligence-inhoud uitlijnen

Kies de gewenste manier waarop documentinhoud moet worden uitgelijnd (links-naar-rechts of rechts-naar-links) als gebruikers Web Intelligence-documenten maken.

De uitlijning van inhoud in de Rich Client-interface is afhankelijk van de landinstellingen in de voorkeuren van het BI-startpunt:

- Inhoud wordt rechts-naar-links uitgelijnd als de opties Voorkeurslandinstellingen voor weergave en Landinstellingen product beide zijn ingesteld op talen die rechts-naar-links worden uitgelijnd.
- In alle andere gevallen wordt de inhoud links-naar rechts uitgelijnd.

> ⓘ Opmerking
>
> Zie de *Gebruikershandleiding voor Business Intelligence-startpunt* voor meer informatie over het instellen van voorkeurslandinstellingen.

> ⓘ Opmerking
>
> Uitlijning van inhoud geldt alleen op het moment dat een document wordt gemaakt en heeft geen gevolgen voor bestaande documenten.

18.6.1.3 Uitbreidingspunten Web Intelligence-gebruikersinterface inschakelen voor bepaalde gebruikersgroepen

U kunt in Web Intelligence bepaalde groepen gebruikers toegangsrechten geven voor aangepaste interface-uitbreidingen. Raadpleeg *SAP BusinessObjects BI Developer's Guide for Web Intelligence and the BI Semantic Layer* voor meer informatie over uitbreidingspakketten en de beschikbare API-oproepen van REST-webservices.

18.6.1.3.1 Uitbreidingspunten Web Intelligence-gebruikersinterface inschakelen

- U hebt de juiste uitbreiding in uw installatie gemaakt en geïmplementeerd. Implementeer een afzonderlijke uitbreiding voor elke uitbreidingsfunctie (bijvoorbeeld: Aangepaste knop of Opslaan als HTML).
- U hebt de uitbreiding toegevoegd aan de lijst met vertrouwde URL's. Raadpleeg de sectie Vertrouwde URL's toevoegen aan de lijst met geautoriseerde URL's [pagina 717] als u dit niet hebt gedaan.

1. Meld u als beheerder aan bij de CMC.
2. Selecteer in de lijst *Ordenen* de optie *Gebruikers en groepen*.
3. Selecteer een gebruikersgroep in de lijst *Groepshiërarchie*.
4. Klik in de lijst *Acties* op *Aanpassing*.
5. Klik op het tabblad *Uitbreidingen* en voer een van de volgende handelingen uit:

Optie	Beschrijving
Een OSGi-uitbreiding toevoegen die is geïmplementeerd op het BI-platform en de bijbehorende toepassingsserver.	Selecteer de aangepaste uitbreidingen die u door de gebruikers wilt laten gebruiken.

Een niet-OSGi-uitbreiding toevoegen die is geïmplementeerd op de toepassingsserver van het BI-platform of op een externe toepassingsserver	1. Klik op *Toevoegen*.
	2. Voer de URL van de uitbreiding in.
	Dit is de URL van het JSON-bestand.
	Opmerking
	Vervang alle spaties in de URL door `%20`.
	Voorbeelden:
	• Apache Tomcat-toepassingsserver:
	`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`
	• Externe toepassingsserver:
	`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`

Optie	Beschrijving
	3. Selecteer *Proxygegevens instellen* indien vereist door uw toepassingsserver en voer de servernaam en het poortnummer in. 4. Selecteer *Geen verificatie* of *Basisverificatie* indien vereist door uw toepassingsserver en voer de gebruikersnaam en het wachtwoord in. 5. Klik op *OK* en selecteer de uitbreiding. 6. Klik op *Opslaan*.
Uitbreidingsgegevens wijzigen.	Klik op *Wijzigen*.
Een uitbreiding uit de CMC verwijderen.	Klik op *Verwijderen*.

6. Klik op *Opslaan en sluiten*.

De ingeschakelde uitbreidingen zijn beschikbaar voor de geselecteerde gebruikersgroep wanneer een document wordt geopend dat zich in de geselecteerde map bevindt. De uitbreidingspunten zijn beschikbaar voor alle Web Intelligence-toepassingsclients: web, Java-applet en Rich Client.

18.6.2 BI-startpunt

18.6.2.1 Wissen van aanwijzingswaarden in het dialoogvenster Plannen inschakelen

Als u een Web Intelligence-document plant op basis van een BEx-query die SAP BW-aanwijzingen bevat, kunnen gebruikers van het BI-startpunt een aanwijzingswaarde wissen zodat deze wordt opgehaald door de SAP BW-gegevensbronvariabele wanneer het document wordt uitgevoerd of repareren voordat de planningstaak wordt uitgevoerd.

Met de procedure hieronder kunt u twee keuzerondjes in de gebruikersinterface weergeven:

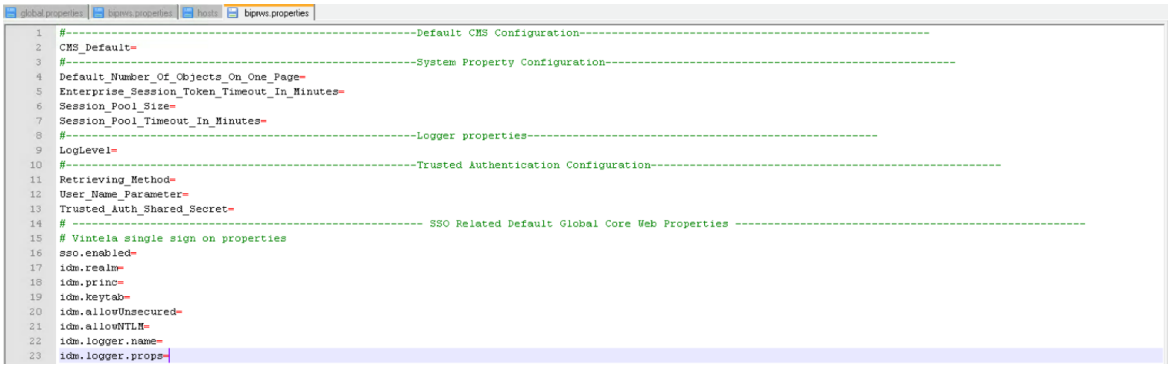
- *Dynamische waarde gebruiken*: Laat de SAP BW-gegevensbron de waarde verwerken.
- *Constante waarde gebruiken*: Voer een vaste waarde in.

1. Voer een van de volgende acties uit in de map `<InstallDir>\<WebAppServer>\webapps\BOE\WEB-INF\config\custom`:
   - Als een bestand `AnalyticalReporting.properties` in de map staat, opent u het bestand in een teksteditor.
   - Als er geen bestand `AnalyticalReporting.properties` in de map bestaat, maakt u een bestand met die naam en opent u het in een teksteditor.
2. Voer een van de volgende acties uit in het bestand `AnalyticalReporting.properties`:
   - Als het bestand al bestond, zoekt u de eigenschap `bex.dynamic_variable.schedule` in het bestand en zorgt u dat de waarde is ingesteld op `true`.
   - Als u het bestand `AnalyticalReporting.properties` hebt gemaakt, voegt u `bex.dynamic_variable.schedule=true` toe aan het einde van het bestand.
3. Sla het bestand op en sluit het af en start de webtoepassingsserver vervolgens opnieuw.

18.7 BI-platform RESTful-webservices configureren op webserver

Voer de onderstaande stappen uit om de configuratie voor RESTful-webservices aan te passen:

1. Kopieer het bestand: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\default\biprws.properties` naar `<INSTALLATIEMAP>>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` en open het om het te bewerken. Wijzig zo nodig de parameters.



Hieronder wordt een tabel weergegeven met een beschrijving van de eigenschappen die in de schermafbeelding staan.

Eigenschap	Beschrijving	Standaardwaarde

`CMS_Default`	De gebruiker kan de naam van het CMS en de het bijbehorende poortnummer opgeven, en eventueel ook de clusternaam.
	Voorbeeld:
	`CMS_HOST_NAME:CMS_PORT_NUMBER`
	Of
	`@CMS_CLUSTER_NAME`
		0

`Default_Number_Of_Objects_On _One_Page`	Het aantal items dat per pagina wordt weergegeven. U kunt deze instelling overschrijven met de parameter `&pageSize=<m>` in de SDK van RESTful-webservices.	50

Eigenschap	Beschrijving	Standaardwaarde
`Enterprise_Session_Token_Timeout_In_Minutes)`	De verlooptijd waarover een aanmeldingstoken geldig blijft. Hierna moet u een nieuw aanmeldingstoken genereren.	60
`Session_Pool_Size`	Het aantal sessies in cache dat op elk gewenst tijdstip kan worden opgeslagen. De sessiepool plaatst RESTful-webservicesessies in cache zodat deze opnieuw kunnen worden gebruikt wanneer een gebruiker een ander verzoek verzendt met hetzelfde aanmeldingstoken in de HTTP-aanvraagheader.	1000
`Session_Pool_Timeout_In_Minutes`	De tijd in minuten waarna sessies in cache verlopen.	2
`LogLevel`	Hiermee kunt u registratie inschakelen en het ernst- en detailniveau instellen op *Geen* (alleen essentiële gebeurtenissen worden geregistreerd), *Laag* (berichten voor opstarten, afsluiten, en aanvraag starten en beëindigen), *Gemiddeld* (fout-, waarschuwings- en de meeste statusberichten) of *Hoog* (Niets wordt uitgesloten. Wordt alleen voor debugging gebruikt. Het CPU-gebruik kan toenemen, wat van invloed kan zijn op de prestaties). De beschikbare menuopties zijn: • `Unspecified` • `None` • `Low` • `Medium` • `High`	Niet opgegeven

Eigenschap	Beschrijving	Standaardwaarde
Log_Location	De locatie van het logboekbestand waarin het gebruik wordt vastgelegd voor een computer waarop BI-platform wordt gehost. **Opmerking** • Er wordt een nieuwe map gemaakt als u het bestandspad opgeeft naar een map die niet bestaat. • De locatie van het logboekbestand wordt ingesteld op de standaardlocatie als de locatie niet is opgegeven in het bestand biprws.properties.	Niet opgegeven
`Retrieving_Method`	Het menu waarin is opgegeven welke querymethode wordt gebruikt om aanmeldingstokens voor vertrouwde verificatie op te halen wanneer u de RESTful-webservice API /logon/trusted gebruikt. • `HTTP_HEADER` wordt gebruikt voor GET-query's met de aanvraagkop accept=application/xml (of application/json). • `QUERY_STRING` wordt gebruikt om een aanmeldingsnaam toe te voegen aan het eind van een URL-query met de RESTful-webservice API, bijvoorbeeld /logon/trusted/?user=johndoe. • `COOKIE` wordt gebruikt wanneer de aanmeldingsnaam wordt opgehaald uit een browsercookie. Het domein, de naam, de waarde en het pad moeten in de cookie zijn opgeslagen.	`HTTP_HEADER`
`User_Name_Parameter`	Het label wordt gebruikt om de vertrouwde gebruiker te identificeren bij het ophalen van een aanmeldingstoken.	`X-SAP-TRUSTEDUSER`

Eigenschap	Beschrijving	Standaardwaarde
`Trusted_Auth_Shared_Secret`	De tekenreekswaarde wordt gegenereerd door de stappen te volgen die worden genoemd inEen waarde voor een gedeeld geheim genereren [pagina 404].	Niet opgegeven
`Basic_Auth_Supported`	Maakt basisverificatie op een Tomcat-webserver mogelijk. Mogelijke waarden zijn: `True` of `False`.	Niet opgegeven
`Basic_Auth_Type`	Stelt de verificatie in op `secEnterprise`, `secLDAP`, `secSAPR3` of `secWinAD` om basisverificatie te ondersteunen.	`secEnterprise`

2. Start Tomcat opnieuw.

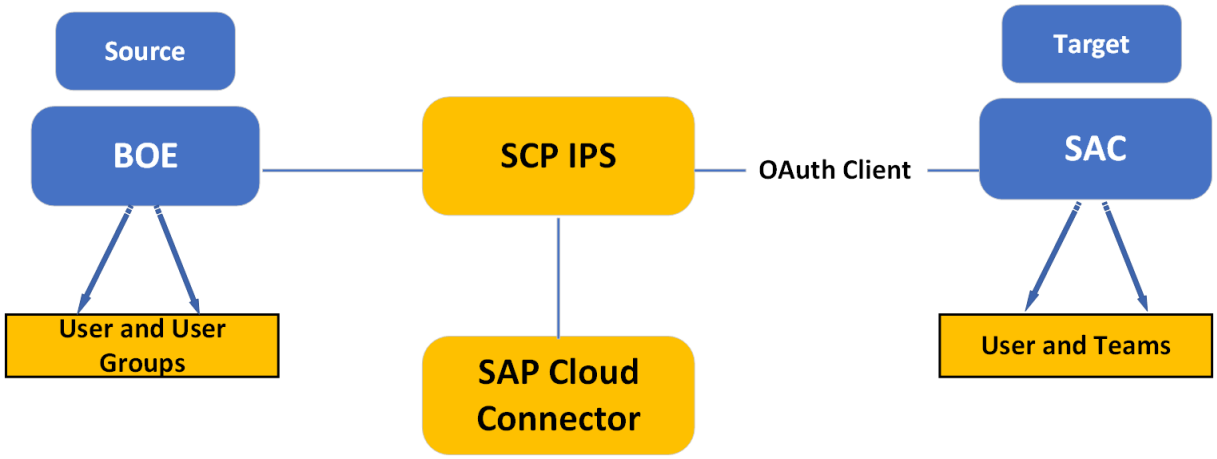
18.8 Hybride gebruikersbeheer

SAP richt zich op een strategie waarbij de cloud voorop staat. Ook klanten gaan steeds meer in de richting van hybride oplossingen waarbij ze assets tussen de On-Premises omgeving en de cloud beheren. Het is van het grootste belang dat wij services via SAP BusinessObjects BI-platform bieden die dit mogelijk maken.

Dit wordt bereikt door op System for Cross-Domain Identity Management (SCIM) gebaseerde API's voor gebruikerstoewijzing te gebruiken, die kunnen worden gebruikt door SAP Cloud Platform Identity Provisioning Service (SCP IPS) om Enterprise-gebruikers van BI-platform toe te wijzen aan elk ander ondersteund SCIM-systeem met behulp van Identity Provisioning Service (IPS) (in het bijzonder SAP Analytics Cloud).

Via SCP IPS en SAP BusinessObjects BI-platform 4.2 SP06 of hoger kunnen Enterprise-gebruikers van BI-platform nu worden toegewezen aan elk ondersteund SCIM-doelsysteem.

De volgende afbeelding beschrijft het hybride scenario beschreven en hoe services tussen On-Premises en de cloud kunnen worden ingeschakeld.



18.9 Uw On-Premises gebruikers toewijzen aan SAP Analytics Cloud

Om entiteiten (gebruikers, groepen, rollen) van het ene systeem aan het andere systeem in uw onderneming toe te wijzen, moet u deze systemen eerst als bron- en doelsystemen toewijzen in de gebruikersinterface van Identity Provisioning.

U kunt uw on-premises gebruikers (BOE) in enkele eenvoudige stappen via de SAP Cloud Platform Identity Provisioning Service (SCP IPS) aan SAP Analytics Cloud toewijzen.

1. Een verbinding tot stand brengen tussen het On-Premises-systeem en de cloud
2. OAuth-clientreferenties maken in SAP Analytics Cloud
3. Het bronsysteem configureren
4. Het doelsysteem configureren
5. Gebruikers en gebruikersgroepen toewijzen aan SAP Analytics Cloud
6. Toegewezen gebruikers en gebruikersgroepen weergeven

18.9.1 Een verbinding tot stand brengen tussen het On-Premises-systeem en de cloud

U kunt een verbinding tot stand brengen tussen het On-Premises-systeem en de cloud (Identity Provisioning System) met behulp van de SAP-cloudconnector (IPS-systeem).

De cloudconnector is geïnstalleerd.

1. Open de beheerpagina van de SAP-cloudconnector en meld u aan bij: `https://<HCC HOST>:8443`.

   > **Opmerking**
   >
   > Vervang `<HCC HOST>` door de hostnaam van het systeem waar de cloudconnector is geïnstalleerd.

2.
3. Selecteer *Connector* in het navigatievenster en klik op het pictogram + (*Subaccount toevoegen*).

   Het dialoogvenster *Subaccount toevoegen* wordt weergegeven.

4. Voer de volgende gegevens in voor uw IPS-account:

   > **Opmerking**
   >
   > Het hebben van de machtiging *On-Premise-verbindingen beheren* voor de gebruiker van het subaccount in IPS is verplicht. De *Regiohost* en *Naam subaccount* zijn te vinden in de sectie *Ondersteuning - Accountinformatie* in IPS.

   a. *Regiohost*: selecteer uw regio in de lijst.
   b. *Naam subaccount*: Voeg uw accountnaam toe. Bijvoorbeeld dd00bb33.
   c. (Optioneel) *Weergavenaam*: voeg een naam toe voor de account.
   d. *Gebruiker subaccount*: voeg de gebruikersnaam van uw subaccount (S-gebruiker) toe.

   e. *Wachtwoord*: voeg het wachtwoord van uw S-gebruiker toe.
   f. *Locatie-ID*: laat dit veld leeg als u de standaardlocatie wilt gebruiken.
   g. (Optioneel) *Beschrijving*: voeg een beschrijving toe voor de cloudconnector.
5. Klik op *Opslaan*.
6. Selecteer in het navigatievenster onder *Weergavenaam* de optie *Cloud naar On-Premises*.

   Weergavenaam is de naam van de tenant van de cloudconnector.
7. Klik onder het tabblad *Toegangscontrole* op het pictogram + (Toevoegen).

   Het dialoogvenster *Systeemtoewijzing bewerken* wordt geopend.
8. Voeg de gevraagde systeemtoewijzingsinformatie toe voor uw BI-platformsysteem, de webtoepassingsserver (bijv. Tomcat) waarop biprws wordt gehost:
   a. *Type back-end*: selecteer het andere SAP-systeem in de vervolgkeuzelijst.
   b. *Protocol*: selecteer HTTP in de vervolgkeuzelijst.
   c. (Optioneel) *Virtuele host*: De virtuele host en poort zijn standaard ingesteld op de interne host en poort. U kunt de naam van de host en poort wijzigen zodat de naam van de interne host en poort niet wordt weergegeven.
   d. (Optioneel) *Virtuele poort*: dit is het poortnummer dat door de virtuele host wordt gebruikt.
   e. *Interne host*: Dit is de hostnaam voor de WAS (bijv. Tomcat) die de Restful-webservice (biprws) host.
   f. *Interne poort*: dit is het poortnummer dat door de interne host wordt gebruikt. (Poort waar BIP RESTful-webservices zijn geïmplementeerd, bijvoorbeeld, biprws.)
   g. *SAProuter*: laat dit veld leeg.
   h. *Type principal*: selecteer de optie Geen in de vervolgkeuzelijst.
   i. *Naam SNC-partner*: laat dit veld leeg.
   j. (Optioneel) *Beschrijving*: voeg een beschrijving van het systeem toe.
9. Schakel het selectievakje *Interne host controleren* in en klik op *Opslaan*.
10. Selecteer het systeem dat u hebt toegevoegd aan de lijst *Virtueel toewijzen aan intern systeem*.
11. Klik in het gebied *Beschikbare resources* op het pictogram + (Toevoegen).

    Het dialoogvenster *Resource toevoegen* wordt weergegeven.
12. Voeg de volgende resourcegegevens toe voor uw account:
    a. *URL-pad*: /biprws/sbop/internal/v2/scim.
    b. *Ingeschakeld*: controleer of het selectievakje is ingeschakeld.
    c. *Toegangsbeleid*: selecteer het keuzerondje *Pad en alle subpaden*.
    d. (Optioneel) *Beschrijving*: voeg een beschrijving voor de resource toe.
13. Klik op *Opslaan*.

> **Opmerking**
>
> De status naast de virtuele host moet groen zijn.

18.10 OAuth-clientreferenties maken in SAP Analytics Cloud

Volg de onderstaande stappen om OAuth-clientreferenties te maken in SAP Analytics Cloud:

1. Meld u aan bij SAP Analytics Cloud.
2. Ga vanuit het hoofdmenu naar *Systeem > Beheer > Appintegratie*.
3. Klik op *Nieuwe OAuth-client*.
4. Geef de gewenste naam op.
5. Selecteer *API-toegang* als het *Doel*.
6. Selecteer *Gebruikerstoewijzing* onder Toegang.
7. Klik op *Toevoegen*.

   Selecteer in de lijst met *Geconfigureerde clients* de client die u zojuist hebt toegevoegd.

   > **Opmerking**
   >
   > Selecteer het pictogram (Bewerken) om de gegenereerde OAuthClient-ID en geheime sleutel (wachtwoord) te bekijken. U hebt deze referenties nodig als u het doelsysteem configureert.
   >
   > De OAuth-client-ID komt overeen met uw gebruikersnaam in de configuratiegegevens van het doelsysteem in SCP IPS en de geheime sleutel komt overeen met uw wachtwoord.

18.11 Het bronsysteem configureren

U moet gegevens van het bronsysteem definiëren waaruit u gebruikers en gebruikersgroepen wilt toewijzen in de SAP Cloud Platform Identity Provisioning Service (SCP IPS).

1. Meld u aan bij de SCP IPS.
2. Selecteer op de pagina Start de tegel *Bronsystemen*.
3. Klik op het pictogram + (Toevoegen) dat zich onder aan het linkervenster bevindt.
4. Selecteer in de keuzelijst met invoervak *Type* het type systeem dat u wilt gebruiken.
5. Voeg een naam toe voor het systeem. (Zorg ervoor dat dit niet een systeemnaam is die al wordt gebruikt.)
6. Voer een beschrijving in voor het systeem, zodat u het later gemakkelijk kunt herkennen in de lijst (optioneel).
7. Klik op *Opslaan*.

   Het nieuwe systeem wordt in het linkervenster weergegeven.

   Let op: als u het systeem op dit punt niet opslaat, worden de standaardtransformaties en -eigenschappen niet opgeslagen.
8. Klik nu op het pictogram (Bewerken) om de transformaties weer te geven en configuratie-eigenschappen toe te voegen.
9. Voeg de volgende informatie toe:
   a. *Verificatie*: BasicAuthentication.
   b. *Host*: <BOE-hostnaam en -poort>.
   c. *ips.delta.read*: Ingeschakeld.
   d. *ips.full.read.force.count*: 2.
   e. *ips.trace.failed.entity.content*: true.
   f. *Wachtwoord*: <BOE-beheerderswachtwoord>.

g. *Proxytype*: OnPremise.
h. *scim.group.filter*: <gebruikersgroep-id of CUID>.

   Bijvoorbeeld `scim.group.filter: groupId eq "4214"`.
i. *scim.user.filter*: <gebruiker-id of CUID>.

   Bijvoorbeeld `scim.filter.filter: userId in "8077"` or `scim.user.filter: userCuid in "AQ.rQ1V1FR9JmQoQa0xYfII"`.
j. *Type*: HTTP.
k. *URL*: http://hostnaam: port/biprws/sbop/internal/v2/scim.
l. *Gebruiker*: beheerder

> **Opmerking**
>
> - U kunt de gegevens van het On-Premises-systeem helemaal opnieuw invullen of een bestaand bestand met de configuratiegegevens importeren.
> - U kunt bepaalde beperkingen of voorwaarden rondom het bronsysteem definiëren via transformaties.
> - Wanneer u een verbindingsdoel selecteert, moet dit compatibel zijn met het relevante systeemtype. Het doel moet alle verbindingsinstellingen specificeren die vereist zijn voor uw identiteitstoewijzingsscenario.
> - De hostnaam/poort die zijn opgegeven in het URL-veld moeten overeenkomen met de virtuele hostnaam/poort die zijn opgegeven in de cloudconnector.

10. Als u het veld *Doelnaam* overslaat, kunt u het tabblad *Eigenschappen* openen om alle verbindings- en configuratie-eigenschappen in te voeren die vereist zijn voor uw toewijzingsscenario.
11. U kunt de standaardsysteemtransformatie wijzigen (indien nodig).
12. Sla de wijzigingen op.

> **Opmerking**
>
> Aan het eind van de Identity Provisioning-URL wordt een door streepjes gescheiden tekenreeks weergegeven. Dit is de automatisch gegenereerde unieke ID van het nieuwe systeem.

18.12 Het doelsysteem configureren

Zorg er voordat u begint voor dat u de OAuth-clientreferenties in SAP Analytics Cloud hebt gemaakt.

1. Klik op de startpagina op het tabblad *Doelsysteem*.
2. Voer op het tabblad *Details* de naam in van het SAP Analytics Cloud-systeem, de SAP Analytics Cloud-URL en de bronsystemen.

   > **Opmerking**
   >
   > De bronsystemen die al zijn geconfigureerd, worden hier standaard weergegeven.

3. Klik op het tabblad *Eigenschappen*.
4. Voeg de volgende informatie toe:

a. *Verificatie*: BasicAuthentication.
b. *csrf.token.path*: api/v1/scim/Users?count=1.
c. *ips.trace.failed.entity.content*: Waar.
d. *OAuth2TokenService-URL*: <OAuthClientTokenURL>.
e. *Wachtwoord*: <Geheim dat is geconfigureerd tijdens OAuthClient-configuratie>.
f. *ProxyType*: internet.
g. *scim.api.csrf.protection*: ingeschakeld.
h. *Type*: HTTP.
i. *URL*: Sap Analytics Cloud-URL.
j. *Gebruiker*: <OAuth Client ID>.

18.13 Gebruikers en gebruikersgroepen toewijzen aan SAP Analytics Cloud

Nadat u het bron- en doelsysteem hebt geconfigureerd met behulp van de SAP Cloud Platform Identity Provision Service, kunt u deze toewijzen via het tabblad *Taken* in het venster *Details bronsysteem*.

Voor gebruikers op het BI-platform dat wordt ingericht, moeten e-mailadressen zijn geconfigureerd.

1. Klik op de tegel *Bronsysteem*.
2. Klik op *Taken*.
3. Selecteer onder *Taken* voor het *Taaktype*: *Taak lezen* de actie *Nu uitvoeren*.

   > **Opmerking**
   >
   > Als u de gebruikers of gebruikersgroepen hebt gewijzigd in BOE, selecteert u *Taak opnieuw synchroniseren* om ervoor te zorgen dat de wijzigingen worden bijgewerkt in SAP Analytics Cloud.

4. Om de voortgang weer te geven, selecteert u *Taaklogboeken* in het linkervenster en bekijkt u de *Status* van de geactiveerde taken.
5. Als u de details van de taakuitvoering wilt bekijken, klikt u op de overeenkomstige rij.

   Het venster *Details taakuitvoering* wordt geopend met de status van de acties.

18.14 Toegewezen gebruikers weergeven in SAP Analytics Cloud

1. Ga naar het hoofdmenu > *Beveiliging* > *Teams*.
2. Ga naar de pagina *Teams*.
3. Selecteer uw BOE-gebruikersgroep.
4. Klik op *Teamleden* om de lijst met teamleden weer te geven die vanuit BOE aan SAP Analytics Cloud zijn toegewezen.

> **Opmerking**
>
> U kunt de lijst met gebruikers ook weergeven via het menu *Gebruikers* onder *Beveiliging*.

18.15 Voorbeeldsjablonen

U kunt de volgende sjablonen gebruiken om een gebruiker of een gebruikersgroep toe te wijzen.

Voorbeeld van bronsysteemconfiguratie

```
{ "connectorTypeString": "SCIM", "accessMode": "READ",
"alias": "SBOP_10.47.228.194",
"relatedSystems": [
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SBOP_43",
"state": "ENABLED",
"transformation": {
"user": {
"condition": "($.memberOf contains '7741') || ($.memberOf contains '7962') ||
($.id contains '8077') || ($.id contains '8081')",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
},
"group": {
"condition": "$.id contains '7741' || $.id contains '7962'",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
```

```
{
"targetPath": "$.meta",
"type": "remove"
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "Administrator",
"ips.full.read.force.count": "2",
"Authentication": "BasicAuthentication",
"host": "adept6991435:6400",
"scim.group.filter": "groupId eq \"7741,7962\" or groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\"",
"ProxyType": "OnPremise",
"ips.delta.read": "enabled",
"ips.trace.failed.entity.content": "true",
"URL": "http://adept6991435:6405/biprws/sbop/internal/v2/scim",
"Password": "Password1",
"scim.user.filter": "groupId eq \"7741\" and groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\" and userId in \"8077\" or
userCuid in \"AQ.rQ1V1FR9JmQoQa0xYfII\""
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```


Voorbeeldtransformatie


```
{
"connectorTypeString": "SAP_ANALYTICS_CLOUD",
"accessMode": "WRITE",
"destinationName": " ",
"alias": "https://idcsac.jp1.sapanalytics.cloud",
"relatedSystems": [
"SBOP_43"
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SAC-Machine",
"state": "ENABLED",
"transformation": {
"user": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"sourceVariable": "entityIdTargetSystem",
"targetPath": "$.id"
},
{
"sourcePath": "$.userName",
"targetPath": "$.userName"
},
{
"sourcePath": "$.name",
"targetPath": "$.name"
```

```
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.active",
"optional": true,
"targetPath": "$.active"
},
{
"sourcePath": "$.emails",
"preserveArrayWithSingleElement": true,
"targetPath": "$.emails"
},
{
"condition": "$.emails[0].length() > 0",
"constant": true,
"targetPath": "$.emails[0].primary"
},
{
"constant": [
"PROFILE:sap.epm:BI_Admin"
],
"preserveArrayWithSingleElement": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.groups",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.groups"
},
{
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
"optional": true,
"targetPath": "$['urn:scim:schemas:extension:enterprise:1.0']['manager']
['managerId']",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
},
"group": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"condition": "$.displayName EMPTY false",
"sourcePath": "$.displayName",
"targetPath": "$.id"
},
{
"condition": "$.id EMPTY false",
"sourcePath": "$.id",
"targetPath": "$.id"
},
{
"sourcePath": "$.displayName",
```

```
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.roles",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.members[*].value",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.members[?(@.value)]",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
}
}
},
"properties": {
"Type": "HTTP",
"User": "<exampleusername>",
"Authentication": "BasicAuthentication",
"OAuth2TokenServiceURL": "https://oauthasservices-
gf097393f.jp1.hana.ondemand.com/oauth2/api/v1/token",
"csrf.token.path": "/api/v1/scim/Users?count=1",
"ProxyType": "Internet",
"ips.trace.failed.entity.content": "true",
"URL": "https://idcsac.jp1.sapanalytics.cloud",
"scim.api.csrf.protection": "enabled",
"Password": "<examplepassword>"
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

19 Verbindingen en universes beheren

19.1 Verbindingen beheren

Een verbinding is een benoemde set parameters waarmee u definieert hoe een of meer SAP BusinessObjects-toepassingen toegang krijgen tot relationele of OLAP-databases. Verbindingsgegevens zoals servernaam, database, gebruikersnaam en wachtwoord kunnen veilig worden opgeslagen in de gegevensopslagruimte voor het BI-platform in de map Verbindingen.

Ontwerpers definiëren universes op basis van verbindingen. Gebruikers van query-, analyse- en rapportagetoepassingen hebben toegang tot de database via de universe, zonder op de hoogte te zijn van onderliggende gegevensstructuren in de database.

U kunt met de volgende toepassingen verbindingen maken:

- Het hulpprogramma voor universe-ontwerp: verbindingen worden opgeslagen in de gegevensopslagruimte.
- Het hulpprogramma voor informatie-ontwerp. verbindingen kunnen lokaal worden gemaakt en vervolgens worden gepubliceerd naar de gegevensopslagruimte, of rechtstreeks worden gemaakt en bewerkt in de gegevensopslagruimte.

> ⓘ Opmerking
>
> Zie de *SAP BusinessObjects Analysis, edition for OLAP Administrator Guide* voor meer informatie hoe u de OLAP-gegevensbronverbindingen beheert.

U geeft gebruikers rechten om verbindingen te maken, bewerken en verwijderen.

U geeft gebruikers toegangsrechten tot universe-verbindingen, zodat ze documenten kunnen maken en weergeven waarin universes en verbindingen worden gebruikt.

Verwante informatie

Beveiligingsinstellingen voor objecten beheren in de CMC [pagina 132]
Verbindingsrechten [pagina 1146]

19.1.1 Een universe-verbinding verwijderen

> → Tip
>
> U kunt verbindingen ook verwijderen via het hulpprogramma voor universe-ontwerp en het hulpprogramma voor informatie-ontwerp.

1. Selecteer een universeverbinding in de lijst in het gebied *Verbindingen*.
2. Klik op *Beheren* > *Verwijderen*.

19.2 Universes beheren

Een universe is een geordende verzameling van metagegevensobjecten waarmee zakelijke gebruikers bedrijfsgegevens kunnen analyseren en hierover kunnen rapporteren in niet-technische taal. Deze objecten omvatten dimensies, meetwaarden, hiërarchieën, attributen, vooraf gedefinieerde berekeningen, functies en query's. De objectlaag van de metagegevens is gebaseerd op een relationeel databaseschema of een OLAP-kubus, zodat de objecten rechtstreeks worden toegewezen aan de databasestructuren. Een universe bevat verbindingen met de gegevensbronnen zodat gebruikers van hulpprogramma's voor query en analyse verbinding kunnen maken met een universe en query's kunnen uitvoeren en rapporten maken met de objecten in een universe, zonder op de hoogte te zijn van de onderliggende gegevensstructuren in de database.

U kunt met de volgende hulpprogramma's universes maken:

- Het hulpprogramma voor universe-ontwerp. Universes die met dit hulpprogramma worden gemaakt, kunnen worden onderscheiden door de extensie .unv en worden daarom .unv-universes genoemd. De .unv-universes worden gedefinieerd op een beveiligde verbinding en opgeslagen in de map Gegevensopslagruimte voor universes.
- Het hulpprogramma voor informatie-ontwerp. Universes die met dit hulpprogramma worden gemaakt, zijn gebaseerd op de nieuwe semantische laag. Ze worden onderscheiden door de extensie .unx en worden daarom .unx-universes genoemd. De .unx-universes worden lokaal geschreven en gepubliceerd naar de map Gegevensopslagruimte voor universes. Ontwerpers kunnen beveiliging op objectniveau definiëren met de beveiligingseditor van het hulpprogramma voor informatie-ontwerp.

U geeft gebruikers rechten tot toepassingen en universes zodat ze universes kunnen maken, bewerken en verwijderen, en beveiliging voor universes kunnen ontwerpen.

U geeft gebruikers rechten tot universes zodat ze documenten die universes gebruiken, kunnen maken en weergeven.

Verwante informatie

Beveiligingsinstellingen voor objecten beheren in de CMC [pagina 132]
Hulpprogramma voor universeontwerp [pagina 1152]
Universe-rechten (.unv) [pagina 1142]
Hulpprogramma voor informatieontwerp [pagina 1153]
Universe-rechten (.unx) [pagina 1144]

19.2.1 Universes verwijderen

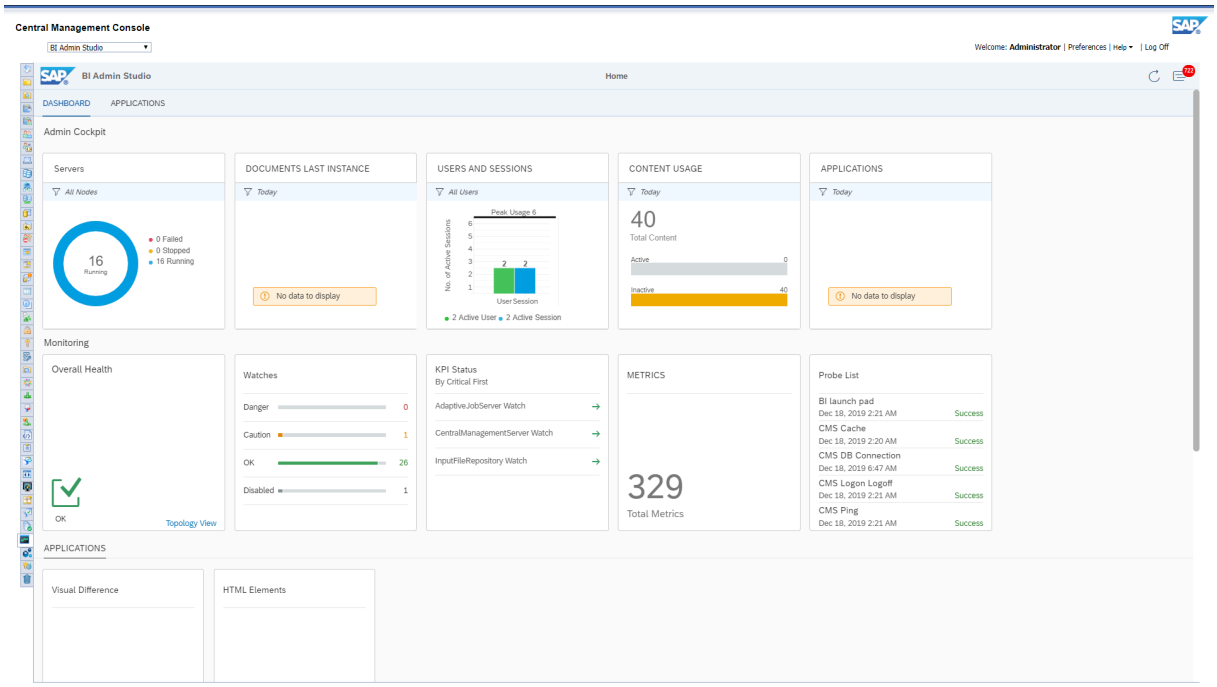
> → Tip
>
> U kunt verbindingen ook verwijderen via het hulpprogramma voor informatie-ontwerp.

1. Selecteer een universe in de lijst in het beheergebied *Universes* van de CMC.
2. Klik op *Beheren* > *Verwijderen*.
3. Klik op *OK* om het verwijderen te bevestigen.

20 BI-beheerderstudio

BI-beheerdersstudio is een toepassing in CMC die Toezicht, Meldingen en de Beheercockpit combineert, en voorheen bekend stond als Cockpit BI-beheerder.

De toepassing bestaat uit twee tabbladen, *Dashboard* en *Toepassingen*.



Dashboard

Het tabblad *Dashboard* biedt een enkele weergave van de dashboards die beschikbaar zijn in *Beheercockpit* en *Toezicht*. U kunt op elk dashboard klikken om gedetailleerde informatie over het dashboard weer te geven. U kunt bijvoorbeeld het dashboard *Servers* selecteren om de lijst met servers op te halen waarvan de *Status* is ingesteld op *Actief*, *Gestopt* en *Mislukt*, naast details als *Servernaam*, *PID* en *Type*. Zie Beheercockpit [pagina 800] voor meer informatie over Beheercockpit en zie Toezicht [pagina 804] voor meer informatie over Toezicht.

Toepassingen

Vanaf het tabblad *Toepassingen* hebt u toegang tot *Visueel verschil* en *Gemachtigde HTML-elementen*. Zie Visueel verschil [pagina 828] voor meer informatie over *Visueel verschil* en zie HTML-elementen autoriseren [pagina 831] voor meer informatie over *HTML-elementen*.

Meldingen

U kunt selecteren voor toegang tot het meldingsvenster. Vanuit het meldingsvenster kunt u de optie *Naar meldingspagina* selecteren voor meer informatie over de meldingen die u hebt gemaakt.

20.1 Beheercockpit

De Beheercockpit is een nieuwe toepassing die is toegevoegd in de CMC. Hiermee kan een beheerder basisgegevens verzamelen over de BI-omgeving. Het betekent Business Intelligence afleiden uit de gegevens in uw Business Intelligence-omgeving. Met de Beheercockpit kunt u informatie verkrijgen over servers, geplande taken, gebruikers en sessies, inhoudsgebruik en toepassingen.

> **Opmerking**
>
> Aan de volgende vereisten moet zijn voldaan om de Beheercockpit te kunnen gebruiken:
>
> - Bewakingsservice moet zijn ingeschakeld.
> - Audit en relevante gebeurtenis moeten zijn ingeschakeld zodat de juiste gegevens worden opgehaald.
> - BI-platform RESTful Web Service moet toegankelijk zijn voor clients.
> - WACS moet actief zijn, tenzij RESTful-webservice wordt geïmplementeerd op Tomcat.
> - Als u SSL configureert voor CMC, moet u ook SSL voor WACS configureren, tenzij de RESTful-webservice is geïmplementeerd in Tomcat.
> - Toegang tot cross domain moet zijn ingeschakeld.
> - Gebruikers moeten deel uitmaken van de beheerdersgroep of van een subgroep om toegang te hebben tot de Beheercockpit.

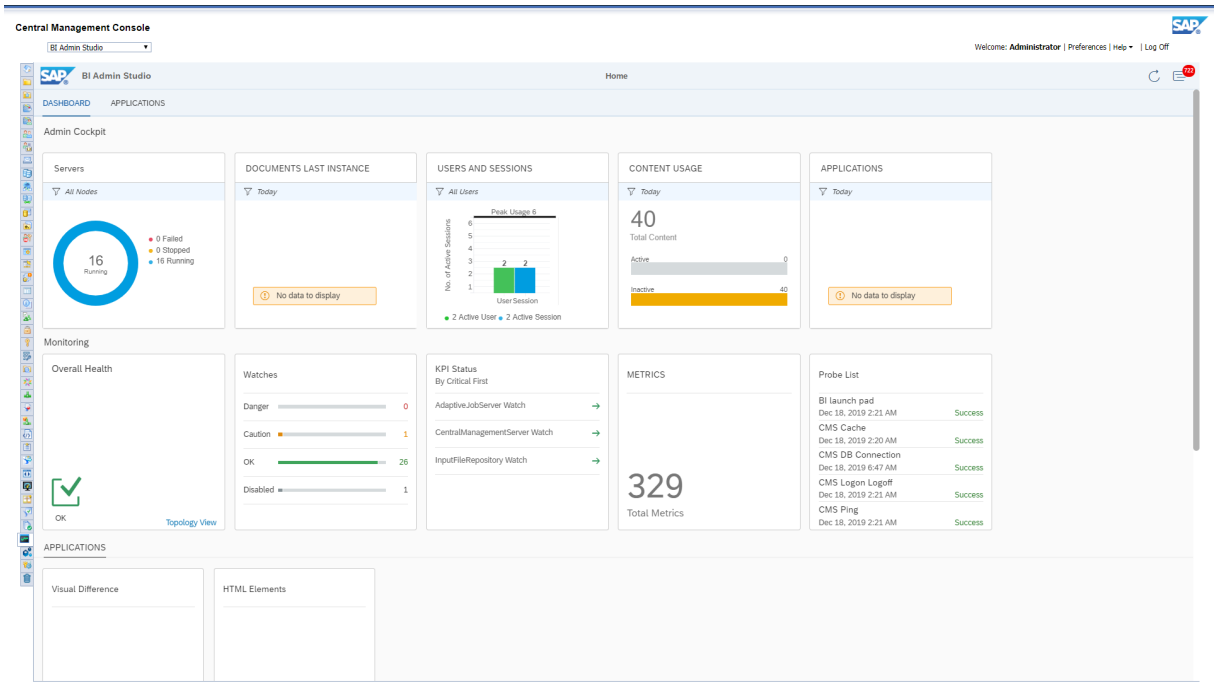
20.1.1 Beheercockpit

De Beheercockpit geeft u een uitgebreide analyse van gegevens die zijn gerelateerd aan de volgende componenten in een beeldvisualisatie:

- Servers
- Laatste documentexemplaar

- Gebruikers en sessies
- Inhoudsgebruik
- Toepassing

> **Opmerking**
>
> Audit database moet ingeschakeld zijn om de analyse van *inhoudsgebruik* en *toepassing* te kunnen weergeven.



U kunt de gegevens die op elke pagina binnen de Beheercockpit worden weergegeven vernieuwen door in de rechterbovenhoek van de startpagina op te klikken.

20.1.2 BI voor servers

Met de Beheercockpit kunt u real-timegegevens over de status en gerelateerde details van alle servers in uw BI-omgeving verkrijgen.

De startpagina biedt u de volgende details:

- Totaalaantal servers
- Aantal servers met fouten
- Aantal gestopte servers

U kunt gegevens op de tegel *Servers* filteren door het gewenste servercluster te selecteren.

Door te klikken op de tegel *Servers*, wordt u doorgestuurd naar de pagina Servers met de details van het totaalaantal servers, de servers die fouten opleveren en de gestopte servers. De pagina Servers geeft u ook de *status*, de *servernaam*, de *PID* (proces-id), het *type*, de *status* en de *tijd laatste bewerking* voor elke server die fouten oplevert.

Op de pagina *Servers* kunt u gegevens overeenkomstig specifieke serverclusters filteren door het gewenste servercluster te selecteren.

In de bijbehorende rij vindt u meer informatie over de fouten opleverende server. Hierdoor wordt u doorgestuurd naar een nieuwe pagina met gegevens over de reden van de fout. U kunt de fouten opleverende server opnieuw starten vanaf deze pagina door *START* te selecteren.

20.1.3 BI in documentexemplaren

U kunt de Beheercockpit gebruiken om gegevens over de status en gerelateerde details voor alle exemplaren van geplande documenten in uw BI-omgeving op te halen.

Op de introductiepagina vindt u de volgende informatie:

- Het totale aantal laatste exemplaren van elk gepland document.
- Het aantal laatste actieve exemplaren van elk gepland document.
- Het aantal laatste fouten opleverende exemplaren van elk gepland document.
- Het aantal laatste in behandeling zijnde exemplaren van elk gepland document.

In de tegel *Laatste documentexemplaar* kunt u gegevens filteren voor een bepaalde periode door de gewenste periode te selecteren uit het vervolgkeuzemenu. De beschikbare tijdsbereiken zijn:

- Vandaag
- Laatste 7 dagen
- Laatste 30 dagen
- Kwartaal
- Jaar

Als u op de tegel *Laatste documentexemplaar* klikt, wordt u naar de pagina Laatste exemplaren geleid waarop de details van het totale aantal laatste exemplaren van elk gepland document staan, uitgesplitst naar status: Actief, Met fouten en In behandeling. Het tabblad *Statistieken* bevat details die u kunt weergeven in de secties *Documenten met meeste exemplaren* en *Exemplaren met langste runtime*. De pagina Documentexemplaren geeft u ook de *exemplaarnaam*, *status*, het *type*, de *eigenaar* en de *eindtijd* voor elke foutstatus.

U kunt de gegevens die te zien zijn op de pagina *Laatste exemplaren* exporteren als .CSV-bestand door op de knop Link exporteren te klikken. U kunt geselecteerde exemplaren ook exporteren door het bijbehorende aankruisvakje te selecteren en vervolgens *Geselecteerde exporteren* uit de vervolgkeuzelijst Exporteren.

In de bijbehorende rij vindt u meer informatie over een fouten opleverend exemplaar. U kunt de taak opnieuw starten vanuit de pagina door *UITVOEREN* te selecteren.

Op het tabblad Statistiek is een nieuw diagramfilter ingeschakeld waarmee u de top 5, top 10, top 15 en top 20 van de documenten kunt filteren en weergeven.

20.1.4 BI voor gebruikers en sessies

Met de Beheercockpit kunt u gegevens over gebruikers en sessies in uw BI-omgeving verkrijgen.

De startpagina geeft u bijvoorbeeld de volgende details:

- Aantal actieve gebruikers
- Aantal actieve sessies

Op de tegel *Gebruikers en sessies* kunt u gegevens flteren voor:

- Alle gebruikers
- Gebruikers met naam
- Gelijktijdige gebruikers

Als u op de tegel *Gebruikers en sessies* klikt, wordt u doorgestuurd naar de pagina 'Gebruikers en sessies' met de gegevens van alle gebruikers, topgebruikers en statistieken. Het tabblad Statistiek bevat details over de meest actieve en de meest inactieve gebruikers.

Op de pagina 'Gebruikers en sessies' vindt u ook de *Gebruikersnaam*, het *Totaal aantal sessies*, de *Laatste tijd van aanmelding*, en de *Sessie met de langste uitvoeringstijd*.

U kunt meer details over een bepaalde gebruiker bekijken door de overeenkomstige regel te selecteren. Hierdoor wordt u doorgestuurd naar een nieuwe pagina met gegevens over de topsessies van die bepaalde gebruiker. U kunt elke sessie van die bepaalde gebruiker vanaf deze pagina beëindigen door de gewenste sessie te selecteren en *Sessie beëindigen* te kiezen.

20.1.5 BI voor inhoudsgebruik

Met de Beheercockpit kunt u gegevens over inhoudsgebruik in uw BI-omgeving verkrijgen.

De startpagina geeft u bijvoorbeeld de volgende details:

- Aantal actieve documenten
- Aantal inactieve documenten

Op de tegel *Inhoudsgebruik* kunt u gegevens filteren voor een specifiek tijdsbereik door het gewenste tijdsbereik te selecteren in het vervolgkeuzemenu.

> ⓘ Opmerking
>
> Als u actieve inhoud hebt verwijderd en gegevens filtert voor een bepaalde periode, staat het verwijderde item nog steeds onder actieve inhoud vermeld als het gedurende de geselecteerde periode actief was.

De beschikbare tijdsbereiken zijn:

- Vandaag
- Laatste 7 dagen
- Laatste 30 dagen
- Kwartaal
- Jaar

Door te klikken op de tegel *Inhoudsgebruik* wordt u doorgestuurd naar een pagina Inhoudsgebruik met de details over de actieve inhoud, inactieve inhoud en statistiek. Het tabblad Statistiek bevat details met betrekking tot Postakken IN met de meeste inactieve inhoud, universes met de meeste inhoud en mappen met de meeste inhoud.

U kunt de gegevens op de pagina *Inhoudsgebruik* naar een CSV-bestand exporteren door de knop 'Koppeling exporteren' te selecteren. U kunt ook geselecteerde taken exporteren door het overeenkomstige selectievakje in te schakelen en *Selectie exporteren* te selecteren in de vervolgkeuzelijst voor export.

Op de pagina Inhoudsgebruik vindt u ook *Inhoudsnaam*, *Type* en *Uitvoeringstijd*.

Op het tabblad Statistiek is een nieuw diagramfilter ingeschakeld waarmee u de top 5, top 10, top 15 en top 20 van de documenten kunt filteren en weergeven.

20.1.6 BI op toepassingen

De Beheercockpit biedt u gegevens over het aantal toepassingen in uw BI-omgeving, gesorteerd op toepassingsnaam.

Op de tegel *Toepassing* kunt u gegevens filteren voor een specifiek tijdsbereik door het gewenste tijdsbereik te selecteren in het vervolgkeuzemenu. De beschikbare tijdsbereiken zijn:

- Vandaag
- Laatste 7 dagen
- Laatste 30 dagen
- Kwartaal
- Jaar

Door te klikken op de tegel *Toepassingen* wordt u doorgestuurd naar een toepassingspagina met de details met betrekking tot *alle toepassingen* en *toptoepassingen*.

Het tabblad *Toptoepassingen* geeft de 5 toepassingen weer met het hoogste aantal documenten binnen het geselecteerde tijdsbereik. De toepassingspagina geeft u ook de *toepassingsnaam*, het *aantal gebruikers* en *aantal onderdelen*.

20.2 Toezicht

Met de Toezichtfunctie kunt u historische en runtime-gegevens van BI-platformservers vastleggen voor rapportage en berichtgeving. Hiermee kunnen systeembeheerders bepalen of een toepassing normaal werkt en of de verwachte reactietijden worden gehaald. De Toezichtfunctie levert belangrijke bedrijfsgegevens en kan daardoor beter inzicht bieden in het BI-platform.

Met de Toezichtfunctie kunt u de volgende taken uitvoeren:

- De prestatie van elke server controleren: Dit is mogelijk met behulp van controles die de status van elke server weergeven als verkeerslicht. De systeembeheerder kan drempelwaarden voor deze controles instellen en meldingen ontvangen wanneer deze drempelwaarden worden overschreden, en actie ondernemen als er sprake is van een fout of uitval.

- Kritieke systeem-KPI's (Key Performance Indicators) weergeven: Dit helpt bij toezicht op activiteiten en resources. Deze KPI's worden op de dashboardpagina of in de Toezichtfuntie weergegeven.
- De volledige implementatie van het BI-platform (in grafische en tabelindeling) op basis van servergroepen, servicecategorieën en Enterprise-knooppunten bekijken.
- Bekijk recente fouten op het dashboardscherm.
- Systeembeschikbaarheid en antwoordtijd controleren: u kunt tests gebruiken om werkstromen te simuleren en te controleren of de servers en services in de BI-platformimplementatie naar verwachting functioneren. Wanneer u de tijd voor retour van deze tests regelmatig controleert, kan de systeembeheerder het patroon van systeemgebruik beoordelen.
- De piekbelasting en piekperiode voor de CMS analyseren: hiermee kan de systeembeheerder bepalen of er meer licenties of systeemresources nodig zijn.
- Integratie met andere bedrijfstoepassingen: de Toezichtfunctie van het BI-platform kan worden geïntegreerd met andere bedrijfstoepassingen, zoals SAP Solution Manager en IBM Tivoli Monitoring.
- Volg de gegevenswaarde *Controleniveau* onder *Central Management Server* wanneer *Gebeurtenissen instellen* is ingesteld op *Uit* (gegevenswaarde 1). Hier kan een controlelijst worden gemaakt en wanneer de gegevenswaarde 1 is, wordt een testmelding verzonden in de controlelijst, samen met een e-mailmelding.

Zie voor meer informatie over het gebruik van de toezichtfunctie, inclusief details van tests en controles: *Online Help voor SAP BusinessObjects Business Intelligence-platform CMC*.

Verwante informatie

Informatie over de bijlage Servergegevens [pagina 1193]

20.2.1 Termen met betrekking tot toezicht

De volgende lijst bevat termen die betrekking hebben op de toezichtfunctie:

Trend

De historische gegevens vastleggen of weergeven om trends te vinden.

Dashboard

De Dashboard-pagina biedt een gecentraliseerde weergave voor de systeembeheerder bij prestatietoezicht op alle servers. Hier vindt u realtime-informatie over de KPI's van het systeem, recente meldingen, controles en relevante grafieken gebaseerd op de controlestatussen.

Controle

Controles bieden de realtime-status en historische trends van servers en werkstromen binnen de BI-platformomgeving. Gebruikers kunnen drempels en meldingen aan controles koppelen. U kunt een controle maken met gebruik van gegevens van tests, servers, SAPOSCOL of afgeleide gegevens.

Afgeleid gegeven

Afgeleide gegevens zijn gegevens die u maakt door twee of meer bestaande gegevens te combineren in een wiskundige vergelijking. U kunt een gegeven maken op basis van de gebruikersvereisten, en vervolgens een controle maken met dit gegeven.

Topologisch gegeven

Topologische gegevens bieden de nettostatus voor elke servicecategorie in het BI-platform. De Crystal Reports-service biedt bijvoorbeeld informatie over de gecombineerde status van alle controles die aan Crystal Reports-servers zijn gerelateerd.

Status

Dit zijn de statuswaarden:

- "0" - "GEVAAR"
- "1" - "ORANJE"
- "2" - "GROEN"

KPI

KPI's (Key Performance Indicators) zijn standaardgegevens in het BI-platform. Ze verstrekken informatie over planningen en aanmeldingssessies. Zo geeft een hoger aantal *RunningJobs* aan dat de servers goed presteren. Een hoger aantal *PendingJobs* duidt daarentegen op slechte prestaties en een hoge systeembelasting.

Test

Met tests kunt u toezicht houden op verschillende services en de verschillende functies van de BI-platformonderdelen simuleren. Wanneer tests worden ingepland voor uitvoer op opgegeven intervallen, kan de systeembeheerder de beschikbaarheid en prestaties van sleutelservices die door het BI-platform geboden worden, in de gaten houden. Deze gegevens kunnen ook gebruikt worden voor capaciteitsplanning.

Verkeerslicht

Een verkeerslicht is een pictogram dat de kleur Groen, Oranje of Rood weergeeft om de status van een test op elk moment aan te geven. Gebruikers kunnen twee of drie statussen instellen voor een controle.

Trending-grafiek

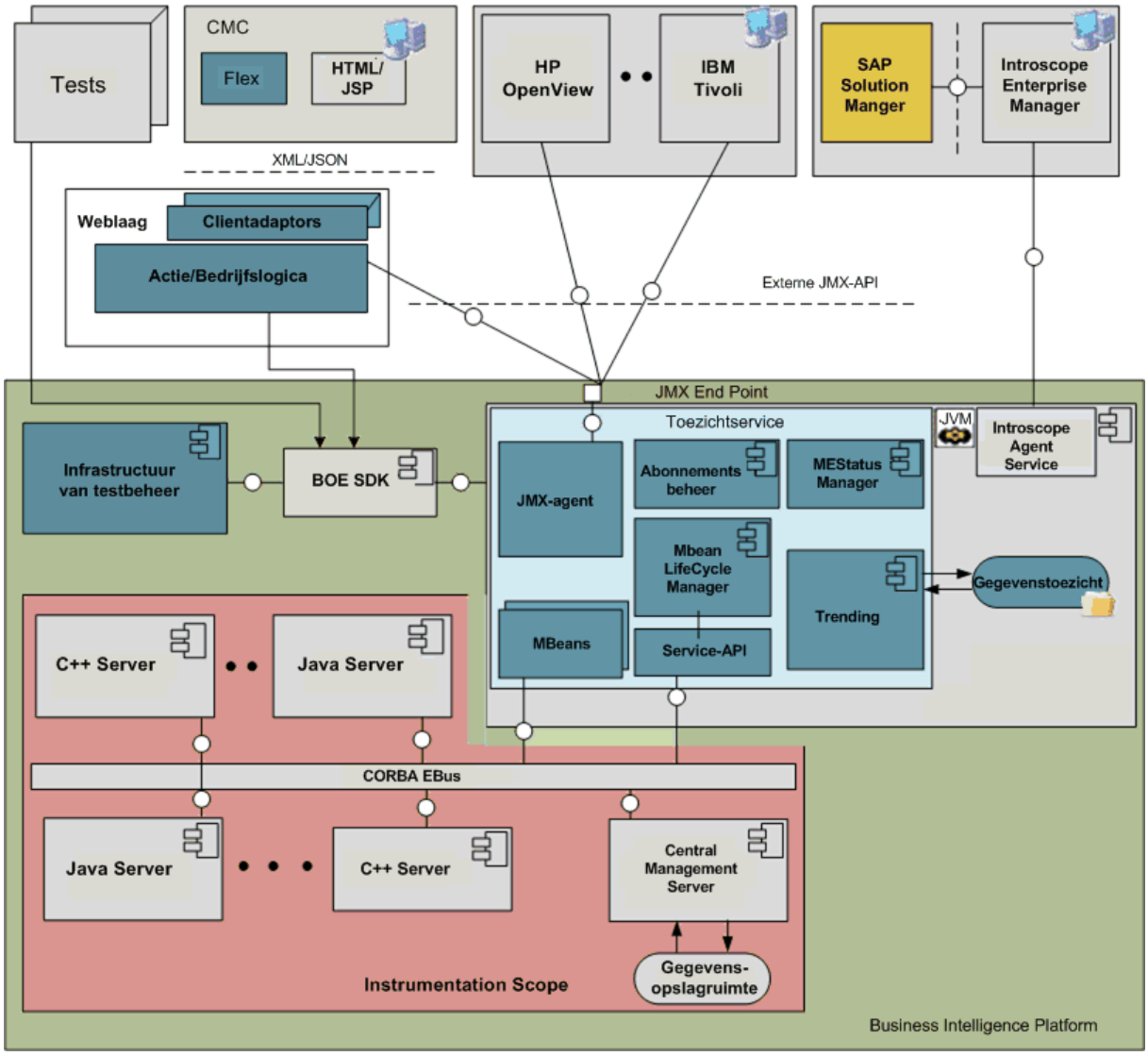
Een trending-grafiek is een grafische representatie van historische gegevens die gegenereerd zijn door tests en servers. Hiermee kan de systeembeheerder op verschillende tijden toezicht houden op het systeem en het patroon van het systeemgebruik beoordelen.

Melding

Een melding is een bericht dat gegenereerd wordt door de toezichtfunctie bij overschrijding van een gebruikergedefinieerde drempelwaarde die is ingesteld voor verschillende gegevens die op een controle zijn toegepast. U kunt ervoor kiezen meldingen per e-mail of op de pagina *Dashboard* te ontvangen.

20.2.1.1 Architectuur

Deze sectie biedt een belangrijk overzicht van de toezichtarchitectuur en een korte uitleg over de functie van de onderdelen. De toezichtarchitectuur wordt hieronder grafisch weergegeven:



De belangrijke onderdelen in de architectuur worden hieronder vermeld:

- De APS (Adaptive Processing Server)
- De agent/server van de Java Management Extensions (JMX)
- MBeans
- JMX-clients
- De beheerconsoles
- Trending-database

De toezichtservice wordt gehost op de Adaptive Processing Server. De toepassing is gebaseerd op JMX-technologie.

De toezichtservice levert de kernservices die beschikbaar zijn in de toezichtfunctie. De toezichtservice levert de volgende services:

- Levert de JMX-agentservice.
- Maakt MBeans dynamisch voor de SAP BusinessObjects-servers.

- Biedt levensduurbeheer voor de MBeans.
- Biedt een mechanisme waarmee nieuwe tests kunnen worden geregistreerd.
- Biedt gebruikers de mogelijkheid om complexe drempelvoorwaarden te maken met de gegevens van de servers.
- Biedt een mechanisme voor drempelberichtgeving en verzendt meldingen.
- Slaat historische gegevens op.

De Planningsservice van test die op de Adaptive Job Server wordt gehost, beheert het uitvoeren en plannen van tests. Er moet daarom een Adaptive Job Server actief zijn om de tests uit te kunnen voeren.

De toezichtfunctie toont tevens een eindpunt van een JMX of een RMI (Remote Method Invocation)-URL. Andere bedrijfstoepassingen zoals IBM Tivoli Monitoring kunnen een verbinding maken met de toezichtfunctie en toegang verkrijgen tot de BI-platformgegevens via een JMX Remote API. De toezichtfunctie gebruikt de Controlegegevensopslagdatabase voor het opslaan van historische gegevens bestemd voor trending. Zie Schema van trending-database [pagina 1229] voor meer informatie over het trending-databaseschema.

20.2.2 Databaseondersteuning configureren voor de Toezichtfunctie

In deze sectie wordt beschreven hoe u de toezichtfunctie instelt en rapporten opstelt op basis van toezichtgegevens.

> **Opmerking**
>
> Alleen controles waarvoor de instelling *Naar trending-database schrijven* is geselecteerd, schrijven toezichtgegevens naar de trending-database.

Er zijn twee databaseopties voor het registreren van toezichtgegevens: registreer informatie in de Auditing Data Store (ADS), of in een andere database die door het platform wordt ondersteund met het JDBC-stuurprogramma.

> **Opmerking**
>
> De Apache Derby-database is uit gebruik genomen in de BI 4.3-release. Raadpleeg 2912759 voor meer informatie over migreren en back-ups maken van gegevens.

U kunt de standaard Auditing Data Store (ADS) gebruiken, die ook wel de controledatabase wordt genoemd. Dit is de relationele database waarin de CMS controlegegevens opslaat. U kunt de ADS gebruiken die bij het BI-platform wordt geleverd, of een andere ondersteunde database die u als uw controledatabase hebt geconfigureerd.

Andere ondersteunde databases zijn:

- DB2
- SQL Server
- My SQL
- Oracle
- SAP HANA-database

- SQL Anywhere
- Sybase

Als u de controledatabase gebruikt, kunnen gebruikers rapporten maken op basis van de controlegegevens en de toezichtgegevens. Wanneer u de gegevens in een relationele database vastlegt, beschikt u over functionaliteit voor back-up en herstel en zijn de gegevens real time beschikbaar.

Verwante informatie

Configuratie voor gebruik van de controledatabase [pagina 810]

20.2.2.1 Configuratie voor gebruik van de controledatabase

Als u de controledatabase wilt gebruiken voor uw toezichtgegevens, moet u extra stappen voor de configuratie uitvoeren:

- In versies voor BI 4.3 was het zo, dat als u gegevens in uw Derby-trending-database had, u de Derby-database moest migreren naar de controledatabase en vervolgens het BI-platform moest configureren om toezichtgegevens vast te leggen in de controledatabase. Dit zijn de stappen op hoog niveau die u moet uitvoeren. Zie de verwante onderwerpen voor meer informatie.
  1. Migreer de Derby-database.
  2. Configureer de SBO-bestanden en voeg aliasnamen toe.
  3. Schakel over naar de controledatabase.
  4. Start de Adaptive Processing Server opnieuw die de Toezichtfunctie host.
  5. Controleer op het toezichtdashboard dat alles naar verwachting werkt. Verifieer dat deze controletabellen in de database zijn gemaakt:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- Als u geen gegevens in uw trending-database hebt, dat wil zeggen, u hebt een nieuwe installatie, hoeft u de database niet te migreren; u hoeft alleen het BI-platform te configureren om toezichtgegevens vast te leggen in de controledatabase. Dit zijn de stappen op hoog niveau die u moet uitvoeren. Zie de verwante onderwerpen voor meer informatie.
  1. Verifieer dat de controledatabase functioneert en dat de controle goed wordt uitgevoerd.
  2. Maak de volgende toezichttabellen in de controlegegevensopslag.
  3. Configureer de SBO-bestanden en voeg aliasnamen toe.
  4. Schakel over naar de controledatabase.
  5. Start de Adaptive Processing Server opnieuw die de Toezichtfunctie host.
  6. Controleer op het toezichtdashboard dat alles naar verwachting werkt. Verifieer dat deze controletabellen in de database zijn gemaakt:

     MOT_MES_DETAILS
     MOT_MES_METRICS

MOT_TREND_DATA
MOT_TREND_DETAILS

> **Opmerking**
>
> Als u toezichtgegevens vastlegt in de controledatabase en u wilt een rapport baseren op deze gegevens, moet u een aangepaste universe ontwikkelen.

Verwante informatie

SBO-bestanden configureren [pagina 812]
Aliasnamen toevoegen in het SBO-bestand [pagina 814]
Overschakelen naar de controledatabase [pagina 815]
De toezichttabellen maken in de controlegegevensopslag [pagina 811]

20.2.2.1.1 De toezichttabellen maken in de controlegegevensopslag

Voer de volgende stappen uit om de doelcontroledatabase voor te bereiden:

1. Na installatie van het BI-platform zijn DLL-bestanden met betrekking tot alle ondersteunde CMS-controledatabases beschikbaar in de locatie `<Installatiemap>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB`. U vindt zeven verschillende bestanden (SQL-extensie) bij de respectievelijke databasenaam. Bijvoorbeeld: `Oracle.sql` voor Oracle, `Sybase ASE.sql` voor Sybase ASE Database enzovoort.
2. Ga naar de doeldatabase (in dit geval de database waar CMS-controle is geconfigureerd) en voer het SQL-bestand uit. De volgende vier toezichttabellen worden gemaakt: `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS` en `MOT_MES_METRICS`. Behalve de tabellen worden ook de vereiste indexen gemaakt.

Als alle tabellen worden gemaakt met de juiste gegevenstypen zoals in het SQL-bestand, hebt u het databaseschema gemaakt dat voor de toezichtfunctie vereist is.

20.2.2.1.2 Inhoud herstellen naar de doeldatabase

De volgende stappen moeten worden uitgevoerd om de inhoud naar de doeldatabase te herstellen:

1. Schakel Identiteit invoegen in.

   De toezichttabellen bevatten een aantal IDENTITY-kolommen. De waarden in deze kolommen worden automatisch gegenereerd. Er zijn bepaalde databases, bijvoorbeeld MS SQL Server en Sybase ASE, die het expliciet invoegen van waarden in deze kolommen niet toestaan. Tijdens gegevensmigratie moeten echter ook de waarden van deze identiteitskolommen worden gemigreerd. Gebruikers moeten het expliciet invoegen van deze waarden daarom activeren via de volgende SQL-opdracht: `SET IDENTITY_INSERT <TABELNAAM> ON`.

2. Importeer het CSV-dumpbestand in de doeltabel.

   Alle programma's van databaseclients bieden gebruikers de mogelijkheid om CSV-gegevens via een menuoptie of opdracht in de tabel te importeren. De gebruiker moet deze optie gebruiken om de gegevens van het CSV-bestand naar de bijbehorende tabel te importeren. Importeer de gegevensbestanden in de volgende volgorde in de nieuwe tabellen:

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`

3. Schakel Identiteit invoegen uit.

   Wanneer de gegevens zijn geïmporteerd, moet de gebruiker de bewerking voor het invoegen van de identiteit voor de tabel uitschakelen via de volgende SQL-opdracht: `SET IDENTITY_INSERT <TABELNAAM> OFF`.

   Gebruikers moeten de bewerking voor het invoegen van de identiteit van een tabel na het importeren van de gegevens uitschakelen zodat de bewerking voor de volgende tabel kan worden ingeschakeld. De bewerking voor het invoegen van de identiteit kan voor slechts één tabel tegelijk ingeschakeld zijn.

Het in- of uitschakelen van de bewerking voor het invoegen van de identiteit is alleen van toepassing op MS SQL Server en Sybase ASE. Voor andere databases, zoals Oracle, MaxDb. DB2, MySQL of SQL Anywhere, is dit niet vereist. U kunt de gegevens rechtstreeks in de tabellen importeren.

20.2.2.1.3 SBO-bestanden configureren

De Toezichtfunctie gebruikt intern de bibliotheken van de Verbindingsserver, en de Verbindingsserver heeft de SBO-configuratie nodig om verbinding met het databasestuurprogramma tot stand te brengen. U moet het databasestuurprogramma en de locatie in het SBO-bestand opgeven om deze verbinding tot stand te brengen.

> **Opmerking**
>
> De Toezichtfunctie refereert aan de verbindingsnaam van de controledatabase en gebruikt JDBC als `<hostName>.<Portnum>.<dbName>` wordt gebruik of anders ODBC. De SBO-bestanden van de verbindingsserver moeten overeenkomstig worden geconfigureerd zodat de Toezichtfunctie verbinding kan maken met de controledatabase.

> **Opmerking**
>
> Voor Oracle-databases worden alleen JDBC-verbindingen ondersteund.

Voorbeeld

- Als het veld Verbindingsnaam dat op de CMC-controlepagina is geconfigureerd `<hostName>.<Portnum>.<dbName>` is, moet het JAR-bestand van het stuurprogramma geconfigureerd worden in: `dataAccess\connectionServer\jdbc\<dbType>.sbo`.

- Als het veld Verbindingsnaam dat op de CMC-controlepagina is geconfigureerd, een ODBC DSN is, moet het stuurprogramma in het volgende bestand worden geconfigureerd: `<Installatiemap>\dataAccess\connectionServer\odbc\<dbType>.sbo`.
- Als voor controle de SAP HANA-database wordt gebruikt, moet het stuurprogramma worden geconfigureerd in het bestand: `<Install_Dir>\dataAccess\connectionServer\odbc\newdb.sbo`.
- Als voor controle de MS SQL Serverdatabase wordt gebruikt, moet het stuurprogramma worden geconfigureerd in het bestand: `<Install_Dir>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Als de database die wordt gebruikt voor controle een DB2-server is, bevat de verbindingsserver geen ondersteunend bestand `db2iseries.sbo`.
  Standaard gebruikt de toezichtfunctie de ODBC-verbindingsmodus om verbinding te maken met de DB2-controledatabase. Om in deze modus te werken moet u de systeem-DSN (voor de DB2-server) toevoegen en configureren op de computer waarop de toezichtfunctie wordt uitgevoerd. Voor informatie over het toevoegen en configureren van de ODBC-verbinding voor DB2, raadpleegt u de volgende koppelingen:
  - 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

> **Opmerking**
>
> Als u de systeem-DSN niet voor DB2 hebt geconfigureerd, mislukt toezichttrending.

SBO-bestanden configureren

De ODBC-bibliotheken zijn gewoonlijk al in de SBO-bestanden geconfigureerd en u hoeft alleen de aliasnamen toe te voegen. Als dat niet het geval is, volgt u deze voorbeelden om de configuratie in het SBO-bestand uit te voeren:

Voorbeeld

- Als de versie van de database die voor controle wordt gebruikt, SAP HANA is, moet de configuratie in SBO als volgt zijn:

```
<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>
```

- Als de versie van de database die voor controle wordt gebruikt, MS SQL Server 2008 is, moet de configuratie in SBO als volgt zijn:

```
<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>
```

- Als de databaseversie die wordt gebruikt voor controle MySQL 5 is, moet SBO dit gegeven bevatten:

```
<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>
```

- Als de versie van de database die voor controle wordt gebruikt Oracle is, moet de configuratie in SBO als volgt zijn:

```
<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>
```

Raadpleeg de *Handleiding voor gegevenstoegang* voor meer informatie over het configureren van het stuurprogramma in SBO-bestanden.

20.2.2.1.4 Aliasnamen toevoegen in het SBO-bestand

Gebruikers moeten niet alleen het stuurprogramma configureren, maar moeten ook een alias in het SBO-bestand toevoegen, onder de databaseversie die voor controle wordt gebruikt. In de volgende tabel worden de aliasnamen vermeld die voor de opgegeven databases moeten worden gebruikt.

Naam van database	Aliasnaam die in SBO moet worden gebruikt
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

U moet de opgegeven namen gebruiken, omdat de Toezichtfunctie het SBO-bestand doorzoekt op deze namen.

Voorbeeld

Als de database die voor controle wordt gebruikt, MS SQL Server 2008 is, moet de alias als volgt aan het SBO-bestand worden toegevoegd:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</
Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```

20.2.2.1.5 Overschakelen naar de controledatabase

Schakel over naar de database zodat de trending-gegevens van de Toezichtfunctie worden opgeslagen in de controledatabase.

1. Klik in het gebied *Beheren* op de startpagina van de CMC op *Toepassingen*.
2. Klik op *BI-beheerdersstudio*.
3. Kik vervolgens op *Toezichteigenschappen*.
4. Dubbelklik op *Toezichtfunctie* om de eigenschappenpagina te openen.
5. Selecteer in het gebied *Instellingen van trending-database* de optie *Controledatabase gebruiken*.

> **Opmerking**
>
> Als u voor controle een Oracle-database gebruikt, moet de *Verbindingsnaam* van de *ADS-database* op de controlepagina in de CMC als JDBC-verbinding worden opgegeven. Geef de verbindingsnaam als volgt op: `<server_name>,<port>,<service_name>`.

> **Opmerking**
>
> Om ervoor te zorgen dat de controletabellen correct worden gemaakt, moet u de volgende machtigingen verlenen voor het account van de databasegebruiker:
>
> UITVOEREN
> REEKS MAKEN
> ACTIVERING MAKEN

20.2.2.2 Toezichtdatabase configureren met JDBC

U hebt een JDBC-verbinding gemaakt. Voer de volgende stappen uit om een JDBC-verbinding te maken:

1. Plaats de JDBC-stuurprogrammacontainer voor de database die u wilt configureren op de volgende locatie: `<INSTALLATIEMAP\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\MON.MonitoringService\lib>`.

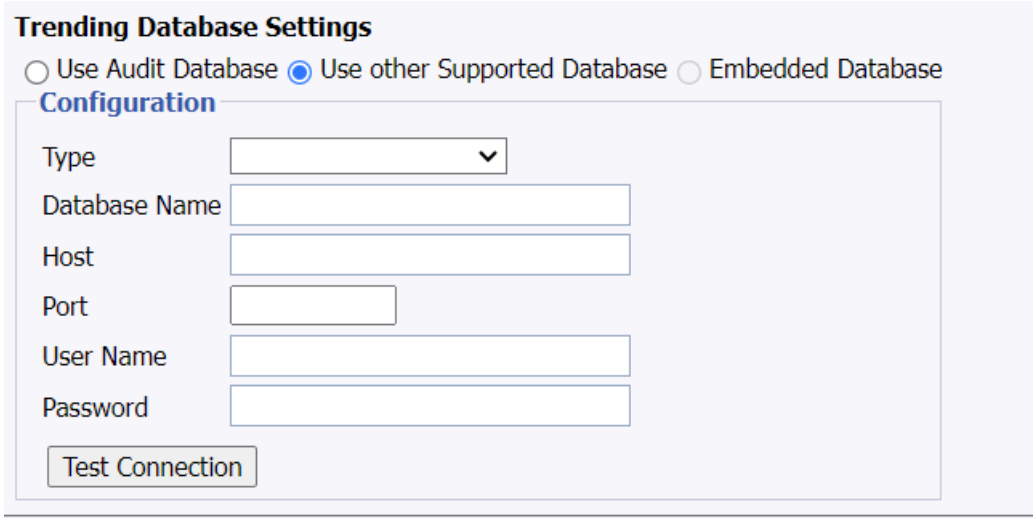
   > **Opmerking**
   >
   > In geclusterde implementaties moet u het JDBC-stuurprogramma kopiëren naar het systeem waarop de toezichtservices worden gehost.

2. Start SIA opnieuw.

Ga als volgt te werk om een nieuwe database voor BI-toezicht te configureren:

1. Meld u aan bij de CMC.
2. Selecteer in het vervolgkeuzemenu op de CMC-startpagina de optie *Toepassingen*.
3. Klik met de rechtermuisknop op *BI-beheerderstudio* en selecteer *Toezichteigenschappen*.

   Het pop-upvenster *Eigenschappen van toezichtfunctie* verschijnt. Standaard wordt het keuzerondje *Controledatabase gebruiken* geselecteerd.
4. Selecteer het keuzerondje *Andere ondersteunde database gebruiken*.
5. Voer het *Type*, de *Databasenaam*, de *Host*, de *Poort*, de *Gebruikersnaam* en het *Wachtwoord* in.



6. **Optioneel:** Voeg het aantal dagen in waarna het platform de historische toezichtsgegevens moet verwijderen met de eigenschap *Alle geschiedenis verwijderen ouder dan X dagen*.
7. Kies *Opslaan en sluiten*.
8. Start de Adaptive Processing Server opnieuw.

   U kunt uw verbinding valideren door *Verbinding testen* te kiezen

> **Opmerking**
>
> Om de wijzigingen van kracht te laten worden, moet u alle APS-servers die de service BI-toezicht hosten opnieuw starten.

U hebt nu een nieuwe database geconfigureerd waarin commentaar uit de BI-toezichttoepassing kan worden opgeslagen.

20.2.3 Configuratie-eigenschappen

In deze sectie worden de eigenschappen van de toezichtfunctie beschreven en hoe u ze kunt bewerken.

De configuratie-eigenschappen van de toezichtfuntie weergeven:

1. Klik op de startpagina van de CMC op *Toepassing*.
2. Klik met de rechtermuisknop op *BI-beheerderstudio* en selecteer *Toezichteigenschappen*. De configureerbare eigenschappen worden hierna beschreven.

Sectie	Veld	Beschrijving
	Toezichtfunctie inschakelen	Selecteer deze optie om de functies voor toezicht in te schakelen. Als u de selectie van deze optie opheft, worden alle functies voor toezicht behalve tests uitgeschakeld. Trending van tests wordt ook uitgeschakeld.

Sectie	Veld	Beschrijving
	Eindpunt-URL van standaard JMX-agent (IIOP)	Dit is de eindpunt-URL van de standaard JMX-agent die gebruikmaakt van het IIOP-protocol. Deze URL wordt automatisch gegenereerd als u de toezichtfunctie inschakelt en de server opnieuw start. Dit is het standaardprotocol voor de toezichtservice. Dit veld is alleen-lezen.
RMI	*RMI-protocol inschakelen voor JMX*	Deze optie is standaard uitgeschakeld. Als u deze optie inschakelt, moet u het RMI-poortnummer opgeven. Deze poort wordt gebruikt voor zowel de RMI-registervermelding als de RMI-connectorpoort. Deze poort moet beschikbaar zijn voor de service, anders wordt de service niet gestart. Nadat u het RMI-poortnummer hebt opgegeven, moet u de server opnieuw starten. Nadat de server opnieuw is gestart, wordt de eindpunt-URL van de RMI JMX-agent gegenereerd. Dit is een alleen-lezen eigenschap met de eindpunt-URL van de JMX-agent die gebruikmaakt van het RMI-protocol. Gebruik deze URL om verbinding te maken met toezicht via andere clients.
Hostgegevens	*Hostgegevens inschakelen*	Deze optie is standaard uitgeschakeld. Als u deze optie inschakelt, moet u het pad naar uw installatie van binair bestand SAPOSCOL opgeven. U moet SAPOSCOL installeren om hostgegevens te kunnen inschakelen. Zie voor meer informatie over het installeren van SAPOSCOL: “SAPOSCOL installeren”.
Instellingen van trending-database	*Controledatabase gebruiken*	Selecteer deze optie om de trendgeschiedenis van gegevens in de ADS-controledatabase (Auditing Data Store) op te slaan. **Opmerking** Dit werkt alleen als Auditing Data Store is geconfigureerd.
	Andere ondersteunde database gebruiken	Selecteer deze optie om de geschiedenis van de gegevens-/controle-trending in een ondersteunde database die u hebt geconfigureerd op te slaan.
	Alle geschiedenis verwijderen ouder dan X dagen	Hiermee geeft u op hoe lang, in dagen, de historische gegevens moeten worden bewaard.

Sectie	Veld	Beschrijving
Overige instellingen	*Vernieuwingsinterval voor meetwaarden (seconden)*	Het minimuminterval dat u kunt opgeven, is 15 seconden. Dit interval bepaalt het volgende: • Abonnementsberekening van de controles: de waarschuwings- en gevarenregels worden continu berekend met het opgegeven tijdsinterval. • De controlestatus berekenen: de controlestatus wordt continu berekend met het tijdsinterval dat wordt opgegeven als de Gebeurtenis-instelling van de controle wordt geselecteerd met de volgende optie: *Controlestatus telkens wijzigen wanneer de waarschuwings- of gevarenregel op waar wordt geëvalueerd*. • Trending-periode: geschiedenismodus voor de grafieken wordt continu vastgelegd met het opgegeven tijdsinterval.
	Interval voor automatisch vernieuwen van toezicht-UI (seconden)	Dit interval wordt gebruikt in de gebruikersinterface voor toezicht (waaronder dashboard, controlelijst en tests) voor automatische vernieuwing. Het minimuminterval is 15 seconden. De functie Automatisch vernieuwen heeft geen invloed op de tijdsduur in Live-modus in grafieken, die standaard is ingesteld op 15 seconden.
	Frequentie van herinneringsmelding (dagen)	Hiermee wordt het aantal dagen opgegeven voordat een meldingsherinnering wordt gegenereerd.

3. Klik op *Opslaan*.

> **Opmerking**
>
> Wanneer u deze eigenschappen wijzigt, behalve wanneer u de Toezichtfunctie in- en uitschakelt, moet u de Adaptive Processing Servers die de toezichtservices hosten, opnieuw opstarten.

SAPOSCOI installeren

Voer de volgende stappen uit om SAPOSCOL te installeren:

1. Download `SAPHOSTAGENT710_XX.SAR` van SAP Marketplace (http://service.sap.com).
2. Extraheer `SAPHOSTAGENT710_XX.SAR` door de opdracht `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` uit te voeren.
3. Installeer `saphostexec` door de opdracht `saphostexec.exe -install` uit te voeren. Nadat saphostexec als service is geïnstalleerd, wordt SAPOSCOL gestart.
4. Controleer de SAPOSCOL-status door de opdracht `saposcol -s` uit te voeren.

20.2.3.1 URL van JMX-eindpunt

De toezichtfunctie toont een URL van een JMX-eindpunt waarmee andere clients verbinding kunnen maken met behulp van een externe JMX-API. De JMX-connectiviteit wordt standaard geboden via het transport IIOP (Internet Inter-Orb Protocol) of CORBA (Common Object Request Broker Architecture). De verbindings-URL wordt weergegeven op de eigenschappenpagina van de toezichtfunctie. Dankzij de verbindingsmogelijkheid via IIOP hoeft u zich geen zorgen meer te maken over firewalls en het weergeven van poorten. De CORBA-poorten zijn standaard beschikbaar. De JMX-client heeft de JAR-bestanden die in de volgende tabel worden vermeld, nodig om verbinding te maken:

Jar-bestanden
`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`

Een andere optie is verbinding maken via de standaard RMI-poort. Zie Configuratie-eigenschappen [pagina 817] voor meer informatie over verbinding maken via de RMI-poort.

20.2.3.2 JMX SSL-configuratie

U kunt nu beveiligde communicatie tot stand brengen tussen JConsole en BOE via JMX SSL-configuratie.

1. Meld u aan bij CMC.
2. Navigeer naar *Toepassingen* > *BI-beheerderstudio* > *Toezichteigenschappen*.
3. Schakel onder *RMI* de optie *RMI-protocol inschakelen voor JMX* in.
4. Voer het RMI-poortnummer in.

   7777
5. Schakel de optie *SSL voor RMI-protocol voor JMX inschakelen* in.
6. Klik op *Opslaan* en *Sluiten*.
7. Start de *Adaptive Processing Server* opnieuw.

> **Opmerking**
>
> De server die de toezichtservice host wordt opnieuw gestart.

20.2.3.2.1 Certificaat genereren

1. Open de opdrachtprompt in de beheerdersmodus of een terminalsessie en navigeer naar deze locatie:

   Windows:

   ```
   INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
   ```

   Linux/Unix:

   ```
   INSTALLDIR/sap_bobj/enterprise_xi40/<PLATFORM>_x64/sapjvm/bin
   ```
2. Voer de opdracht uit om een certificaat te genereren: `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore`
3. Voer alle vereiste informatie in voor het maken van een certificaat.
4. 4. Zodra het uitvoeren is geslaagd, wordt een certificaatbestand gemaakt in dezelfde sapjvm/bin-map: `serverkeystore`

20.2.3.2.2 Een certificaatopslagbestand toevoegen aan de toezichtservice

1. Navigeer in CMC naar *Servers* > *Lijst met servers*.
2. Selecteer *Adaptive Processing Server* (toezichtservice voor serverhosting).
3. Selecteer *Eigenschappen*.
4. Navigeer naar de sectie *JMX SSL-configuratie*.
5. Voer bij *Certificaat - locatie voor opslag bestand* het pad van de *bestandslocatie van de certificaatsleutelopslag* in.

6. Voer de informatie over het *Wachtwoord voor toegang tot privésleutel* in.

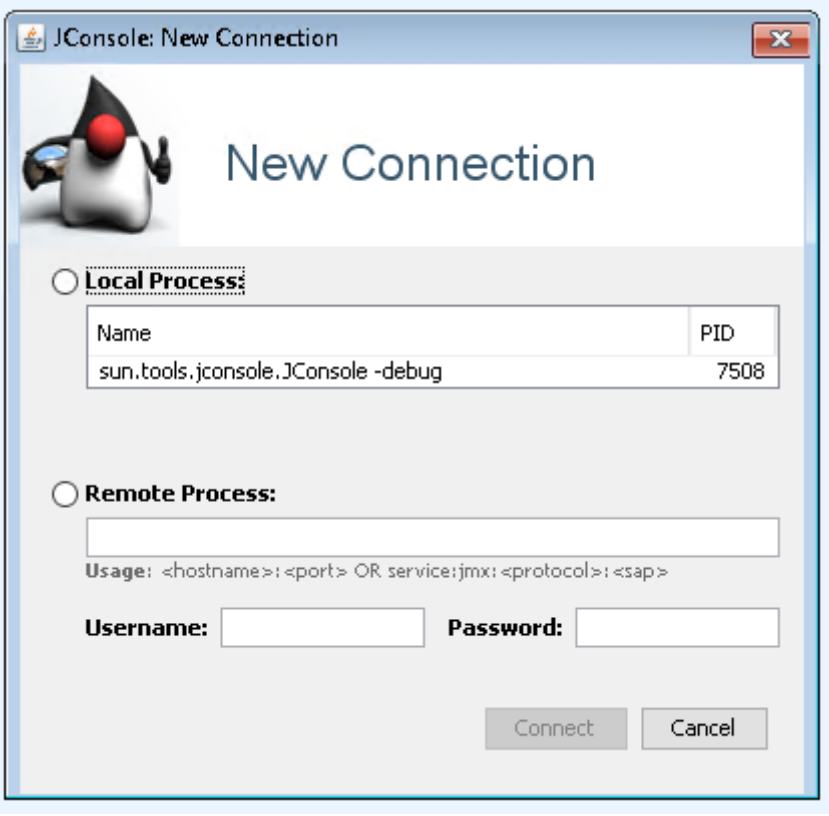
   Wachtwoord 1

20.2.3.2.3 Verbinding maken met JConsole

1. Voer de opdracht uit om `JCONSOLE.exe` te starten in de opdrachtprompt (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`)

   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:\Program Files
   (x86)\SAP BusinessObjects\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\bin\serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```

2. Zodra de bovenstaande opdracht is uitgevoerd, wordt de JConsole Viewer gestart zoals hieronder wordt getoond.



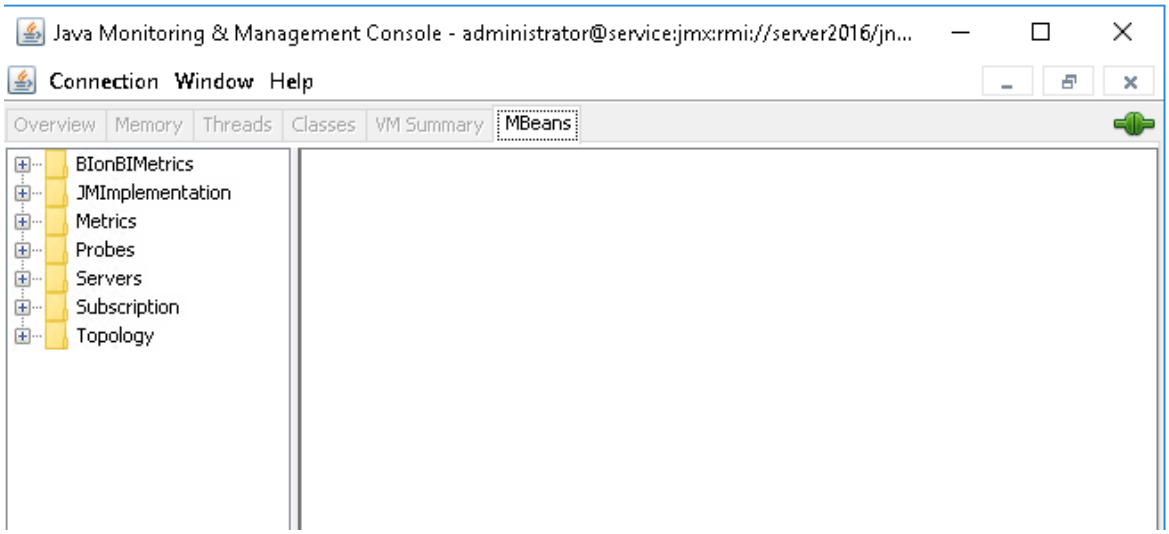
3. Klik op het keuzerondje *Extern proces* om het veld in te schakelen.
4. Voer de *Eindpunt-URL van RMI JMX-agent* en de gekoppelde *Gebruikersnaam* en *Wachtwoord* in.

   De indeling van *Eindpunt-URL van RMI JMX-agent* is: `service:jmx:rmi://<HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

   `service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.

5. Klik op *Verbinding maken*.

6. De JConsole Viewer *JAVA Monitoring & Management Console* (Java-console voor controle en beheer) wordt gestart.



7. In de JConsole Viewer kunt u naar verschillende secties zoals BIonBIMetrics, Metrics (Metrische gegevens), Probes (Tests), Servers en Topology (Topologie) navigeren om de gerelateerde gegevens op te halen.

20.2.3.3 HTTPS-verificatie voor controletests

HTTPS-serververificatie voor controletests wordt ondersteund, maar moet voor gebruik als volgt worden geconfigureerd:

1. Importeer het servercertificaat naar de truststore van de client. Zo kan de clientzijde (de test) de identiteit van de server verifiëren. Voer de volgende opdracht uit: `<INSTALLATIEHOOFDMAP\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<INSTALLATIEHOOFDMAP>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" –file ca.cer`
   `ca.cer` is het zelfondertekende certificaat van de server of het certificaat van de certificeringsinstantie (meestal een interne instantie) die het servercertificaat heeft gegenereerd. Als het certificaat is gegenereerd door een bekende certificeringsinstantie, hoeft u het certificaat niet te importeren en kunt u deze stap overslaan. Het servercertificaat wordt namelijk geverifieerd bij de certificeringsinstantie, waarvan de openbare sleutel standaard in de truststore staat.
2. Wijzig de *URL-basis* in de testinstellingen van BI-startpunt naar `https://<URL>/BOE/BI`, waarbij <URL> verwijst naar de host door de naam die in het certificaat is gebruikt.

HTTPS-clientverificatie voor controletests wordt niet ondersteund.

20.2.3.4 Wachtwoordcodering voor tests

Wanneer u tests gebruikt, zorgt u dat wachtwoorden gecodeerd zijn door de parameter `true` toe te voegen aan de wachtwoordparameter van elke controletest wanneer u de test via de opdrachtregel maakt. Raadpleeg het

onderwerp *Tests beheren via de opdrachtregel* in de Help van de CMC voor meer informatie en een voorbeeld van de syntaxis.

20.2.4 Integratie met andere toepassingen

Enterprise-oplossingen, zoals IBM Tivoli Monitoring, kunnen worden geïntegreerd met de Toezichtfunctie als JMX-clients die verbinding maken via de JMX-eindpunt-URL. Na integratie kunnen de SAP BusinessObjects-gegevens worden weergegeven via de gebruikersinterface van de client.

20.2.4.1 De toezichtfunctie integreren met SAP Solution Manager

Als u de toezichtfunctie wilt integreren met SAP Solution Manager, moet Wily Introscope in uw systeem geïnstalleerd en actief zijn. De SAP Solution Manger moet geconfigureerd zijn voor het Introscope-werkstation. Voer de volgende stappen uit tijdens de installatie van het BI-platform:

1. Bij de stap "Connectiviteit configureren voor Introscope Enterprise Manager" geeft u de hostnaam en poortdetails op. Er wordt een Introscope-agent geïnstalleerd in `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wily` wanneer het BI-platform wordt geïnstalleerd.
2. Start het Wily Introscope-werkstation en klik op *Nieuwe investigator*. U kunt de SAP BusinessObjects-servergegevens weergeven en virtuele gegevens testen in de JMX-sectie van de geconfigureerde agent.

> **Opmerking**
>
> U kunt de Wily Introscope-agent (IS) configureren via *CMC* > *Servers* > *Serverknooppunt* > *Tijdelijke aanduidingen*. De host en poort van de IS Enterprise Manager worden hier ook geconfigureerd voor de IS-agent voor het communiceren met de toezichttoepassing. Zie *Servers beheren* in de Help voor CMC voor meer informatie.
>
> Voor het beschikbaar maken van JMX-gegevens in IS moet u ervoor zorgen dat zowel de IS-agentservices als de toezichtservices beschikbaar zijn in het AdaptiveProcessingServer-exemplaar.
>
> Als u IS-instrumentatie inschakelt, wordt de code-instrumentatie automatisch ingeschakeld.

20.2.5 Clusterondersteuning voor toezichtserver

De Toezichtfunctie ondersteunt het maken van clusters en biedt daarmee failover-functionaliteit.

Met clusterondersteuning is op elk moment slechts één service actief en zijn alle andere services passief. Als er twee toezichtservices (s1 en s2) in een clusteromgeving zijn, is er slechts één actief. Zowel s1 als s2 proberen actief te worden, maar wanneer een van de twee hierin slaagt, wordt de andere service inactief of passief.

De passieve service controleert af en toe (elke minuut) de beschikbaarheid van de actieve service. Als de actieve service niet beschikbaar is, probeert de passieve service zich onmiddellijk te activeren.

> **Opmerking**
>
> Het verdient aanbeveling de toezichtfunctie op een apart APS-exemplaar (Adaptive Processing Server) te hosten om fouten of slechte prestaties van de APS te voorkomen.

20.2.6 Problemen oplossen

In deze sectie worden stapsgewijze oplossingen geboden voor een scala aan problemen die zich kunnen voordoen wanneer u met de Toezichtfunctie werkt.

20.2.6.1 Dashboard

De koppeling Toezicht wordt niet weergegeven op de CMC-pagina

- Controleer of de gebruiker de juiste toegangsrechten heeft.
- Zorg ervoor dat de gebruiker is toegevoegd aan de groepen Toezichtgebruiker of Beheerder, of aan een andere groep die deel uitmaakt van deze groepen.

KPI's (Key Performance Indicators) zijn niet zichtbaar op het dashboard Toezicht.

- Controleer of de vereiste gegevens zichtbaar zijn door *CMS-servereigenschappen* > *Gegevens* te selecteren.
- Zorg ervoor dat de Central Management Server reageert zoals verwacht.

20.2.6.2 Meldingen

Kan geen meldingen ontvangen op de pagina Meldingen

- Controleer of de optie *Mijn meldingen inschakelen* in de eigenschappen van de meldingstoepassing is geselecteerd.
- Controleer of u de juiste rechten hebt voor het ontvangen van meldingen.
- Controleer of de recente meldingen zichtbaar zijn op het dashboard voor toezicht.

> **Opmerking**
>
> U kunt een Crystal Reports-document sturen naar de e-mail-id die u instelt om te testen of de SMTP naar verwachting werkt.

Kan geen e-mailmeldingen ontvangen

- Controleer of de optie *E-mail inschakelen* in de eigenschappen van de meldingstoepassing is geselecteerd.
- Controleer of de e-mailinstellingen voor het ontvangen van e-mailmeldingen goed zijn.
- Controleer of de SMTP-server actief is.
- Zorg dat het Adaptive Job Server-exmplaar is ingeschakeld.
- Controleer de SMTP-instellingen in het doel van het Adaptive Job Server-exemplaar.

20.2.6.3 Controlelijst

Kan geen historische gegevens ophalen voor Controle

- Controleer het pollinginterval op de pagina *Eigenschappen* van de toezichtfunctie.
- Controleer het traceringsbestand in de logboekmap.
- Controleer of de systeemtijd van de server en client gelijk is in een specifieke tijdzone.

Er is een fout opgetreden bij het ophalen van gesynchroniseerde livegegevens

Controleer of het Adaptive Processing Server-exemplaar actief is.

Het tabblad Controlelijst is uitgeschakeld

- Controleer of de toezichtservice actief is.
- Controleer of de toezichtfunctie foutberichten vastlegt in een logboek.
- Controleer of de servers en de bijbehorende gegevens zichtbaar zijn in jConsole.

20.2.6.4 Tests

Kan geen Tests plannen

- Controleer of het AdaptiveJobServer-exemplaar dat de Planningsservice van test host, actief is.
- Zorg ervoor dat de rapport-CUID die gebruikt wordt voor Crystal Reports-rapporten en Web Intelligence-documenten, juist is.
- Zorg ervoor dat de gebruiker beheerdersrechten heeft of lid is van de Beheerdersgroep.

- Controleer of de gebruiker de juiste rechten heeft om Crystal Reports- of Web Intelligence-documenten die in de bijbehorende tests worden gebruikt, te openen, vernieuwen en exporteren.

Planningsstatus van test is In behandeling

- Controleer of het ProbeSchedulingService-exemplaar is geïnstalleerd.
- Controleer of het AdaptiveJobServer-exemplaar dat de Planningsservice van test host, actief is.

Er is een fout opgetreden bij het ophalen van trendgegevens uit de database

Controleer of het AdaptiveProcessingServer-exemplaar actief is.

probeRun.bat kan niet worden uitgevoerd

- Controleer of `java_home` is ingesteld.
- Controleer of de juiste parameters zijn ingevoerd in de opdrachtaanwijzing.

> **Opmerking**
>
> Voer **`probeRun.bat -help`** in de opdrachtaanwijzing in om te controleren of alle parameters geschikt zijn.

20.2.6.5 Gegevens

Hostgegevens worden niet vermeld

- Zorg ervoor dat SAPOSCOL actief is.
- Zorg ervoor dat de optie *Hostgegevens inschakelen* geselecteerd is op de pagina *Eigenschappen* van de toezichtfunctie.
- Start het AdaptiveProcessingServer-exemplaar opnieuw op om de wijzigingen te implementeren.
- Zorg ervoor dat het *Pad naar uw installatie van binair bestand SAPOSCOL* juist is.

Er is een fout opgetreden bij het ophalen van de JMX-client

Controleer of het AdaptiveProcessingServer-exemplaar actief is.

SAPOSCOL-gegevenswaarde is nul op de pagina Gegevens

- Zorg ervoor dat SAPOSCOL actief is.
- Voer de volgende stappen uit op de host waarop SAPOSCOL geïnstalleerd is:
  1. `saposcol -s` om de status te controleren
  2. `saposcol -m` om een momentopname te verkrijgen van de gegevens die door SAPOSCOL zijn verzameld

20.2.6.6 Diagram

Grafieken tonen verschillende tijden voor de live- en geschiedenismodi

Zorg ervoor dat de systeemtijd van de server en client gelijk is in een specifieke tijdzone.

20.3 Visueel verschil

Met visueel verschil kunt u de verschillen tussen twee versies van een LCMBIAR of van een object of van beide bekijken. U kunt deze functie gebruiken om het verschil tussen bestanden of objecten te bepalen en zo verschillende rapporttypen te ontwikkelen en onderhouden. Deze functie biedt een vergelijkingsstatus tussen de bron- en doelversies. Als bijvoorbeeld een eerdere versie van het gebruikersrapport juist is en de huidige versie niet goed is, kunt u het bestand vergelijken en analyseren om vast te stellen wat het probleem is.

Startpagina

De startpagina van Visueel verschil bevat de volgende tabbladen en vensters:

- Nieuwe vergelijking: op dit tabblad kunt u een nieuwe vergelijking tussen objecten instellen
- Zoeken naar vergelijkingen: in dit veld kunt u zoeken naar objecten die al vergeleken zijn
- Venster Vergelijkingen: hier worden de tabbladen met filters en verschillen weergegeven
- Venster Vergelijkingen: verschillen: in dit venster worden de vergeleken objecten weergegeven met de naam van de vergelijking, de datum/tijd en de status van de verschillen

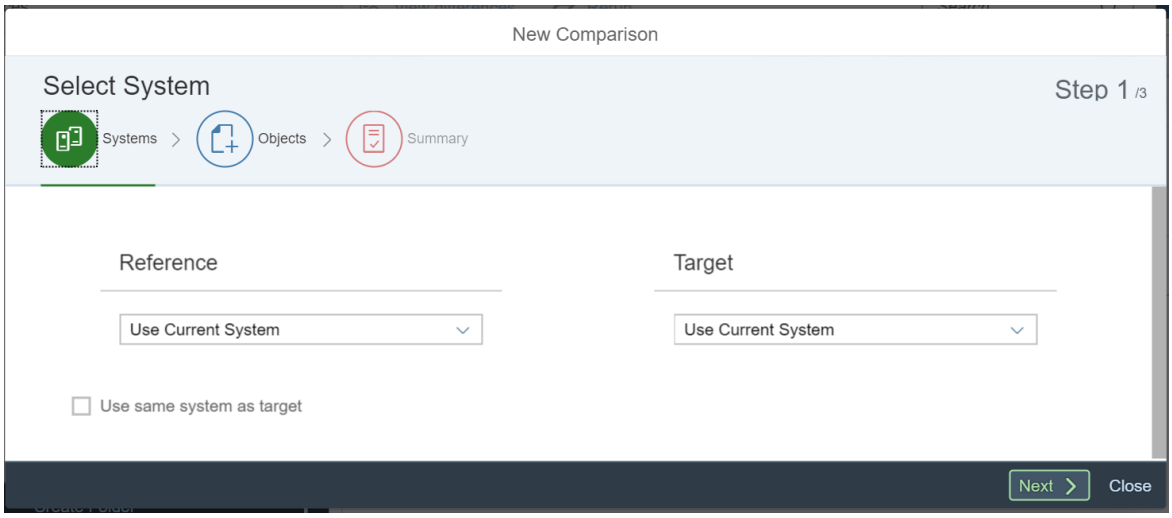
20.3.1 Objecten of bestanden vergelijken met Visueel verschil

Voer de volgende stappen uit om bestanden te vergelijken op visuele verschillen:

1. Meld u aan bij de CMC-toepassing.
2. Klik op de CMC-startpagina op het tabblad *Beheren* op de koppeling *Visueel verschil*.
   De pagina Visueel verschil wordt weergegeven. De vergeleken bestanden worden opgeslagen in de map Verschillen of in submappen die door de gebruiker zijn gemaakt.

   > **Opmerking**
   >
   > Om een nieuwe submap te maken, selecteert u Create Folder +.

3. Selecteer + om een nieuwe vergelijking te maken.
   De wizard *Nieuwe vergelijking* wordt weergegeven.



4. Selecteer het *Referentie*- en *Doel*-systeem uit de vervolgkeuzelijst.
   U kunt verbinding maken met een van de volgende referentie- en doelsystemen:

   > **Opmerking**
   >
   > Als een object in het Versiebeheersysteem wordt toegevoegd, ontstaat de optie om versies te selecteren in de volgende stap.

   - CMS
   - Lokaal bestandssysteem
5. In het scherm *Objectselectie* zoekt en selecteert u het object of een bestand uit het *Referentie*- en *Doel*-systeem.
6. Wijzig indien nodig de *Naam van vergelijking*.
7. Selecteer *Vergelijken* om de objecten te vergelijken.

   > **Opmerking**
   >
   > - U kunt de verschillen controleren door eerst de vergelijking te selecteren en vervolgens *Verschillen weergeven*. De verschillen worden met oranje en de ontbrekende objecten met rood gemarkeerd.

- U kunt opnieuw een vergelijking uitvoeren door eerst de vergelijking te selecteren en vervolgens *Opnieuw uitvoeren* te selecteren.

Het vergelijkingsproces start onmiddellijk.

U kunt ook de filteroptie gebruiken om de vergeleken objecten per type te bekijken, en met verschillen of met gedeelde attributen.

20.3.2 Objecten of bestanden vergelijken met het Versiebeheersysteem

U kunt taken of mappen voor Promotiebeheer vergelijken in een Versiebeheersysteem via de optie Visueel verschil.

Voer de volgende stappen uit om objecten in een versiebeheersysteem te vergelijken:

1. Meld u aan bij de CMC-toepassing.
2. Klik op de CMC-startpagina op het tabblad *Beheren* op de koppeling *Visueel verschil*.
   De pagina Visueel verschil wordt weergegeven. De vergeleken bestanden worden opgeslagen in de map Verschillen of in submappen die door de gebruiker zijn gemaakt.

   > **Opmerking**
   >
   > Klik op het mappictogram om een nieuwe submap te maken.

3. Klik op *Nieuwe vergelijking*.
   Het venster *Visueel verschil - vergelijkingen* wordt weergegeven.
4. Selecteer *Aanmelden bij VMS* in *Systeem selecteren* onder Verwijzing.
5. Voer de aanmeldingsreferenties in voor VMS en klik op *Aanmelden*.
   Nu wordt het dialoogvenster *Visueel verschil - Automatisch doelsysteem selecteren* weergegeven.
6. Klik op *Nee* als u een ander doelsysteem wilt instellen, of klik op *Ja* als het doelsysteem hetzelfde moet zijn als het referentiesysteem.
7. Klik op *Bladeren* om in de referentie- en doelsystemen de objecten of taken te selecteren die u wilt vergelijken.
8. Klik op *Toevoegen*.
   De objecten die zijn geselecteerd om te vergelijken, worden weergegeven in het venster *Nieuwe vergelijking*.
   U kunt de bestanden meteen vergelijken, of de vergelijking voor later plannen. Als u de bestanden wilt vergelijken, gaat u door naar de volgende stap.
9. Klik op *Vergelijken* om de mappen of objecten te vergelijken.
   Het vergelijkingsproces gaat direct van start. Eventuele verschillen worden weergegeven in de *viewer van Visueel verschil*. De verschillen worden met oranje en de ontbrekende objecten met rood gemarkeerd.
   U kunt ook de filteroptie gebruiken om de vergeleken objecten per type te bekijken, en met verschillen of met gedeelde attributen.
10. Klik op *Opslaan* om het verschillenrapport op te slaan.
11. Geef de locatie op waar u het rapport wilt opslaan, en klik op *OK*.

20.4 HTML-elementen autoriseren

Geef een lijst geautoriseerde HTML-elementen op om gebruikers te laten profiteren van betrouwbare HTML-elementen en uw organisatie te beschermen tegen indringers.

Wanneer een gebruiker een document opent dat een cel bevat met de eigenschap Lezen als HTML of de eigenschap Lezen als hyperlink in de HTML-viewer of Interactive Viewer van Web Intelligence, kan de viewer de HTML interpreteren. Dit gedrag hangt of van de manier waarop u de weergave van deze cellen hebt gedefinieerd in de weergave-instellingen van Web Intelligence en de HTML-elementen die u autoriseert.

Wanneer u de geautoriseerde HTML-elementen opgeeft en een document in de leesmodus een niet-geautoriseerd element bevat, wordt alleen de tekst uit het element behouden - niet de elementcode of -attributen. In een document dat een geautoriseerd element en zowel geautoriseerde als niet-geautoriseerde attributen bevat, worden alleen het element en de geautoriseerde attributen behouden.

Als u alleen specifieke HTML-elementen in de weergave-eigenschappen van Web Intelligence voor JavaScript wilt autoriseren, selecteert u *Enkel op de pagina Geautoriseerde HTML-elementen gedefinieerde HTML-elementen inschakelen* en geeft u de HTML-elementen op de pagina *Gemachtigde HTML-elementen* op.

Standaard worden alleen de HTML-elementen die vereist zijn voor een juiste werking van Web Intelligence geautoriseerd. U kunt elementen toevoegen aan of verwijderen van de standaardlijst.

⚠ Let op

- Dankzij de mogelijkheden voor formules biedt Web Intelligence ingesloten JavaScript/HTML-code in documentcellen.
  Deze code kan worden ingeschakeld of uitgeschakeld in de Central Management Console. Door JavaScript, HTML's en hyperlinks te autoriseren, erkent u echter het risico dat u wordt blootgesteld aan cross-site scripting. Met cross-site scripting kunnen aanvallers websites aanpassen of codes uitvoeren op andere systemen. Deze kwetsbaarheid heeft invloed op producten zoals internetbrowsers wanneer ze scripts uitvoeren. In de meeste gevallen zijn cross-site scripting-aanvallen het gevolg van onbeveiligd programmeren op het doelsysteem.
- De code kan worden afgestemd door een lijst met geautoriseerde HTML-codes en -attributen. SAP is echter niet verantwoordelijk voor de compatibiliteit van deze code en de mogelijke neveneffecten. Uw code kan bijvoorbeeld mogelijk enkele aanpassingen vereisen vanwege browserupdates, ondersteuning voor de JavaScript-code of de manier waarop de code dynamisch wordt ingesloten op de webpagina. Vanuit een technisch standpunt wordt de toepassing vanaf versie 4.3 als een toepassing van één pagina uitgevoerd. Er is geen technische scheiding tussen het rapport en de webpagina. De code vereist mogelijk enkele aanpassingen om in die nieuwe context te kunnen worden uitgevoerd.
- Het verwijderen van elementen van de standaardlijst kan negatieve gevolgen hebben voor de werking van Web Intelligence en daarom raden we dit af.

U kunt het volgende autoriseren:

- Het element `<a>` met het attribuut `href` om een referentie toe te voegen.
- Een set attributen voor alle elementen in uw lijst door het element * te koppelen aan de lijst met attributen.
  U kunt niet alle attributen autoriseren die aan een element zijn gekoppeld.
- Elementen die mogelijk JavaScript bevatten, zoals `<script>`, `<onClick>` en `<onMouseEnter>`.
  U kunt geen JavaScript-trefwoorden autoriseren.

Voorbeeld

Geautoriseerde HTML-elementen

Element	Attributen
*	style, class, id
img	src
link	ref

In de volgende tabel wordt vermeld hoe Web Intelligence HTML-elementen weergeeft in documenten als een resultaat van de autorisaties.

Gevolg van de autorisaties voor HTML-elementen

Oorspronkelijke HTML	Uiteindelijke HTML	Uitleg
`<link title="SAP" ref="www.sap.com">`	`<link ref="www.sap.com">`	Het element `<link>` en het attribuut `ref` worden geautoriseerd, zodat de link als een actieve link wordt weergegeven in het document. Het attribuut `title` wordt niet geautoriseerd en wordt daarom verwijderd uit het document.
`<img src="datasource" id="I1">`	`<img src="datasource" id="I1">`	Het element `<img>` en het gekoppelde attribuut `src` worden geautoriseerd en het attribuut `id` wordt geautoriseerd voor elementen. De oorspronkelijke HTML blijft ongewijzigd.
`<div title="datasource" id="D1">`	Verwijderd.	Het element `<div>` wordt niet geautoriseerd. Het element en de gekoppelde attributen worden daarom verwijderd uit het document.
`<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>`	`...as shown in the picture below:<img src="../picture.jpg">`	Het element `<p>` wordt niet geautoriseerd en wordt daarom verwijderd. Alleen de tekst die zich bevindt in het element `<p>` blijft behouden. Het element `<img>` en het gekoppelde attribuut `src` worden geautoriseerd en blijven dus behouden. Het attribuut `alt` wordt niet geautoriseerd en wordt daarom verwijderd uit het document.

Weergave-instellingen voor Web Intelligence wijzigen [pagina 708]De lijst met geautoriseerde HTML-elementen wijzigen [pagina 833]

20.4.1 De lijst met geautoriseerde HTML-elementen wijzigen

Geef de betrouwbare HTML-elementen op die u wilt autoriseren en waarvoor u beveiliging wilt bieden tegen mogelijk schadelijke elementen door de lijst met geautoriseerde HTML-elementen te wijzigen.

Web Intelligence autoriseert alleen de elementen die u definieert op de pagina *Gemachtigde HTML-elementen* wanneer de JavaScript-weergave-eigenschap *Enkel op de pagina Geautoriseerde HTML-elementen gedefinieerde HTML-elementen inschakelen* actief is in de Web Intelligence-eigenschappen.

1. Ga naar CMC en selecteer *BI-beheerderstudio*.
2. Blader op het *startscherm van de Central Management Console* omlaag naar *HTML-elementen*.
3. Wijzig de lijst zoals in de volgende tabel wordt beschreven:

Wijziging	Stappen
Een element toevoegen	Klik op *Een nieuw element toevoegen* en voer het element en de bijbehorende attributen in die u wilt autoriseren. **Opmerking** • Als u bepaalde attributen voor alle HTML-elementen wilt autoriseren, voert u * als het element in en voegt u de attributen toe. • Wanneer u probeert een HTML-element toe te voegen dat zich al op de lijst bevindt, worden alleen nieuwe attributen voor het element aan de lijst toegevoegd.
Een element bewerken	Klik op het element en klik op *Het geselecteerde element bewerken*.
Een element verwijderen	Klik op het element en klik op *Het geselecteerde element verwijderen*.
De standaardlijst met geautoriseerde HTML-elementen herstellen	Klik op *Opnieuw instellen*. De standaardlijst bevat alleen de elementen die vereist zijn voor een juiste werking van Web Intelligence.

21 CMS-rapportage

21.1 CMS-rapportage

Voordat u begint met rapportage op de CMS, moet u een basisbegrip van de volgende concepten hebben:

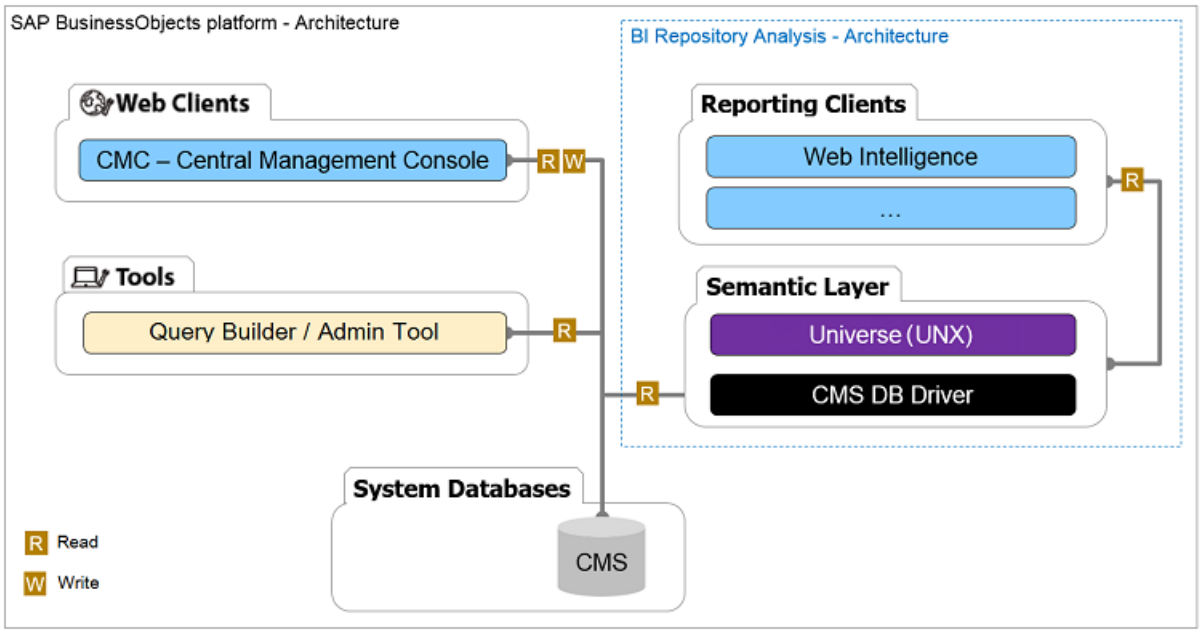
- De architectuur van het SAP BusinessObjects-platform
- De structuur van de CMS-systeemdatabase
- InfoObject-eigenschappen en -relaties

Verwante informatie

De architectuur van het SAP BusinessObjects-platform [pagina 834]
De structuur van de CMS-systeemdatabase [pagina 835]

21.1.1 De architectuur van het SAP BusinessObjects-platform

Het schema is ontworpen met het oog op het verschaffen van meer inzicht in de architectuur van het SAP BusinessObjects-platform.



De volgende tabel biedt u meer informatie over de onderdelen van het SAP BusinessObjects-platform.

De onderdelen van het SAP BusinessObjects-platform

Onderdelen	Beschrijving
CMC - Central Management Console	Een webgebaseerde tool waarmee u beveiligingsinstellingen kunt configureren en de volgende items kunt beheren: • Gebruiker • Inhoud • Server
CMS-systeemdatabase	Een database waarin de volgende informatie over BI-platform is opgeslagen: • Gebruiker • Server • Document • Configuratie • Verificatie De CMS-systeemdatabase wordt beheerd door de Central Management Server (CMS); er kan naar worden verwezen als systeemgegevensopslagruimte.
BEx Query Designer (ook beheertool genoemd)	Een webgebaseerde tool die u kunt gebruiken om query's uit te voeren op de BusinessObjects-gegevensopslagruimte en de benodige informatie op te halen die niet in CMC staat.
BI Repository Analysis	Met deze oplossing voert u query's op de CMS uit via de semantische laag van het BI-platform Universe (UNX) en CMS-DB-stuurprogramma.

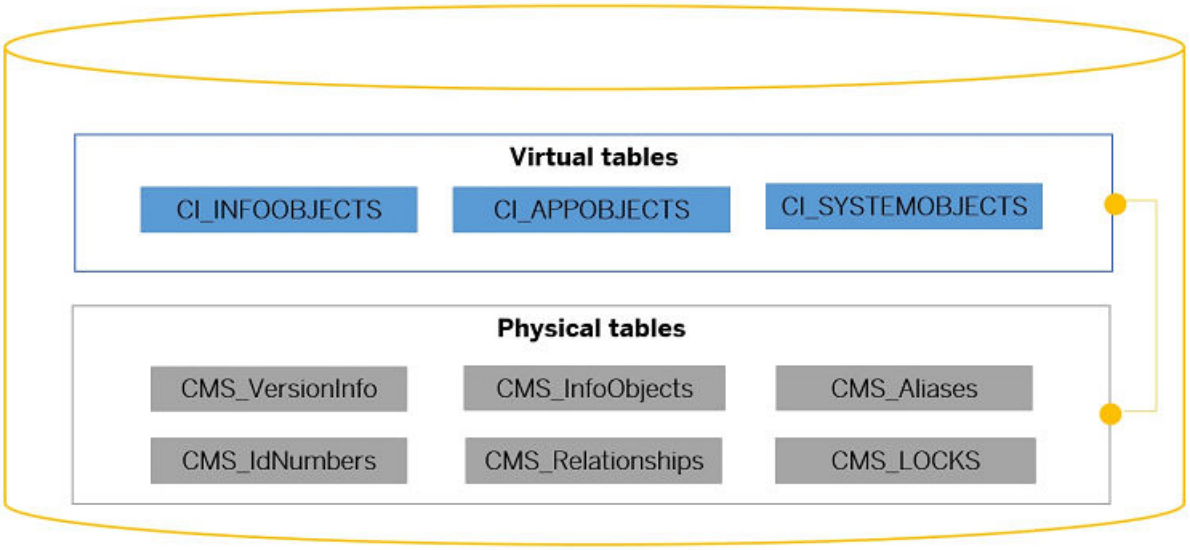
21.1.2 De structuur van de CMS-systeemdatabase

De CMS-systeemdatabase wordt beheerd door de Central Management Server (CMS); er kan naar worden verwezen als systeemgegevensopslagruimte. Het CMS-systeem is een database waarin BI-platforminformatie in de vorm van InfoObjects wordt opgeslagen.

De CMS-systeemdatabase omvat twee soorten tabellen:

- Fysieke databasetabel: de CMS-metagegevens worden opgeslagen in fysieke databasetabellen.
- Virtuele tabel: de CMS-server bladert door de InfoObjects vanuit virtuele tabellen.

Het volgende schema geeft u een overzicht van de structuur van de CMS-systeemdatabase.



Zie de verwante onderwerpen voor meer informatie over de structuur van de CMS-systeemdatabase.

Verwante informatie

Fysieke databasetabellen [pagina 836]
Virtuele tabellen [pagina 837]

21.1.2.1 Fysieke databasetabellen

de CMS-metagegevens worden opgeslagen in fysieke databasetabellen.

Fysieke databasetabellen

Fysieke tabel	Beschrijving
CMS_VersionInfo	Omvat de huidige versie van BusinessObjects Enterprise (BOE)
CMS_InfoObjects	Hoofdtabel in de systeemgegevensopslagruimte In elke rij is één InfoObject opgeslagen.
CMS_Aliases	Koppelt de gebruikersalias(sen) aan de bijbehorende gebruikers-ID. Een gebruiker heeft een alias voor elk beveiligingsdomein waarin de gebruiker een lid is. Een gebruiker heeft echter maar één gebruikers-ID.
CMS_IdNumbers	Genereert unieke object-ID's en type-ID's.

Fysieke tabel	Beschrijving
CMS_Relationships	Slaat de relaties tussen InfoObjects op.
CMS_LOCKS	Hulptabel vanCMS_RELATIONS

21.1.2.2 Virtuele tabellen

De CMS-server bladert door de InfoObjects vanuit drie virtuele tabellen.

Virtuele tabellen

Virtuele tabel	Beschrijving
InfoObjects-tabel	Bevat InfoObjects die de eindgebruiker kan weergeven zoals: • Rapportagedocumenten • Programma's • Sneltoetsen • Mappen • Categorieën • Inboxen
Appobjectentabel	Bevat InfoObjects die documenten gebruiken zoals: • Universes • Verbindingen • Overloads
Systeemobjectentabel	Bevat InfoObjects die de BI-platform gebruikt om te functioneren zoals: • Gebruikers • Groepen • Licentiesleutels

21.1.3 Info InfoObjects

Voordat u de InfoObject-metagegevens opvraagt, moet u een duidelijk begrip hebben van de volgende concepten.

- InfoObject-eigenschappen
- Relaties tussen InfoObjects

Als u begrijpt hoe de InfoObjects worden geordend in de CMS-gegevensopslagruimte, kunt u snel en gemakkelijk in de gegevensopslagruimte bladeren en problemen oplossen die zijn gerelateerd aan de CMS-gegevensopslagruimte.

Verwante informatie

InfoObject-eigenschappen [pagina 838]
Relaties tussen InfoObjects [pagina 838]

21.1.3.1 InfoObject-eigenschappen

De volgende tabel bevat de belangrijkste eigenschappen voor InfoObjects en hun beschrijvingen

InfoObject-eigenschappen

InfoObject-eigenschappen	Beschrijving
SI_NAME	De naam van het object
SI_KIND	Het soort object
SI_OWNER	De gebruikersnaam van de eigenaar
SI_OWNERID	De gebruikers-ID van de eigenaar
SI_CHILDREN	Het aantal onderliggende elementen
SI_CUID	CUID's zijn Cluster Unique Identifiers voor de unieke identificatie van InfoObjects.
SI_UNIVERSE	De door het document gebruikte universes.(UNV)

21.1.3.2 Relaties tussen InfoObjects

De InfoObjects worden geordend in drie hiërarchieën:

- Maphiërarchie
- Hiërarchie gebruiker/gebruikersgroep
- Hiërarchie server/servergroep

De CMS- en clienttoepassingen gebruiken de maphiërarchie om door InfoObjects te navigeren.

Zie de verwante onderwerpen voor meer informatie over de relaties tussen InfoObjects.

Verwante informatie

Maphiërarchie [pagina 839]
Hoofdmap [pagina 839]

21.1.3.2.1 Maphiërarchie

De maphiërarchie is een platte lijst die is gecreëerd van een bovenliggend element van een InfoObject. Alle InfoObjects moeten een bovenliggend element hebben dat is gedefinieerd in de eigenschap SI_PARENTID.

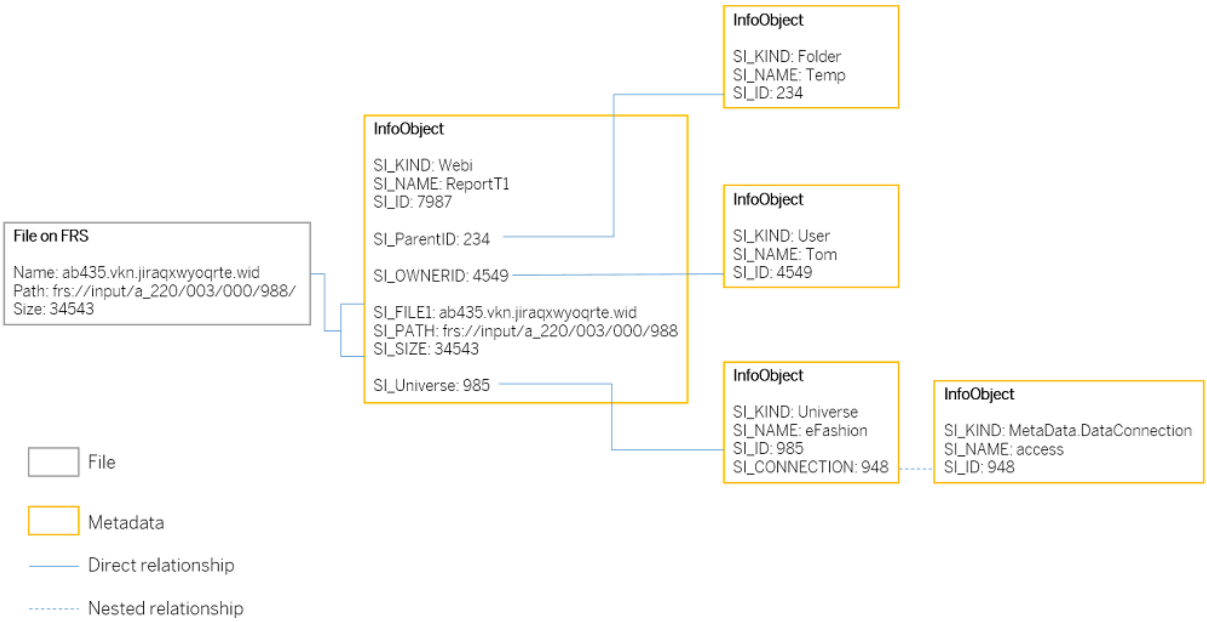
De CMS gebruikt de eigenschap bovenliggende ID om de maphiërarchie te creëren die virtueel is. De hiërarchie komt inderdaad niet overeen met de manier waarop InfoObjects worden opgeslagen in de gegevensopslagruimte.

21.1.3.2.2 Hoofdmap

De bovenste map in de hiërarchie van de CMS-gegevensopslagruimte is de map CMS-cluster. Hoofdmappen bevinden zich op een niveau onder de map CMS-cluster. Hoofdmappen zijn virtueel en komen niet overeen met iets in het bestandssysteem.

InfoObjects worden geordend in hoofdmappen voor de CMS- en clienttoepassingen om deze gemakkelijk en snel te vinden. In clienttoepassingen kan bijvoorbeeld worden genavigeerd in de verzameling InfoObjects door eerst de hoofdmap van het InfoObject en vervolgens de eigenschap van de bovenliggende ID en de eigenschappen van de onderliggende ID's te gebruiken. Hetzelfde soort InfoObjects bevindt zich gewoonlijk onder dezelfde hoofdmap.

Het volgende diagram helpt u bij het begrijpen van de relaties tussen InfoObjects.



Zoals u kunt zien, maakt de structuur van het InfoObject het mogelijk om een oneindig aantal relaties en geneste relaties te hebben.

21.2 Overzicht van CMS-rapportage

Als beheerder moet u het gebruik van het Business Intelligence-platform begrijpen en optimaliseren. De voorbeeldkit voor CMS-rapportage omvat het CMS-databasestuurprogramma waarmee u de metagegevensobjecten van de CMS-database kunt visualiseren en rapporteren. U kunt nu een universe en native rapportageclients gebruiken om query's uit te voeren op de metagegevensobjecten van de CMS-gegevensopslagdatabase. Deze metagegevensobjecten omvatten informatie over Business Intelligence-platform zoals:

- Verbindingen
- Documenten
- Planningen
- Universes
- Gebruikers

U kunt het CMS-rapportagevoorbeeld importeren; dit bevat vooraf gedefinieerde objecten waarmee u rapporten en dashboards kunt maken met behulp van de volgende toepassingen voor SAP BusinessObjects-gegevensanalyse en rapportage:

- SAP BusinessObjects Web Intelligence
- SAP Crystal Reports for Enterprise

U kunt met de voorbeeldkit voor CMS-rapportage werken voor een snelle en gemakkelijke manier om rapportage op de CMS te starten. Hieronder vindt u de belangrijkste fases voor het maken van een CMS-rapport:

- Importeer het CMS-rapportagevoorbeeld: U gebruikt Promotiebeheer in de CMC om het CMS-rapportagevoorbeeld te importeren.
- Een CMS-rapport maken: Met SAP BusinessObjects Web Intelligence kunt u een CMS-rapport maken met de CMS-voorbeelduniverse als gegevensbron.

Zie de Gerelateerde informatie voor een end-to-endprocedure met een gedetailleerder overzicht van het aanmaakproces.

Verwante informatie

Voorbeeldkit CMS-rapportage
Een CMS-rapport maken
De voorbeeldkit voor CMS-rapportage met promotiebeheer importeren [pagina 842]

21.3 CMS-databaseverbinding

U gebruikt een CMS-databasestuurprogramma om een beveiligde verbinding met de CMS-database te maken. U kunt de standaardverbinding die beschikbaar is in het CMS-rapportagevoorbeeld gebruiken of u kunt uw eigen CMS-databaseverbinding maken.

Voor de CMS-databaseverbinding moet u een relationele verbinding gebruiken. De volgende tabel beschrijft de parameters van een relationele verbinding.

Parameters voor een relationele verbinding

Parameter	Beschrijving
Verificatiemodus	De methode die wordt gebruikt om de aanmeldingsreferenties van de gebruiker te verifiëren bij toegang tot de gegevensbron: • *Opgegeven gebruikersnaam, wachtwoord en systeem-ID wijzigen*: hiermee worden de parameters *Gebruikernaam* en *Wachtwoord* gebruikt die voor de verbinding zijn gedefinieerd. U kunt de gegevensbron vanuit een lokaal systeem of een systeem op afstand benaderen. **Opmerking** Zorg ervoor dat de gebruiker de rechten heeft om de content van deze sessie te zien. • *Sessietoken gebruiken*: Gebruikt de huidige gebruikerssessie. U kunt alleen de content zien die u mag zien en waarmee u mag werken. U kunt de gegevensbron alleen vanuit een lokaal systeem benaderen. **Opmerking** Deze verificatiemodus is om beveiligingsredenen de aanbevolen keuze.
Systeem-id	De naam van de CMS indien *Verificatiemodus Opgegeven gebruikersnaam en wachtwoord gebruiken* is.
Gebruikersnaam	De gebruikersnaam waarmee u de gegevensbron kunt openen als de *Verificatiemodus Opgegeven gebruikersnaam en wachtwoord gebruiken* is.
Wachtwoord	Het wachtwoord waarmee u de gegevensbron kunt openen als de *Verificatiemodus Opgegeven gebruikersnaam en wachtwoord gebruiken* is.

21.4 Voorbeeldkit CMS-rapportage

U moet de voorbeeldkit voor CMS-rapportage gebruiken om te beginnen met het maken van documenten voor CMS-rapportage. Het CMS-databasestuurprogramma is geïntegreerd in het Business Intelligence-platform en het CMS-rapportagevoorbeeld bevindt zich op de volgende locatie:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`.

Dit voorbeeld omvat het volgende:

- Verbinding (BI platform CMS system database.cns)
- Universe (BI platform CMS system database.unx)
- Web Intelligence-voorbeelden

Meer informatie over CMS-rapportage vindt u op het SAP Community-netwerk.

Verwante informatie

De voorbeeldkit voor CMS-rapportage met promotiebeheer importeren [pagina 842]

21.4.1 De voorbeeldkit voor CMS-rapportage met promotiebeheer importeren

Zorg voordat u van start gaat ervoor dat u toegang hebt tot het CMS-rapportagevoorbeeld dat zich in de volgende locatie bevindt:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`

U gebruikt het hulpprogramma voor promotiebeheer in de Central Management Console (CMC) om het CMS-rapportagevoorbeeld te importeren.

1. Klik in de Central Management Console op *Promotiebeheer*.
2. Klik op *Importeren* > *Bestand importeren*.
3. Selecteer *Bestandssysteem*.
4. Klik op *Bestand kiezen* om het voorbeeld te selecteren.
5. Selecteer in het deelvenster *Nieuwe taak* de optie *Aanmelden bij nieuwe CMS* voor het veld *Doel*.
6. Voer de aanmeldingsparameters in en klik daarna op *Aanmelden* > *Maken*.
7. Klik in het deelvenster *Promotietaken* op het voorbeeld en selecteer daarna *Verhogen*.
8. Klik in het dialoogvenster *Verhogen* op *Verhogen*.

Als de *Verhogingsstatus* van het CMS-rapportagevoorbeeld *Geslaagd* is, hebt u het voorbeeld succesvol in uw Business Intelligence 4.2-systeem geïmporteerd. Zie het verwante onderwerp om de voorbeelduniverse voor CMS-rapportage te gebruiken.

Verwante informatie

Voorbeeldkit CMS-rapportage [pagina 842]

21.4.2 De CMS-voorbeelduniverse

De CMS-voorbeelduniverse omvat een vooraf gedefinieerde universe die algemene rapportagescenario's ondersteunt. Al naargelang uw analyse- en rapportagebehoeften kunt u de vooraf gedefinieerde universe bewerken en uitbreiden. In het venster *Query's* vindt u ook een lijst met vooraf gedefinieerde query's. Deze query's kunnen dienen als korte handleiding voor universefuncties.

In de tabel staan enkele van de meest nuttige query's met hun betekenis.

Nuttige query's om op de CMS-universe uit te voeren

Query	Beschrijving
Details voorbeeldgebruikersrelatie	Hiermee kunt u zien tot welke groep een gebruiker behoort.
Voorbeeldmappad (universe)	Hiermee kunt u de locatie van een universe zoeken.
Relaties voorbeeldplanningsinfo	Hiermee kunt u de door gebruikers geplande acties visualiseren.
QT-voorbeeldeigenschappen met filter (server)	Hiermee kunt u de eigenschappen van een InfoObject visualiseren.

21.4.3 De CMS-voorbeelduniverse uitbreiden

U kunt een gekoppelde universe maken om de CMS-voorbeelduniverse uit te breiden. Een gekoppelde universe is een .UNX-universe die een koppeling naar een toegewezen kernuniverse in de CMS bevat.

In dit geval werkt de CMS-voorbeelduniverse als een kernuniverse zodat de gekoppelde universe de gegevensverzameling en bedrijfslaag als geprefabriceerde bouwstenen kan gebruiken. Als u de gekoppelde universe hebt gemaakt kunt u de gegevensverzameling en bedrijfslaag uit de CMS-voorbeelduniverse opslaan als nieuwe bestanden, zodat ze een levenscyclus hebben die onafhankelijk is van de CMS-voorbeelduniverse.

U kunt de CMS-databaseverbinding van de CMS-voorbeelduniverse of een andere verbinding die compatibel is met de CMS-database gebruiken.

U kunt tabellen toevoegen, joins maken die de kerngegevensverzamelingtabellen koppelen aan de nieuwe en componenten toevoegen aan de bedrijfslaag op dezelfde manier als u voor elke andere universe doet. Wijzigingen in de kerncomponenten worden automatisch overgedragen naar de gekoppelde universe als deze bij de CMS wordt ingecheckt.

21.5 Een rapport op CMS maken

Met SAP BusinessObjects Web Intelligence kunt u een rapport op CMS maken met de CMS-voorbeelduniverse als gegevensbron.

1. Open Web Intelligence en klik in de werkbalk *Bestand* op het pictogram *Nieuw*.
2. Selecteer de CMS-voorbeelduniverse.

   Als u de Web Intelligence Rich Client gebruikt, klikt u op *Selecteren*.

   Nu wordt het *queryvenster* geopend.
3. Selecteer de dimensies en meetwaarden die u wilt opnemen in de query en sleep deze naar het deelvenster *Resultaatobjecten*.
4. Selecteer de objecten waarvoor u queryfilters wilt definiëren en sleep ze naar het deelvenster *Queryfilters*. Als u een snelfilter voor een object wilt maken, selecteert u het object in het deelvenster *Resultaatobjecten* en klikt u op het pictogram *Voeg een snelfilter toe* in de werkbalk *Resultaatobjecten*.
5. Klik op *Query uitvoeren*.

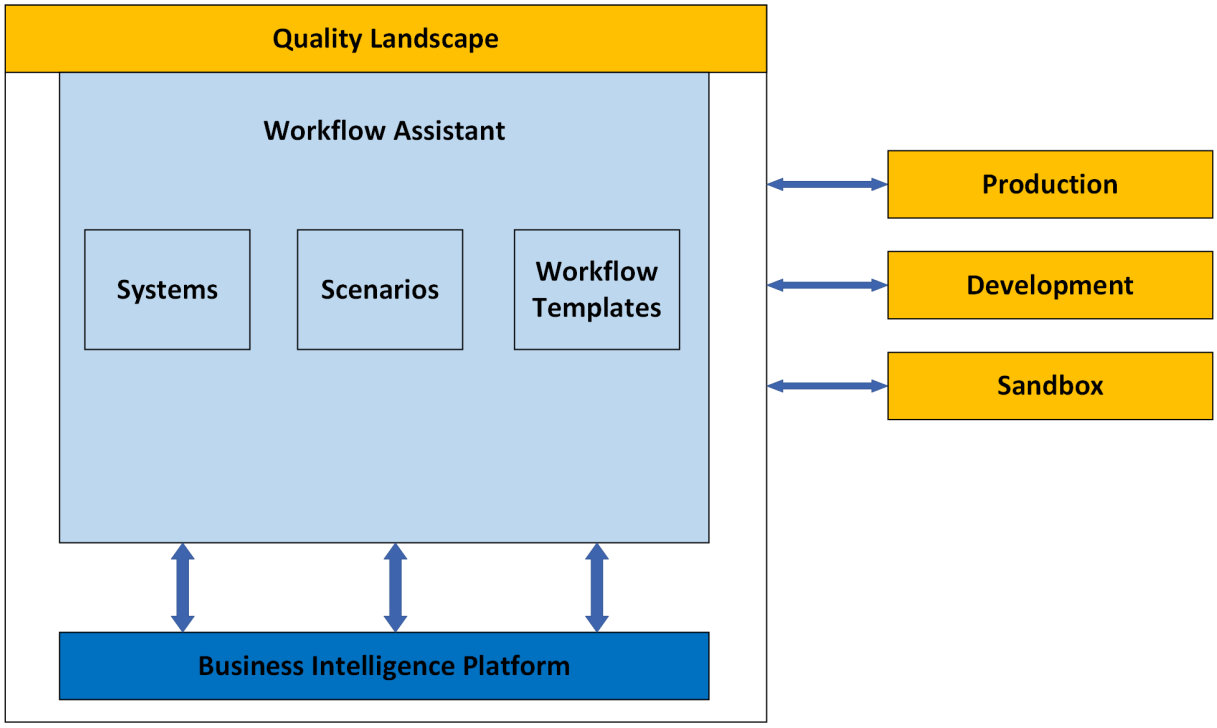
22 Workflowassistent

Het automatiseringsframework en agentservices zijn nu samengevoegd in één service met de naam Workflowassistent. Workflowassistent is een toepassing in de Central Management Console (CMC) voor het beheer van BI-systemen en de automatisering van BI-taken.

> **Opmerking**
>
> De functionaliteit van het automatiseringsframework in de BI-beheerconsole wordt nu uitgevoerd via Workflowassistent. De URL van de BI-beheerconsole `(http://<systemName>:<portNo>/BOE/BIAdminConsole)` en de berichtenwachtrijservice zijn niet meer in gebruik.

Workflowassistent geeft de inhoud weer als tabbladen: *Scenario's*, *Workflowsjablonen* en *Systemen*. Vanuit deze tabbladen kunt u inzoomen op de relevante sectie voor gedetailleerdere informatie en functies.

Workflowassistent werkt met een concept op basis van rollen, zodat gebruikers alleen toegang hebben tot de tabbladen waarvoor ze zijn geautoriseerd.



Informatie over systemen

Systeem verwijst naar een of meer BI-machines waarvoor u toegangsrechten hebt. Systeembeheer is een toepassing waarmee u centraal toegang hebt tot uw BI-landschappen en deze kunt beheren. Om gebruik te kunnen maken van de mogelijkheden van de Workflowassistent, moet u eerst uw BI-landschappen registreren met behulp van de toepassing Systeembeheer.

Informatie over de Workflowassistent

Met de Workflowassistent kunt u complexe en wederkerende BI-taken vereenvoudigen.

> **Voorbeeld**
>
> Stel dat u de volgende BI-taken in de weergegeven volgorde moet uitvoeren:
>
> 1. Aanmelden bij het het BI-platform.
> 2. De bron van bepaalde Web Intelligence-documenten van `.unv` in `.unx` wijzigen.
> 3. Deze Web Intelligence-documenten vernieuwen.
> 4. Afmelden bij het het BI-platform.

Met de Workflowassistent hoeft er minder handmatig te worden gedaan. U kunt een scenario maken met behulp van taak- en workflowsjablonen, dit scenario opslaan, uitvoeren en de resultaten weergeven.

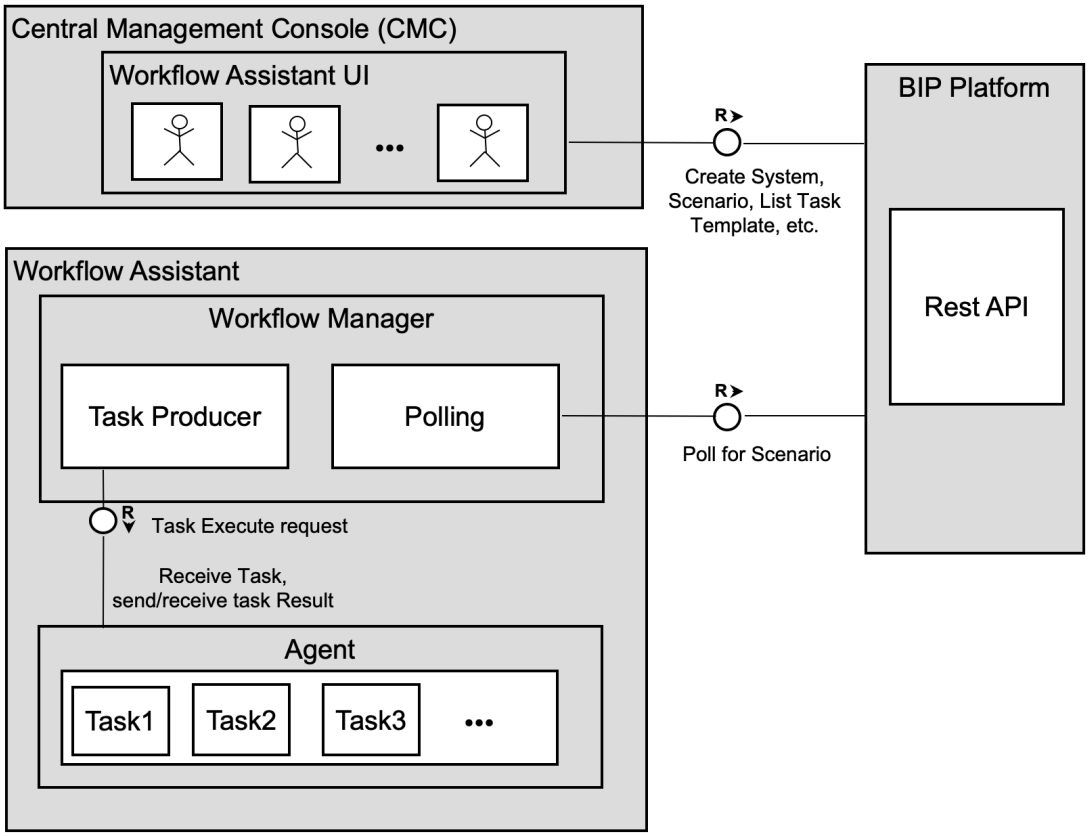
22.1 Doelgroep

Deze handleiding is bedoeld voor bepaalde gebruikers van het Business Intelligence-platform (BI) en bepaalde BI-platformontwikkelaars.

- BI-platformgebruikers die deze handleiding gebruiken moeten toegangsrechten hebben voor de Central Management Console (CMC) en de Workflowassistent. Deze gebruikers hebben de rol van beheerder of gedelegeerde beheerder.
- BI-platformontwikkelaars die deze handleiding gebruiken, moeten bekend zijn met het werken met Java SDK's en JSON-schema's voor aangepaste taken kunnen maken met behulp van de SDK voor taaksjablonen.

22.2 De architectuur

Het onderstaande diagram helpt u om de architectuur van de Workflowassistent en de onderlinge verbindingen tussen de onderdelen beter te begrijpen.



Woordenlijst met begrippen die in het bovenstaande diagram worden gebruikt:

Begrip	Definitie
Workflowassistent-UI	Een UI om workflowsjablonen en scenario's te maken die op een bepaald systeem kunnen worden uitgevoerd.
Workflowmanager	Een workflowmanager vraagt scenario's van een platform op, beheert de uitvoering van de scenario's en slaat de resultaten op.
Agent	Dit is een lichtgewicht proces waarmee de taken binnen scenario's worden uitgevoerd.

22.3 Woordenlijst

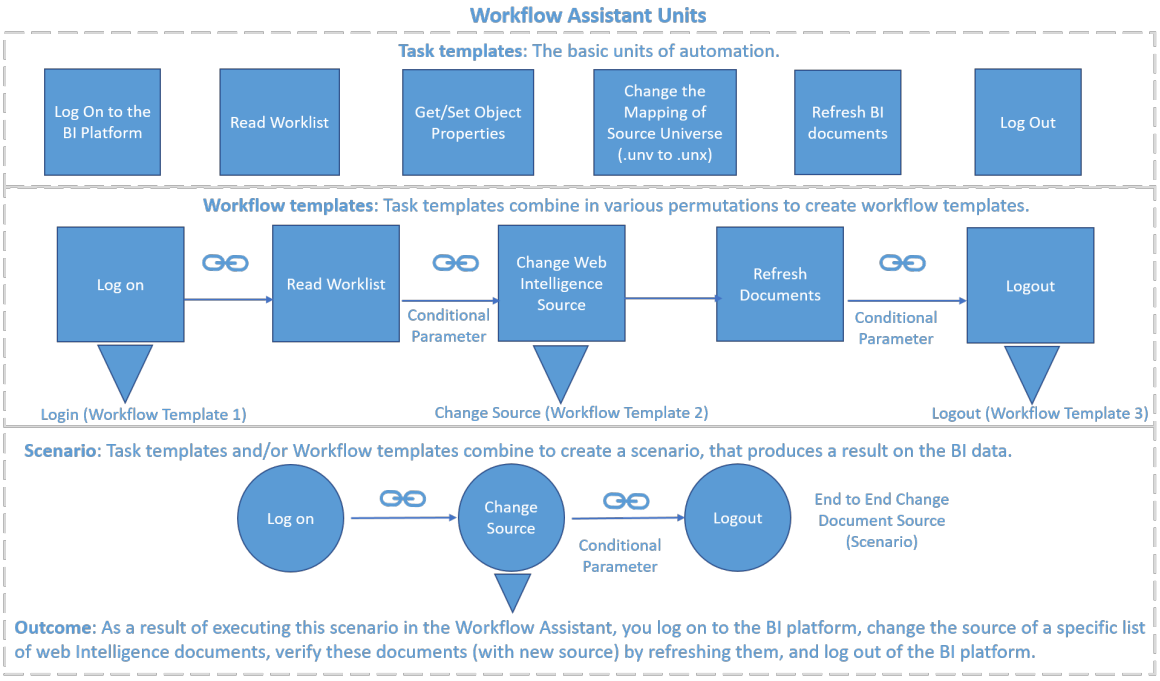
De Workflowassistent heeft zijn eigen specifieke terminologie.

Veelgebruikte begrippen in de Workflowassistent

Begrip	Definitie
Standaardtaaksjabloon	De basiseenheid van automatisering die standaard in de toepassing wordt verstrekt. Deze eenheden kunnen worden gebruikt in scenario's of workflowsjablonen. Bijvoorbeeld een eenvoudige taak als aanmelden bij het BI-platform, vernieuwen van BI-documenten, gegevens lezen, de toewijzing van universe- of Web Intelligence-brondocumenten wijzigen (van unv in unx), het toevoegen van gebruikers aan uw landschap of afmelden.
Aangepaste taaksjabloon	Een taaksjabloon (basiseenheid van automatisering) die door ontwikkelaars wordt gemaakt voor specifieke vereisten. **⚠ Beperking** U kunt een aangepaste taaksjabloon niet maken via de gebruikersinterface van Workflowassistent. Hiervoor is de SDK voor taaksjablonen vereist.
Workflowsjabloon	Een logische groep taaksjablonen die in de vereiste volgorde is gerangschikt om de uitkomst van een workflow te bereiken.
Standaardworkflowsjabloon	Workflowsjablonen die kant-en-klaar in de Workflowassistent worden verstrekt. Beheerders kunnen standaardworkflowsjablonen direct gebruiken bij het maken van scenario's voor hun diverse BI-automatiseringsvereisten.
Aangepaste workflowsjabloon	Een workflowsjabloon die door beheerders voor hun eigen speciale vereisten worden gemaakt. Deze wordt in de Workflowassistent gemaakt door standaard- of aangepaste taaksjablonen te groeperen.
Scenario	Een uitvoerbare entiteit die wordt gemaakt met behulp van taaksjablonen of workflowsjablonen in de vereiste volgorde.

Begrip	Definitie
Voorwaardelijke parameter	De schakel tussen taaksjablonen of workflowsjablonen, die de beheerstroom aanstuurt, is gebaseerd op een van de volgende voorwaarden: • Doorgaan (standaardwaarde) • Als geslaagd • Als mislukt • Als gedeeltelijk geslaagd **Opmerking** Met een voorwaardelijke parameter kunt u ook een *"Vertragingstijd"*(in seconden) instellen om ervoor te zorgen dat de volgende taak in het scenario pas na een bepaalde tijd start als de vorige taakuitvoering is voltooid. **→ Onthouden** De Workflowassistent gebruikt de voorwaardelijke parameterwaarde: 'Doorgaan', alleen als de vorige taak is voltooid met een van deze drie statuswaarden: 'Geslaagd', 'Gedeeltelijk geslaagd' of 'Mislukt'. Als de vorige taak de status 'Fout' of 'Niet uitgevoerd' heeft, wordt de status van het volgende knooppunt automatisch ingesteld op 'Niet uitgevoerd'.

Deze illustratie helpt u om de onderlinge verbinding tussen enkele van de bovenstaande begrippen beter te begrijpen:



22.4 Informatie over installeren en bijwerken

Afhankelijk van of u een nieuwe installatie uitvoert of een bestaande installatie bijwerkt, is uw toegang tot back-endfunctionaliteit mogelijk anders.

Wanneer u een **nieuwe installatie** van SAP BusinessObjects BI platform (standaardinstallatie) uitvoert, krijgt u volledige toegang tot de Workflowassistent op de computers waarop u het BI-platform hebt geïnstalleerd en geconfigureerd. Dit omvat toegang tot de Workflowassistent-toepassing in de CMC en de back-endfunctionaliteit (Workflowassistent-service).

Wanneer u echter een update van het BI-platform SP5 of hoger naar 4.3 uitvoert, is de volledige functionaliteit van Workflowassistent beschikbaar, maar moet u nog wel de SAP Note doornemen die onder Beperkingen wordt vermeld. Voer na het installeren van de update de installatieworkflow 'Wijzigen' uit om de back-endservices te verkrijgen. Raadpleeg de *Updatehandleiding voor ondersteuningspakketten* op de pagina SAP Business Intelligence-platform van de Help Portal voor meer informatie over het wijzigen van de installatie.

> **Opmerking**
>
> Workflowassistent maakt deel uit van het BOE.war-bestand. Nadat u een update van het BI-platform versie 4.2 SP4 of lager naar versie 4.2 SP5 en hoger hebt uitgevoerd, wordt de webtoepassing alleen geïmplementeerd als de functionaliteit *Java-webtoepassingen* tijdens de installatie van de bestaande versie was geselecteerd.

> ⚠ Let op
>
> U moet de Workflowassistent niet installeren op meerde computers binnen systemen, aangezien clustering van de Workflowassistent niet wordt ondersteund.

Workflowassistent biedt nu ondersteuning voor de besturingssystemen AIX en Solaris.

> ⚠ Beperking
>
> - Wanneer u voor AIX- en Solaris platformen BI versie 4.3 op 4.2 SP05 of een hogere versie installeert, wordt Workflowassistent standaard geïnstalleerd. Er is echter een extra handeling nodig om de back-endservices te verkrijgen.
> - Wanneer u een update van het BI-platform 4.2 SP4 of lager naar 4.2 SP5 of hoger uitvoert, ziet u dat sommige mappen niet in Workflowassistent worden vermeld. Zie 2882649 voor meer informatie.

22.5 De Workflowassistent configureren

Wanneer u de Workflowassistent installeert als onderdeel van de installatie van het BI-platform, krijgt u de service standaard tijdens het instellen.

U kunt vervolgens vertrouwde verificatie configureren om de Workflowassistent te gaan gebruiken.

22.5.1 Basisconfiguratie

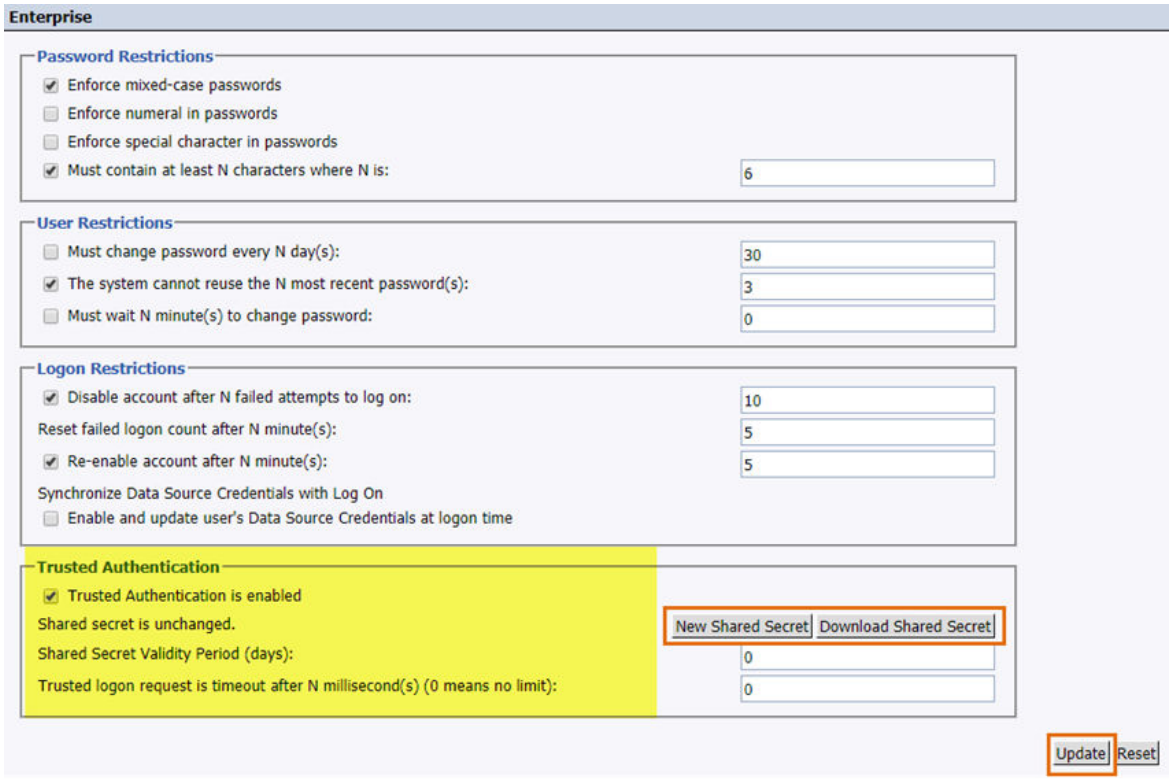
22.5.1.1 Enterprise-verificatie configureren voor Workflowassistent

U hebt de Workflowassistent geïnstalleerd als onderdeel van de installatie van het BI-platform.

Volg de onderstaande procedure om vertrouwde (Enterprise-)verificatie te configureren voor de Workflowassistent:

1. Meld u aan bij de Central Management Console (CMC) door verbinding te maken met de CMS van het hoofdknooppunt.
2. Selecteer *Verificatie* in de vervolgkeuzelijst en dubbelklik op *Enterprise*.

Het dialoogvenster 'Enterprise' wordt weergegeven zoals hieronder:



3. Zorg dat in de sectie 'Vertrouwde verificatie' *Vertrouwde verificatie* is ingeschakeld.
4. Kies *Nieuw gedeeld geheim*.
   De sleutel voor het gedeelde geheim wordt gegenereerd.
5. Kies *Gedeeld geheim downloaden*.
6. Selecteer *Bijwerken*.
7. Sla de sleutel van het gegenereerde gedeelde geheim (TrustedPrincipal.conf) op:
   a. In Windows in `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0\win64_x64/`.
   b. In Linux in `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/linux_x64/`.
   c. In AIX in `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/aix_rs6000_64/`.
   d. In Solaris in `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/solaris_sparcv9/`.

> **Opmerking**
>
> Zie het onderwerp Vertrouwde verificatie inschakelen [pagina 256] voor meer informatie over het maken van vertrouwde verificatiecertifcaten met verschillende opties.

22.5.1.2 Een standaardgebruiker maken voor de Workflowassistent-back-endservice

1. Maak een nieuwe gebruiker in de Workflowassistent met de naam **WAGebruiker**.

2. Wijs de juiste rechten aan door naar de map `Workflow Assistant` te gaan en het recht Volledig beheer toe te wijzen aan de account **WAGebruiker**.

   De Workflowassistent-back-endservice begint de account **WAGebruiker** te gebruiken.

   Als er geen **WAGebruiker**-account is, gebruikt Workflowassistent de account *Administrator*.

   > ⓘ Opmerking
   >
   > De nieuwe gebruiker hoeft geen deel uit te maken van de gebruikersgroep *Administrator*.

22.5.1.3 De Workflowassistent-service starten

Dit onderwerp biedt instructies voor het starten van de *Workflowassistent-service*.

1. Configureer Enterprise-verificatie voor de Workflowassistent-service. Raadpleeg Enterprise-verificatie configureren voor Workflowassistent [pagina 851] voor meer informatie.
2. Ga als volgt te werk om de *Workflowassistent-service* te starten:
   a. Start in Windows *Central Configuration Manager* (CCM) en start de *Workflowassistent-service*.
   b. Ga in Unix naar `<INSTALLDIR>/AdminConsole/WorkflowAssistant/startWfAssistant.sh`.

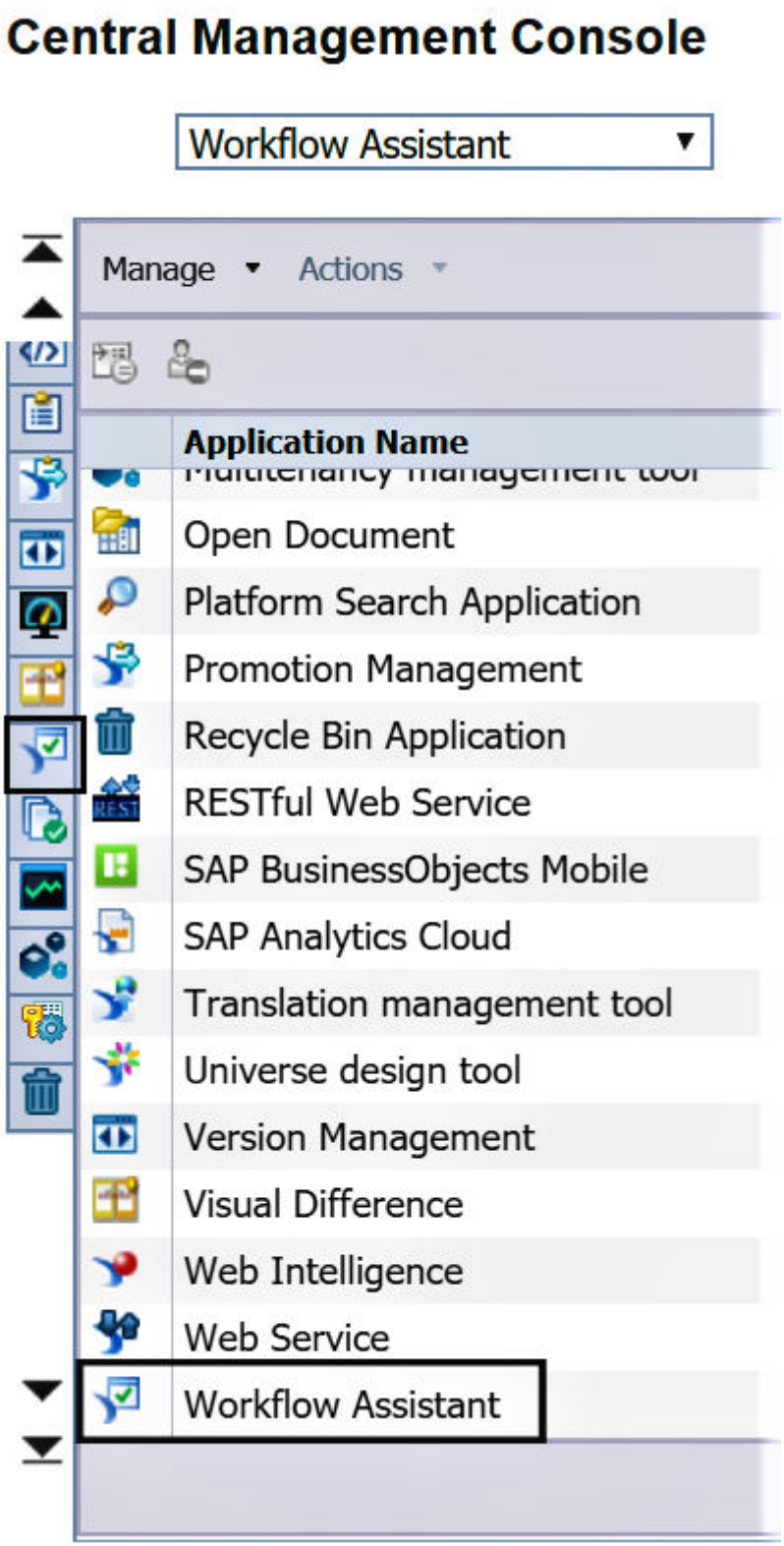
   U bent er nu klaar voor om de *Workflowassistent* te gebruiken en scenario's uit te voeren.

   > ⓘ Opmerking
   >
   > Om er zeker van te zijn dat Workflowassistent is gestart,
   > controleert u de inhoud van het bestand `message.properties` in `<BOE-installatiemap>\AdminConsole\WorkflowAssistant\service-logs`. De inhoud van `message.properties` moet als volgt zijn:
   >
   > ```
   > STATUS_WFM=success
   > MESSAGE_AGENT=Agent - Started\!\!
   > STATUS_AGENT=success
   > MESSAGE_WFM=Workflow Assistant - Started\!\!
   > ```

22.6 Workflowassistent-rechten beheren via de Central Management Console

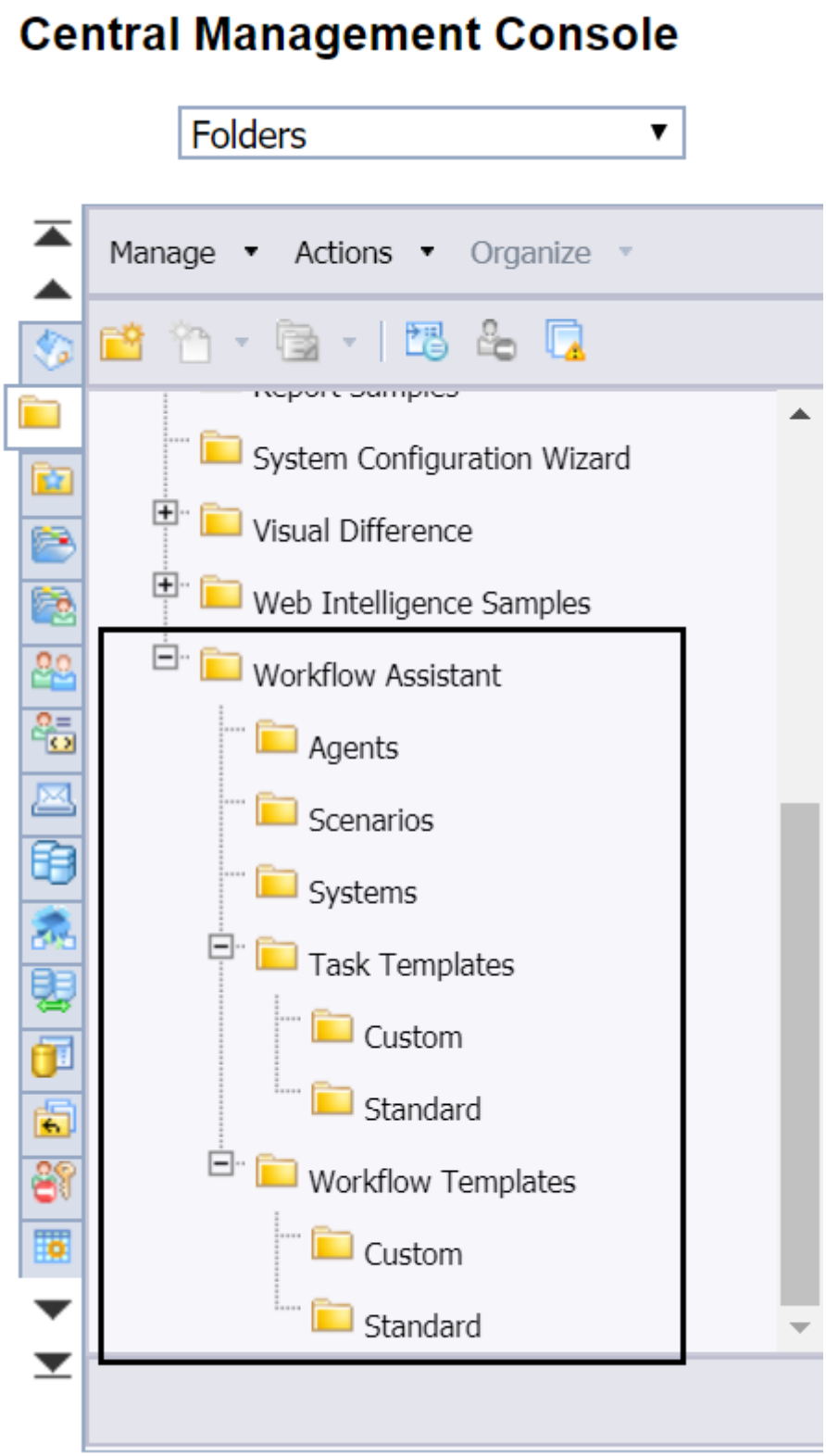
U beheert de beveiliging voor de Workflowassistent via de Central Management Console.

Workflowassistent wordt vermeld onder *Toepassingen* van de *Central Management Console*.



U kunt de toegangsrechten en algemene beveiligingsinstellingen voor de volgende entiteiten beheren in de Workflowassisent:

- Systemen
- Scenario's
- Taaksjablonen
- Workflowsjablonen



Zie Beveiligingsinstellingen voor objecten beheren in de CMC voor informatie over het beheren van beveiligingsinstellingen voor objecten in de CMC.

> **Opmerking**
>
> - U kunt de toegang tot een functionaliteit in Workflowassistent, zoals *Systemen*, *Scenario's*, *Taaksjablonen* en *Workflowsjablonen*, beheren door rechten aan de gebruiker toe te wijzen op map- of objectniveau. Ontbrekende rechten hebben geen gevolgen voor de gebruikersinterface. Dit betekent dat een gebruiker het recht *Objecten toevoegen aan de map* in de map *Scenario* moet hebben om een scenario te maken.
> - Bijvoorbeeld: een gebruiker ziet een optie om een scenario te maken in Workflowassistent, ook al heeft deze geen rechten in de map *Scenario* in CMC. Als de gebruiker nog steeds probeert om een scenario te maken en op te slaan in de map *Scenario*, wordt er een foutbericht geretourneerd.

Toepassingsrechten beheren

Met de juiste toepassingsspecifieke rechten kunt u de volgende taken in Workflowassistent weigeren of uitvoeren:

- Als u *Taaksjabloon maken* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten toevoegen aan de map*.
- Als u *Workflowsjabloon maken* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten toevoegen aan de map*.
- Als u *Scenario maken* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten toevoegen aan de map*.
- Als u *Taaksjabloon bewerken* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten bewerken*.
- Als u *Taaksjabloon bewerken die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten bewerken die het eigendom zijn van de gebruiker*.
- Als u *Workflowsjabloon bewerken* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten bewerken*.
- Als u *Workflowsjabloon bewerken die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten bewerken die het eigendom zijn van de gebruiker*.
- Als u *Scenario bewerken* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten bewerken*.
- Als u *Scenario bewerken dat het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten bewerken die het eigendom zijn van de gebruiker*.
- Als u *Taaksjabloon weergeven* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten weergeven*.
- Als u *Taaksjabloon weergeven die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten weergeven die het eigendom zijn van de gebruiker*.
- Als u *Workflowsjabloon weergeven* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten weergeven*.
- Als u *Workflowsjabloon weergeven die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten weergeven die het eigendom zijn van de gebruiker*.
- Als u *Scenario weergeven* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten weergeven*.
- Als u *Scenario weergeven dat het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten weergeven die het eigendom zijn van de gebruiker*.

- Als u *Taaksjabloon verwijderen* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten verwijderen*.
- Als u *Taaksjabloon verwijderen die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Taaksjabloon en weigert u *Objecten verwijderen die het eigendom zijn van de gebruiker*.
- Als u *Workflowsjabloon verwijderen* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten verwijderen*.
- Als u *Workflowsjabloon verwijderen die het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Workflowsjabloon en weigert u *Objecten verwijderen die het eigendom zijn van de gebruiker*.
- Als u *Scenario verwijderen* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten verwijderen*.
- Als u *Scenario verwijderen dat het eigendom is van de gebruiker* wilt weigeren, gaat u naar de map Scenario en weigert u *Objecten verwijderen die het eigendom zijn van de gebruiker*.
- Als u *Scenario uitvoeren voor alle combinaties* wilt weigeren, gaat u naar het betreffende scenario en weigert u *Objecten toevoegen aan de map*.
- Als u *Scenario uitvoeren dat het eigendom is van de gebruiker voor alle combinaties* wilt weigeren, gaat u naar het betreffende scenario en weigert u *Objecten toevoegen aan mappen waarvan de gebruiker eigenaar is*.
- Als u *Landschap maken* wilt weigeren, gaat u naar de map Landschap en weigert u *Objecten toevoegen aan de map*.
- Als u *Landschap bewerken en weergeven* wilt weigeren, gaat u naar de map Landschap en weigert u *Objecten bewerken* en *Objecten weergeven*.
- Als u *Landschap verwijderen* wilt weigeren, gaat u naar de map Landschap en weigert u *Objecten verwijderen*.
- Als u *Gebruikersreferenties toevoegen aan landschap* wilt weigeren, gaat u naar de map Landschap en weigert u *Objecten toevoegen aan de map*.

> ⓘ Opmerking
>
> Alle bovenstaande rechten kunnen worden toegepast op afzonderlijke taaksjablonen, workflowsjablonen en scenario's.

22.7 Werken met de Workflowassistent

De Workflowassistent is een toepassing in de CMC waarmee u herhalende en complexe BI-beheertaken kunt automatiseren. In de volgende secties gaat u leren hoe u de BI-beheertaken kunt automatiseren.

22.7.1 Standaardtaaksjablonen

Standaardtaaksjablonen zijn ingebouwd (kant-en-klaar geleverd) in de Workflowassistent. Wanneer u scenario's of workflowsjablonen maakt, kunt u deze taaksjabonen gebruiken.

Standaardtaaksjabloon	Beschrijving
Aanmelden	Hiermee wordt een sessie met de doelserver van het BI-platform tot stand gebracht.
Documenten vernieuwen	Hiermee wordt de lijst met beschikbare documenten geopend en vernieuwd via de bewerking `<Nu plannen>`. **Opmerking** Voor documenten met aanwijzingen moeten de standaardwaarden worden opgegeven in de documenten vóór de uitvoering.
Bron Web Intelligence wijzigen	Hiermee wordt de toewijzing van de bronuniverse voor uw lijst met documenten van .unv in .unx, .unx in .unx, of .unv in .bex gewijzigd.
Gebruiker en gebruikersgroep toevoegen/ verwijderen	Hiermee worden gebruikers en gebruikersgroepen toegevoegd aan of verwijderd uit het BI-landschap. **Opmerking** Deze taaksjabloon komt overeen met de `<importfunctionaliteit>` op het BI-platform. Zie het onderwerp Gebruikers of gebruikersgroepen bulksgewijs toevoegen voor meer informatie over de importfunctionaliteit.
Eigenschappen ophalen	Hiermee worden de waarden van bepaalde eigenschappen voor de doorzochte InfoObjects opgehaald.
Eigenschappen instellen	Hiermee worden de waarden van bepaalde eigenschappen voor de gegeven InfoObjects in de CMS ingesteld.
Werklijst lezen	Hiermee worden CSV-bestanden als invoer gelezen en worden de kommagescheiden waarden geretourneerd, die door daaropvolgende taken kunnen worden gebruikt. Gebruik deze taaksjabloon als een groot aantal waarden (bulkgegevens) moet worden gebruikt door workflowsjablonen in uw scenario en het niet haalbaar is om de waarden handmatig in te voeren via het invoervenster van Workflowassistent.
Query uitvoeren op werklijst	Hiermee wordt een query uitgevoerd op de CMS-tabellen en wordt de uitvoer geleverd in CSV-indeling.
Uitvoer opslaan	Hiermee worden de waarden die zijn verkregen van de *Uitvoerparameter* van een taak opgeslagen in de CMS.
Servereigenschappen instellen	Hiermee worden de waarden van bepaalde eigenschappen voor de gegeven server(s) ingesteld.
Afmelden	Hiermee wordt de taaksessie met de doelserver van het BI-platform beëindigd.

22.7.1.1 Aanmelden

Parameters voor Taaksjabloon voor aanmelding

Invoerparameters

Naam	Type	Beschrijving
Systeem	Tekenreeks	Naam van het geregistreerde landschap in de Workflowassistent

22.7.1.2 Documenten vernieuwen

Parameters voor Documenten vernieuwen

Invoerparameter

Naam	Type	Beschrijving
*Documenten	CSV	Document-ID's (ID/CUID) voor documenten die moeten worden vernieuwd. Een gebruiker kan ook documenten kiezen in de Gegevensopslagverkenner met de invoerhulp. CSV-indeling: ID of CUID

Uitvoerparameters

Naam	Type	Beschrijving
SuccessfullyRefreshedDocuments	CSV	Documenten die met succes zijn vernieuwd. CSV-indeling: ID, CUID
UnsuccessfullyRefreshedDocuments	CSV	Documenten die niet met succes zijn vernieuwd. CSV-indeling: ID, CUID
Alles	CSV	Lijst met verwerkte documenten. CSV-indeling: ID, CUID

22.7.1.3 Bron Web Intelligence wijzigen

Parameters voor Bron Web Intelligence wijzigen

Invoerparameters

Naam	Type	Beschrijving
*Document	CSV	De CUID van het Web Intelligence-document opgeven waarvoor u de UNV door UNX, UNX door UNX of UNV door BEx wilt vervangen. Een gebruiker kan ook documenten kiezen uit de Gegevensopslagverkenner via de invoerhulp of door de uitvoer van een taak aan een andere taak toe te wijzen. CSV-indeling: ID of CUID
*UniverseMapping	CSV	Universes (UNV, UNX, BEx) toewijzen op basis van ID of CUID. Een gebruiker kan de universes ook toewijzen via het scherm Toewijzing van universes in de invoerhulp. CSV-indeling (voor UNV-UNX): unv_cuid, unx_cuid of unv_id, unx_id CSV-indeling (voor UNX-UNX): src_cuid,dest_cuid,type CSV-indeling (voor UNV-BEx): src_cuid,dest_cuid,type,technical_name
Documentactie	Tekenreeks	Als u de bron wilt wijzigen zonder het document op te slaan, wijst u de volgende waarde toe: 'Testen' Als u de bron wilt wijzigen en het document wilt opslaan, wijst u de volgende waarde toe: 'Wijzigen'

Uitvoerparameters

Naam	Type	Beschrijving
Geslaagd	CSV	Documenten waarvoor de bron met succes is gewijzigd. CSV-indeling: ID, CUID
Mislukt	CSV	Documenten waarvoor het wijzigen van de bron is mislukt. CSV-indeling: ID, CUID
Alles	CSV	Lijst met invoerdocumenten. CSV-indeling: ID, CUID

Beperking

- Alleen de UNV die is gemaakt in de BEx-query kan worden vervangen door een andere BEx-query.
- BEx-query's met aanwijzingen worden niet ondersteund.
- Er vindt alleen toewijzing plaats als universeobjecten van een soortgelijk type zijn en een dichtstbijzijnde naam met BEx-queryobjecten hebben.
- Universeobjecten die met labels zijn gemaakt, worden niet ondersteund.

22.7.1.4 Gebruiker en gebruikersgroep toevoegen/verwijderen

Parameters voor Gebruiker en gebruikersgroep toevoegen/verwijderen

Invoerparameters

Naam	Type	Beschrijving

*Gegevens	CSV	Gebruikersspecifieke gegevens.
		
		Zie de onderstaande CSV-voorbeeldgegevens. Zie het onderwerp *Gebruikers of gebruikersgroepen bulksgewijs toevoegen* in de *Beheerdershandleiding voor Business Intelligence-platform* voor meer informatie over CSV-gegevens.
		
		`command,group,user,fullname,password,mail,profileName,profileValue`
		`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue`

> **Opmerking**
>
> U kunt ook een CSV-bestand zonder een CSV-koptekst maken en als invoer voor uw scenario gebruiken.
>
> Het in het CSV-bestand gekozen wachtwoord moet voldoen aan het wachtwoordbeleid.

> **→ Tip**
>
> U kunt opeenvolgende komma's gebruiken om een invoerveld over te slaan.

22.7.1.5 Eigenschappen ophalen

Parameters voor Eigenschappen ophalen

Invoerparameters

Naam	Type	Beschrijving
*InfoObject	CSV	CSV-waarden voor InfoObjects. Het voorvoegsel 'si_' moet niet worden opgegeven voor de eigenschappen. CSV-indeling: ID of CUID

Naam	Type	Beschrijving
*Eigenschap	CSV	CSV-waarden of -eigenschappen. Het voorvoegsel 'si_' moet niet worden opgegeven voor de eigenschappen. Voor InfoObjects van een gebruiker is de ondersteunde eigenschap 'property;data'.

Uitvoerparameters

Naam	Type	Beschrijving
Geslaagd	CSV	Lijst met InfoObjects waarvoor de eigenschapswaarde met succes is gevonden of toegewezen. CSV-indeling: ID of <gezochte eigenschap>
Mislukt	CSV	Lijst met InfoObjects waarvoor de eigenschapswaarde niet met succes is gevonden of toegewezen. CSV-indeling: ID, CUID
Alles	CSV	Lijst met alle verwerkte InfoObjects. CSV-indeling: ID, CUID

22.7.1.6 Eigenschappen instellen

Parameters voor Eigenschappen instellen

Invoerparameters

Naam	Type	Beschrijving
*InfoObject	CSV	CSV-waarden voor InfoObjects. Het voorvoegsel 'si_' moet niet worden opgegeven voor de eigenschappen. CSV-indeling: ID of CUID

Naam	Type	Beschrijving
*Eigenschap	CSV	CSV-waarden of -eigenschappen. Voor InfoObjects van een gebruiker is de ondersteunde eigenschap 'property;data'.

Uitvoerparameters

Naam	Type	Beschrijving
Geslaagd	CSV	Lijst met InfoObjects waarvoor de eigenschapswaarde met succes is opgehaald of ingesteld. CSV-indeling: ID of <gezochte eigenschap>
Mislukt	CSV	Lijst met InfoObjects waarvoor de eigenschapswaarde niet met succes is opgehaald of ingesteld. CSV-indeling: ID, CUID
Alles	CSV	Lijst met alle verwerkte InfoObjects. CSV-indeling: ID, CUID

22.7.1.7 Servereigenschappen instellen

Parameters voor Servereigenschappen instellen

Invoerparameters

Naam	Type	Beschrijving
*Server	CSV	ID's (ID/CUID) voor servers die moeten worden gewijzigd. Een gebruiker kan ook servers kiezen in de Gegevensopslagverkenner met de invoerhulp. CSV-indeling: ID of CUID

Naam	Type	Beschrijving
*Eigenschap	CSV	CSV-waarden met eigenschap en waarde. Bijvoorbeeld: `hostname;new value`. Ondersteunde eigenschappen: hostname

Uitvoerparameters

Naam	Type	Beschrijving
Geslaagd	CSV	Lijst met servers waarvoor de eigenschapswaarde met succes is ingesteld. CSV-indeling: ID
Mislukt	CSV	Lijst met servers waarvoor de eigenschapswaarde niet met succes ingesteld. CSV-indeling: ID
Alles	CSV	Lijst met alle verwerkte verwerkt. CSV-indeling: ID

22.7.1.8 Werklijst lezen

Parameters voor Werklijst lezen

Invoerparameters

Naam	Type	Beschrijving
*Bestand	CSV	CSV-bestand met de voor lezen vereiste gegevens. Een gebruiker kan ook een CSV-bestand kiezen in de Gegevensopslagverkenner met de invoerhulp. CSV-indeling: <Header1>, <Header2>, ..<HeaderN> **Opmerking** Zie Werken met CSV-gegevens [pagina 873] voor meer informatie over de gegevensindelingen en scheidingstekens in CSV.

Uitvoerparameters

Naam	Type	Beschrijving
Waarden	CSV	De zoeklijst die wordt gelezen uit het invoerbestand en wordt geretourneerd in een kommagescheiden indeling.

22.7.1.9 Uitvoer opslaan

Parameters voor de taak Uitvoer opslaan

Invoerparameters

Naam	Type	Beschrijving
*Parameter	CSV	Wijs de uitvoer uit de vorige taak toe.
*Bestandsnaam	Tekenreeks	Geef de bestandsnaam op om de uitvoer op te slaan.
*Doelmap kiezen	Tekenreeks	Selecteer de map waarin het bestand moet worden opgeslagen.

Naam	Type	Beschrijving
*Opties voor opslaan	Tekenreeks	Als u een bestand met dezelfde naam wilt overschrijven, kiest u de waarde: *Overschrijven*. Als u de naam van een bestand met dezelfde naam wilt wijzigen met achtervoegsel _1, _2, enzovoort, kiest u de waarde: *Naam wijzigen*

> **Opmerking**
>
> **Uitvoerparameter:**
>
> De uitvoer wordt verkregen in een bestand in CMS. Daarom is er geen parameter beschikbaar voor gebruik.

22.7.1.10 Afmelden

Parameters voor Afmeldingstaak

Invoerparameter

Naam	Type	Beschrijving
SessionToken	Tekenreeks	Sessietoken (gegenereerd vanwege de aanmelding)

22.7.2 Informatie over standaardworkflowsjablonen

Standaardworkflowsjablonen zijn ingebouwd (kant-en-klaar geleverd) in de Workflowassistent. Wanneer u scenario's maakt, kunt u deze workflowsjabonen gebruiken.

Beschikbare standaardworkflowsjablonen in de Workflowassistent

Naam sjabloon	Beschrijving
Aanmelden	Hiermee wordt een sessie met de doelserver van het BI-platform tot stand gebracht.
Documenten vernieuwen	Hiermee wordt de opgegeven lijst met Web Intelligence-documenten vernieuwd.

Naam sjabloon	Beschrijving
Eigendom van document wijzigen	Hiermee wordt een query uitgevoerd naar de eigenaar van het document en wordt dezelfde eigenaar aan een ander document toegewezen.
Type licentie van gebruiker wijzigen	Hiermee wordt een query uitgevoerd naar een lijst met gebruikers op basis van gebruikersspecifieke voorwaarden en wordt het licentietype gewijzigd.
Bron Web Intelligence wijzigen en documenten controleren	Hiermee wordt de toewijzing van bronuniverse gewijzigd van .unv in .unx, .unx in .unx of .unv in .bex en worden de documenten voor Web Intelligence-documenten bulksgewijs gevalideerd.
Gebruikers toevoegen/verwijderen	Hiermee kan een beheerder gebruikers en groepen toevoegen of verwijderen.
Afmelden	Hiermee wordt de taaksessie met de doelserver van het BI-platform beëindigd.

22.7.3 Informatie over aangepaste taaksjablonen

U kunt de standaardtaaksjablonen in de Workflowassistent gebruiken om workflowsjablonen te ontwerpen en scenario's uit te voeren. Als de standaardsjablonen niet voldoende aan uw behoeften voldoen, kunt u uw eigen taaksjabloon en invoegtoepassing ontwikkelen voor de Workflowassistent.

Maak uw eigen aangepaste taaksjabloon met de SDK voor aangepaste taaksjablonen die ontwikkelaars een API biedt voor het implementeren van nieuwe taaksjablonen. Zie Aangepaste taaksjablonen maken in het BI-automatiseringsframework voor meer informatie.

22.7.4 Workflowsjablonen beheren

U kunt aangepaste workflowsjablonen maken, bewerken en verwijderen in de Workflowassistent.

22.7.4.1 Aangepaste workflowsjablonen maken

U maakt aangepaste workflowsjablonen met behulp van standaard- of aangepaste taaksjablonen.

1. Kies op de startpagina de optie *Workflowassistent*.
2. Kies op de pagina *Workflowassistent* het tabblad *Workflowsjablonen*.
3. Kies het pictogram + (*Toevoegen*) rechtsboven van *Workflowsjablonen*.
4. Kies op het tekenpapier *Workflowsjabloon maken* het pictogram > (*Uitvouwen*) links van de taaksjablooncategorieën *Standaard* en *Aangepast* in het linkervenster.

5. Sleep de gewenste taaksjablonen naar het tekenpapier rechts op de pagina.
6. Geef uw neergezette taaksjabloon een nieuwe naam op het tekenpapier.
7. (Optioneel) Kies het pictogram (*Koppeling*) dat tussen twee taaksjablonen verschijnt en selecteer de benodigde waarde voor voorwaardelijke parameters in de lijst die op het scherm verschijnt.

   Hier kunt u ook de benodigde `<Vertragingstijd>` (in seconden) invoeren.
8. (Optioneel) Stel waarden in voor invoerparameters. Deze worden als standaardwaarden gebruikt als de workflowsjabloon in een scenario wordt gebruikt.
9. Kies *Opslaan*.
10. Voer in het dialoogvenster *Workflowsjabloon* een naam (verplicht) in voor uw workflowsjabloon en voeg indien nodig een beschrijving toe.
11. Kies *Opslaan* in het dialoogvenster *Workflowsjabloon opslaan*.

    De nieuwe workflowsjabloon wordt weergegeven in de view *Workflowsjablonen* van de Workflowassistent.

> **Opmerking**
>
> Wijzigingen aan de bestaande workflowsjablonen hebben geen invloed op de bestaande scenario's.

22.7.4.2 Aangepaste workflowsjablonen bewerken

U bewerkt aangepaste workflowsjablonen in de Workflowassistent.

1. Kies op het tabblad *Workflowsjablonen* van de Workflowassistent (*Meer*) en selecteer *Bewerken*.
2. Bewerk op het scherm *Workflowsjabloon bewerken* de workflowsjabloon door taaksjablonen toe te voegen of te verwijderen, waarden voor de invoerparameters de wijzigen of door de voorwaardelijke parameters tussen taaksjablonen te wijzigen.
3. Kies *Opslaan als*.
4. Wijzig in het dialoogvenster *Workflowsjabloon opslaan* desgewenst de naam van de workflowsjabloon.
5. Selecteer *Opslaan*.

   De wijzigingen in de workflowsjabloon worden opgeslagen en u keert terug naar de startpagina van de Workflowassistent.

22.7.4.3 Aangepaste workflowsjablonen verwijderen

U verwijdert aangepaste workflowsjablonen in de Workflowassistent.

1. Kies op het tabblad *Workflowsjablonen* van de Workflowassistent (*Meer*) en selecteer *Verwijderen*.
2. Kies *Verwijderen* in de waarschuwing die wordt weergegeven.

   De verwijderde workflowsjabloon wordt niet meer weergegeven op het tabblad *Workflowsjablonen* van de Workflowassistent.

22.7.5 Scenario's beheren en resultaten weergeven

U maakt een scenario door taaksjablonen en workflowsjablonen met elkaar te verbinden. U kunt scenario's beheren en resultaten weergeven in de Workflowassistent.

22.7.5.1 Scenario's maken

In dit onderwerp wordt uitgelegd hoe u scenario's kunt maken in de Workflowassistent

1. Kies op de startpagina van de CMC de optie *Workflowassistent*.

   Op de pagina die op het scherm verschijnt, worden de beschikbare scenario's weergegeven.
2. Klik op het +-teken (*Map of scenario maken*) en selecteer *Scenario*.
3. Kies op de pagina *Scenario maken* het pictogram > (*Uitvouwen*) links van de taaksjablooncategorieën *Standaard* en *Aangepast* in het linkervenster.

   > ⓘ Opmerking
   >
   > U kunt de beschrijving van de taak bekijken door de muis op de naam van de taaksjabloon te houden.
4. Sleep de gewenste workflowsjablonen naar het tekenpapier rechts op de pagina.
5. (Optioneel) Kies het pictogram (*Koppeling*) dat tussen twee taaksjablonen verschijnt en selecteer de benodigde waarde voor voorwaardelijke parameters in de lijst die op het scherm verschijnt.

   Hier kunt u ook de benodigde `<Vertragingstijd>` (in seconden) invoeren.
6. Klik op een workflowsjabloon op het tekenpapier.

   Er verschijnt rechts van het tekenpapier een invoervenster.
7. Kies in het invoervenster rechts > (*Uitvouwen*) om voor elke taaksjabloon de invoerparametervelden weer te geven en selecteer de benodigde waarden in de velden.

   > ⚠ Let op
   >
   > - Let op dat de invoerwaarden die u opgeeft voor de sjabloonparameters geen persoonsgegevens van u bevatten en voldoen aan de AVG-richtlijnen (Algemene verordening gegevensbescherming). Zie het onderwerp Gegevensbeveiliging en privacy [pagina 175] voor meer informatie over de AVG.

   > ⓘ Opmerking
   >
   > In de Parametergegevens kunt u meer informatie krijgen over de parameters. Zie Informatie over parametergegevens [pagina 874] voor meer informatie over Parametergegevens.
8. Kies *Opslaan*.

   > → Onthouden
   >
   > Voordat u een scenario kunt uitvoeren, moet u voor elke taaksjabloon in een scenario gegevens invoeren. Maar u kunt de gegevens ook opgeven met de optie *Uitvoeren met parameter*.
9. Voer in het dialoogvenster *Scenario opslaan* de nodige gegevens in op de tabbladen *Scenario opslaan* en *Waarschuwen per e-mail*.

a. Voer op het tabblad *Scenario opslaan* een naam (verplicht) in voor het scenario, voeg een beschrijving toe en selecteer de locatie waar het scenario wordt opgeslagen.
b. Selecteer op het tabblad *Waarschuwen per e-mail* de schakelknop om deze optie in te schakelen. Hier worden de opties zoals in de onderstaande afbeelding

weergegeven.
c. Selecteer een of meer opties. Met uw selectie bepaalt u de criteria voor de verzending van een waarschuwing per e-mail.
d. U kunt de *standaardinstelling gebruiken* of deze optie uitschakelen met de schakelknop. In CMC zijn de volgende standaardinstellingen gedefinieerd. Zie de *Beheerdershandleiding voor Business Intelligence* voor meer informatie over het definiëren van standaardinstellingen voor e-maildoelen.
e. Als u *Standaardinstelling gebruiken* uitschakelt, voert u e-mailadressen in bij *Van, Aan*, *CC* (optioneel) en *BCC* (optioneel), evenals een *onderwerp* en een *bericht*. U kunt ook tijdelijke plaatsaanduidingen toevoegen aan elk veld.

10. Kies *Opslaan* of *Opslaan en uitvoeren*.

    Het nieuwe scenario verschijnt in de view *Scenario's* van de *Workflowassistent* en afhankelijk van de criteria die u hebt geselecteerd op het tabblad *Waarschuwen per e-mail* wordt een e-mail gestuurd.

22.7.5.1.1 Invoerparameters opgeven

Wanneer u workflowsjablonen in *Workflowassistent* maakt, kunt u invoerwaarden toevoegen tijdens het ontwerpen en tijdens runtime. Dit betekent dat u de invoerwaarden kunt toevoegen tijdens het maken en uitvoeren van een scenario. U kunt op twee manieren invoerwaarden toevoegen aan een *Scenario*:

1. Invoerhulp
2. Uitvoer van een taak toewijzen als invoer van een andere taak

Invoerhulp

U kunt een object als een document en een werklijst kiezen in de Gegevensopslagverkenner met de *Invoerhulp*. In een scenario voor het vernieuwen van het document kunt u bijvoorbeeld een document kiezen door het pictogram *Invoerhulp* in het veld *Documenten* te kiezen.

Uitvoer van een taak toewijzen als invoer van een andere taak

U kunt de uitvoer van de eerste taak als invoer voor de tweede taak opgeven tijdens het uitvoeren van een scenario. U moet @ in een invoerveld typen om de lijst met waarden weer te geven die uit de eerste taak zijn verkregen.

- De indeling van een invoerwaarde is **@<WorkflowTemplate>.<TaskTemplate>.<OutputParameter>**.

- Op de lijst met invoerwaarden worden alleen de compatibele waarden weergegeven die uit de eerste taak zijn verkregen. Als het invoerveld bijvoorbeeld CSV als het gegevenstype accepteert, worden de invoerwaarden uit de vorige taak die in CSV-indeling zijn weergegeven.

> **Opmerking**
>
> De invoerparameters bieden ondersteuning voor een CSV-bestand als invoer. Zie Werken met CSV-gegevens [pagina 873] voor meer informatie.

22.7.5.1.2 Werken met CSV-gegevens

De meeste standaardtaaksjablonen bieden ondersteuning voor invoerparameterwaarden in CSV-indeling. De taaksjabloon *Document vernieuwen* biedt bijvoorbeeld ondersteuning voor de CSV-indeling voor het invoerveld *Documenten*. Dit betekent dat u een CSV-bestand dat gegevens in de indeling **naam, CUID en status** bevat als invoer kunt selecteren voor *Documenten*.

> **Opmerking**
>
> Als het taakinvoerveld **CUID** accepteert en u een CSV-bestand selecteert dat andere parameters bevat inclusief **CUID**, gebruikt het invoerveld alleen de **CUID**-kolomwaarden uit het CSV-bestand. Zie voor een voorbeeld de onderstaande CSV-gegevens:
>
> naam, CUID, status;
>
> Diagrammen, AW4AVT1AUhVAogA6P7OQv9c, geslaagd;
>
> Verkooprapport, BW3AVT1AUhVAogA743QCDsD, geslaagd;
>
> In dit voorbeeld gebruikt het invoerveld AW4AVT1AUhVAogA6P7OQv9c en BW3AVT1AUhVAogA743QCDsD, en worden de andere waarden genegeerd.

Kolom- en rijscheidingsteken

Het ondersteunde kolomscheidingsteken is **,**. Het rijscheidingsteken is **;**. Met een kolom- en rijscheidingsteken in een invoerveld worden de gegevens in kolom- en rij-indeling gescheiden. Zie voor een voorbeeld de onderstaande CSV-gegevens:

naam, CUID, status;

Diagrammen, AW4AVT1AUhVAogA6P7OQv9c, geslaagd;

Verkooprapport, BW3AVT1AUhVAogA743QCDsD, geslaagd;

Hier geeft de komma aan dat **naam, CUID en status** kolommen zijn, en geeft de puntkomma het einde van de rij aan.

> **Opmerking**
>
> Als een CSV-bestand invoer is voor de taaksjabloon *Werklijst lezen* is het kolomscheidingsteken dan **,**. Het rijscheidingsteken is **;** of een nieuwe regel.

> ⚠ Let op
>
> Een waarde in de CSV-gegevens mag nooit een komma of een puntkomma bevatten.

22.7.5.1.3 Informatie over parametergegevens

U kunt de parametergegevens bekijken nadat u een parameter in het invoervenster van een scenario hebt uitgevouwen en geselecteerd. In de taaksjabloon Documenten vernieuwen is er bijvoorbeeld een invoerveld Documenten. Wanneer u het invoerveld Documenten selecteert, worden de parametergegevens weergegeven.

De parametergegevens bestaan uit twee secties:

1. Invoerparameter
2. Uitvoerparameter

Invoerparameter

Bij Invoerparameter wordt uitgelegd welk type invoer vereist is voor het geselecteerde veld. Het is specifiek voor het invoerveld binnen de taaksjabloon.

Uitvoerparameters

Bij Uitvoerparameters wordt uitleg gegeven over de verschillende uitvoer die wordt verkregen van de taak. Het is specifiek voor de gehele taak en niet voor slechts één invoerveld.

22.7.5.2 Scenario's bewerken

U bewerkt scenario's in de Workflowassistent.

1. Kies op het tabblad *Scenario's* van de Workflowassistent de optie ··· (*Meer*) en selecteer *Bewerken*.

   Het scherm "Scenario bewerken" wordt weergegeven.
2. Breng in het scherm *Scenario bewerken* de gewenste bewerkingen in het scenario aan door de taaksjablonen/workflowsjablonen toe te voegen/te verwijderen of door de invoerparameterwaarden van de sjablonen te wijzigen.
3. Kies *Opslaan*.

   Het dialoogvenster "Scenario opslaan" wordt weergegeven.
4. Wijzig in het dialoogvenster *Scenario opslaan* desgewenst de naam van het scenario en kies *Opslaan*.

De wijzigingen in het scenario worden opgeslagen en u keert terug naar de startpagina van de Workflowassistent.

22.7.5.3 Scenario's verwijderen

U verwijdert scenario's in de Workflowassistent.

1. Kies op het tabblad *Scenario's* van de Workflowassistent ⋯ (*Meer*) en selecteer *Verwijderen*.
2. Kies *Verwijderen* in de waarschuwing die wordt weergegeven.

   Het verwijderde scenario wordt niet meer weergegeven op het tabblad *Scenario's* van de Workflowassistent.

22.7.5.4 Scenario's uitvoeren en resultaten weergeven

U kunt scenario's uitvoeren en resultaten weergeven in de Workflowassistent.

1. Kies in de view *Scenario's* van de Workflowassistent de optie ⋯ (*Meer*) en selecteer *Uitvoeren* of *Uitvoeren met parameter*.

   Met *Uitvoeren met parameter* wordt een dialoogvenster weergegeven met alle invoerparameters van het scenario en u kunt hier waarden wijzigen of ontbrekende waarden instellen.

   > ⓘ Opmerking
   >
   > De waarden die in dit parametervenster worden ingesteld, worden niet opgeslagen bij het scenario. Ze worden alleen gebruikt voor het exemplaar dat wordt uitgevoerd.

   Het scenario (tegel of item op lijst) geeft eerst Uitvoeren of In behandeling als de nieuwe status weer. Nadat de uitvoering is voltooid, wordt de status bijgewerkt in de relevante waarde (`<Geslaagd/Gedeeltelijk geslaagd/Mislukt/In behandeling/Fout/Wordt uitgevoerd met fout>`).
2. Als u de resultaten van het scenario wilt weergeven (terwijl het wordt uitgevoerd of nadat het met succes is uitgevoerd), kiest u ⋯ (*Meer*) en selecteert u *Resultaten weergeven*.

   > ⓘ Opmerking
   >
   > U kunt de optie Geschiedenis weergeven selecteren om de resultaten van de vorige uitvoeringen van een scenario weer te geven.
3. Vouw op de pagina *Resultaten* de resultaten uit om de uitvoerings- en voltooiingsdetails van elke workflowsjabloon en taaksjabloon in het scenario weer te geven. Nadat u de resultaten hebt bekeken, kunt u teruggaan naar het hoofdscherm met de knop < (*Terug*).

   > ⓘ Opmerking
   >
   > U kunt de optie Exporteren selecteren om het scenario op te slaan in PDF-indeling.

> **Opmerking**
>
> 1. U kunt een maximale tijd instellen voor een taak om op een agent te reageren door de tijd (in seconden) toe te voegen aan de sleutelwaarde task_time_out in het bestand wfmanager_conf.properties. Standaard is de sleutelwaarde task_time_out ingesteld op 86400, ofwel één dag.
>
> 2. De task_time_out wordt ingesteld voor alle agenten in de Workflowassistent.

22.7.5.5 Scenario's stoppen

U kunt nu een scenario stoppen terwijl uw taak nog wordt uitgevoerd.

Vereisten:

U kunt alleen doorgaan met de onderstaande stappen als een scenario de status Uitvoeren of In behandeling heeft.

- Selecteer in de view Scenario's de optie *Meer* voor het scenario.
- Kies Stoppen.

> **Opmerking**
>
> Met de optie Stoppen wordt het scenario niet onmiddellijk gestopt. Nadat u de optie Stoppen hebt geselecteerd, wordt de huidige taak, die wordt uitgevoerd, eerst voltooid, en vervolgens wordt het scenario gestopt. Dit betekent dat alleen de taken die in behandeling zijn in het scenario niet worden uitgevoerd.

22.7.6 De statuswaarden van taaksjablonen, workflowsjablonen en scenario's

Mogelijke statuswaarden van onderdelen (taaksjabloon/workflowstatus/scenario) met beschrijving

Status	Beschrijving
Gemaakt (C)	Wanneer een onderdeel is gemaakt, maar nog niet is uitgevoerd.
In behandeling (P)	Wanneer een onderdeel is geactiveerd voor uitvoering en in de wachtrij wacht op uitvoering.
Uitvoeren (R)	Wanneer een onderdeel wordt uitgevoerd.

Status	Beschrijving
Geslaagd (S)	Wanneer alle verwerkte items met succes zijn uitgevoerd. De verwerkte documenten zijn bijvoorbeeld met succes vernieuwd na de taak Document vernieuwen. **Opmerking** Als zelfs maar één workflowsjabloon in een scenario niet met succes is uitgevoerd, krijgt het gehele scenario niet de status 'Geslaagd'.
Gedeeltelijk geslaagd (PS)	Wanneer slechts enkele van de verwerkte items met succes zijn uitgevoerd. Wanneer enkele documenten bijvoorbeeld niet worden vernieuwd na de taak Document verwerken, wordt de status gewijzigd in Gedeeltelijk geslaagd.
Mislukt (F)	Wanneer geen van de items met succes is uitgevoerd.
Fout (E)	Wanneer een onderdeel een fout of uitzonderingen aantreft tijdens uitvoering.
Wordt uitgevoerd met fout (RE)	Wanneer een onderdeel een fout op de server aantreft, maar de uitvoering niet wordt gestopt.
Niet uitgevoerd	Wanneer een taaksjabloon of workflowsjabloon in een scenario niet wordt uitgevoerd vanwege instellingen van voorwaardelijke parameters. Als de beheerder er bijvoorbeeld voor kiest om de voorwaarde `<Als geslaagd>` tussen twee workflowsjablonen in te stellen, waardoor de volgende workflowsjabloon niet wordt uitgevoerd als de vorige workflowsjabloon is mislukt. In dit geval houden de volgende en daaropvolgende workflowsjablonen de status `<Niet uitgevoerd>`.

Opmerking

Dit zijn de legenda's voor de tabellen:

- TTS: Status taaksjabloon
- WFTS: Status workflowsjabloon
- SS: Status scenario

Statusmatrix: Status van taaksjablonen en resulterende status van workflowsjablonen

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	S	S	E	NE	E (Fout)
S	S	S	PS	NE	PS (Gedeeltelijk geslaagd)
S	S	PS	F	NE	F (Mislukt)
S	PS	F	R	NE	R (Uitvoeren)
S	E	NE	NE	NE	E (Fout)

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	E	RE	NE	NE	RE (Wordt uitgevoerd met fouten)

In de onderstaande matrix wordt uitgelegd hoe de status van elke workflowsjabloon de algehele status van het scenario beïnvloedt.

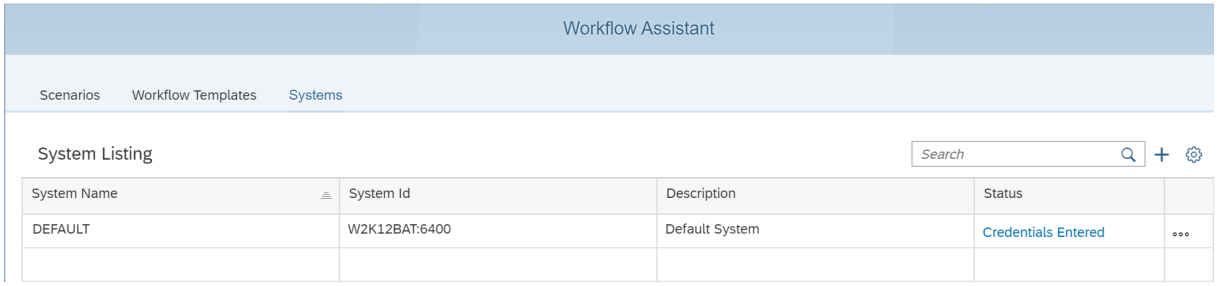
Statusmatrix: Status van workflowsjablonen en resulterende status van scenario

WFTS1	WFTS2	WFTS3	WFTS4	WFTS5	SS
S	S	S	E	NE	E (Fout)
S	S	S	PS	NE	PS (Gedeeltelijk geslaagd)
S	S	PS	F	NE	F (Mislukt)
S	PS	F	R	NE	R (Uitvoeren)
S	E	NE	NE	NE	E (Fout)
S	E	RE	NE	NE	RE (Wordt uitgevoerd met fouten)

22.7.7 Werken met Systemen

Op het tabbladSystemen kunt u meerdere BI-landschappen registreren. Systemen biedt u toegang tot uw geregistreerde BI-landschappen.

Momentopname van het tabblad *Systemen*



U kunt de volgende acties uitvoeren op het tabblad *Systemen*:

- Een nieuw systeem toevoegen (registreren)

  > → Onthouden
  >
  > Het is verplicht om uw systemen op dit tabblad te registreren zodat u deze systemen in andere views zoals *Scenario's* en *Workflowsjablonen* kunt weergeven.

- Een bestaand systeem wijzigen (bewerken of verwijderen)
- Verbinding maken met het systeem (of de verbinding verbreken) door uw referenties (`User Name, Password, Authentication`) in te voeren

> **Opmerking**
>
> Het systeem waarop u de Workflowassistent hebt geïnstalleerd wordt op het tabblad *Systemen* weergegeven als het "Standaardsysteem". Om verbinding te maken met dit landschap, moet u echter uw referenties invoeren.

- De kolommen die worden weergegeven in de view Systemen aanpassen

22.7.7.1 Nieuw BI-systeem registreren

U kunt pas verbinding maken met het BI-systeem waarvoor u bevoegd bent en de mogelijkheden van de Workflowassistent gebruiken als u de BI-systemen hebt geregistreerd (toegevoegd) in de Workflowassistent.

Dit doet u als volgt:

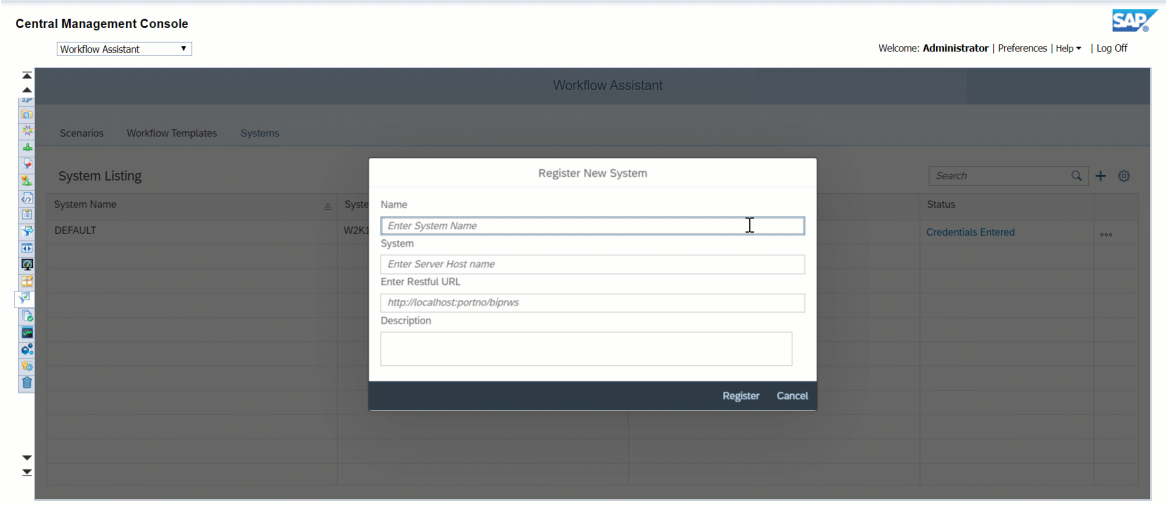
1. Meld u aan bij de Workflowassistent.
2. Navigeer op de *startpagina* naar het tabblad *Systemen*.

   Hier vindt u een overzicht van uw beschikbare geregistreerde systemen.
3. Kies het pictogram + (*Toevoegen*).

   Het dialoogvenster 'Nieuw systeem registreren' verschijnt op het scherm.
4. Voer bij `<Naam>` een alias in die u in uw systeem kunt herkennen.
5. Voer bij `<Systeem>` de serverhostnaam of het IP-adres in waarmee uw computer of cluster van computers wordt geïdentificeerd.
6. Voer bij `<RestFul URL>` de URL naar de RESTful-webservices voor de BI-platformserver in. U kunt desgewenst een `<beschrijving>` voor het systeem toevoegen.
7. Kies *Registreren*.

   > **Opmerking**
   >
   > U kunt hetzelfde BI-systeem registreren met verschillende namen, maar het is raadzaam een BI-systeem slechts één keer in de weergave Systemen te hebben.

   Het geregistreerde systeem wordt toegevoegd aan de lijst in de tabel Lijst met systemen.



22.7.7.2 Bestaande BI-systemen wijzigen

In de weergave Systemen kunt u uw geregistreerde systemen wijzigen.

Dit doet u als volgt:

1. Meld u aan bij de Workflowassistent en navigeer naar het tabblad *Systemen*.
2. Kies in de weergave Systemen (*Meer*) → *Bewerken* voor het systeem in de lijst dat u wilt wijzigen.

   Het dialoogvenster *Systeem bewerken* verschijnt op het scherm.
3. Wijzig de waarden van de velden `<Naam>` (alias), `<Systeem>`, `<RestFul-URL>` of `<Beschrijving>` conform uw behoeften en kies *Gereed*.

   De wijzigingen worden weergegeven in de tabel Lijst met systemen.

   > **Opmerking**
   >
   > Als u een systeem wilt verwijderen, kiest u (*Meer*) → *Verwijderen* voor het systeem in de lijst dat u wilt verwijderen en bevestigt u de verwijdering in het dialoogvenster dat vervolgens wordt weergegeven.

22.7.7.3 Verbinding maken met geregistreerde BI-systemen

U kunt verbinding maken met uw geregistreerde systemen via het veld `<Status>` in de tabel Lijst met systemen. U moet verbinding maken met het BI-systeem wanneer u uw systemen wilt gebruiken in de scenario's in Workflowassistent.

Volg de hier beschreven procedure om verbinding te maken met een toegevoegd BI-systeem:

1. Meld u aan bij de Workflowassistent en navigeer naar het tabblad *Systemen*.
2. Kies de vlagreeks (*No Credentials Entered* (Geen referenties ingevoerd)) die verschijnt in het veld `<Status>` van de geregistreerde systemen waarmee u nog niet bent verbonden.

   Het dialoogvenster "Referenties invoeren" wordt geopend.
3. Voer uw referenties voor het BI-systeem in (op basis van de autorisatie van uw systeembeheerder): `<Gebruikersnaam>`, `<Wachtwoord>` en `<Verificatie>`. Kies vervolgens *Opslaan*.

   De Workflowassistent controleert uw referenties en werkt de `<status>` van uw BI-landschap bij tot *Ingevoerde referenties* als de referenties kloppen. Als de referenties niet kloppen, wordt er een foutmelding weergegeven en blijft het veld `<Status>` ongewijzigd.

22.7.7.4 De weergave Systemen aanpassen

U kunt de weergave Lijst van systemen aanpassen door de zichtbaarheid van velden (kolommen) in de view te wijzigen.

Ga als volgt te werk om specifieke kolommen van de weergave Systemen te verbergen/tonen:

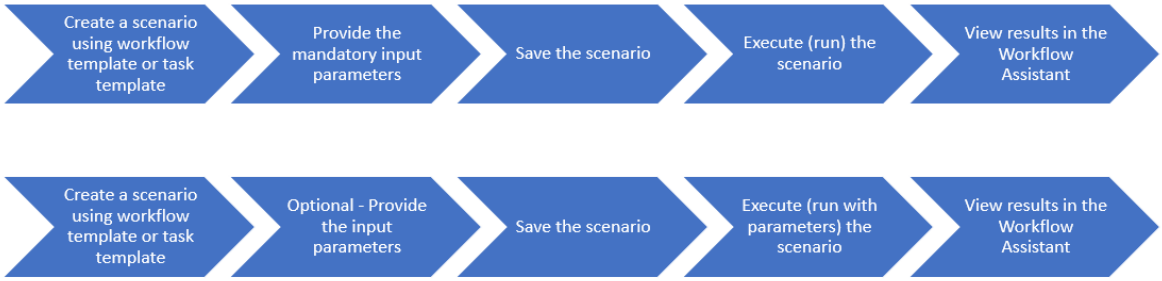
1. Meld u aan bij de Workflowassistent en navigeer naar het tabblad *Systemen*.

2. Kies (*Instellingen*) en schakel de kolommen (veldkopteksten) uit die u wilt verbergen in de tabel Lijst van systemen.

   De uitgeschakelde kolommen worden niet meer weergegeven in de tabel Lijst van systemen.
3. Kies *Instellingen* en selecteer de veldkopteksten opnieuw om een verborgen kolom weer op te nemen in de weergave.

22.7.8 Volledige processtroom van de Worklowassistent

Bekijk een visuele weergave.



22.8 Logboekbestanden controleren

In dit onderwerp wordt uitgelegd hoe u de logboekbestanden van de Workflowassistent kunt controleren.

Workflowassistent

Voor de Workflowassistent moet u het traceringsniveau in het bestand *WorkflowAssistant_Trace.ini* in `<INSTALLATIEMAP>\AdminConsole\WorkflowAssistant` kiezen. Traceringsbestanden kunnen ook worden geconfigureerd met behulp van het bestand **_Trace.ini** door de volgende omgevingsvariabelen in te stellen:

- `BO_TRACE_CONFIGDIR` om de mapnaam van configuratiebestanden in te stellen voor logboekbestanden, bijvoorbeeld: `C:\BOTraces\config`
- `BO_TRACE_CONFIGFILE` om de naam van het configuratiebestand in te stellen, bijvoorbeeld `BO_trace.ini`
- `BO_TRACE_LOGDIR` om de mapnaam voor logboekbestanden in te stellen, bijvoorbeeld: `C:\BOTraces`

> **Opmerking**
>
> De `INI`-bestandsnaam is hoofdlettergevoelig.

Maak het configuratiebestand `BO_trace.ini` als volgt:

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

U kunt uw logboekbestanden standaard controleren in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\logging`.

23 Prullenbak

23.1 Prullenmand

Info over prullenmand

Prullenmand is een nieuwe toepassing in de CMC. Wanneer de gebruiker een item uit het BOE-systeem verwijdert, wordt dit verplaatst naar de prullenmand, waar het tijdelijk wordt opgeslagen totdat de prullenmand wordt leeggemaakt. Dit geeft de gebruiker de gelegenheid rapporten/mappen te herstellen die per ongeluk zijn verwijderd en ze terug te zetten op hun oorspronkelijke locatie.

De beheerder kan met de prullenmandapplicatie:

- herstel van verwijderde items (zoals rapporten en mappen) initiëren
- items uit de prullenmand permanent verwijderen
- de prullenmand automatisch opschonen

Als de prullenmand is ingeschakeld, kunt u de volgende typen InfoObjecten recyclen:

- Inhoud van persoonlijke map
- Gebeurtenissen
- Kalenders
- Inhoud van openbare map
- Universes
- Verbindingen
- Openbare categorieën
- Persoonlijke categorieën
- Inboxen
- Profielen
- Aangepaste rollen

23.1.1 Item uit prullenmand herstellen

De prullenmand geeft een lijst met verwijderde items weer. Ga als volgt te werk om een item uit de prullenmand te herstellen:

1. Meld u aan bij de CMC.
2. Selecteer in het deelvenster *Beheren* op de CMC-startpagina *Prullenmand*.

3. Klik met de rechtermuisknop op het item dat u wilt herstellen en selecteer *Herstellen* in het snelmenu.
4. Selecteer *OK*.

   U kunt naar de locatie van het herstelde item navigeren om de herstelbewerking te bevestigen.

   > **Opmerking**
   >
   > Als u een item uit de prullenmand herstelt en er bestaat al een ander item met dezelfde naam op de herstellocatie, wordt het item onder de volgende naam opgeslagen op de herstellocatie: "<itemnaam> hersteld(1, 2, ...)".
   >
   > Wanneer de bovenliggende map van een item in de prullenmand wordt verwijderd, wordt de bovenliggende map opnieuw gemaakt als het item is hersteld. De bovenliggende map bevat dan echter alleen het/de uit de prullenmand herstelde item(s).
   >
   > In de prullenmand kunt u een item niet openen/navigeren.
   >
   > Als u een item uit een map verwijdert en de beheerder beperkt daarna de wijzigingsrechten van die map, kunt u het item nog steeds naar de oorspronkelijke map herstellen.

U hebt een item uit de prullenmand nu hersteld.

23.1.2 Items uit de prullenmand permanent verwijderen

Als beheerder hebt u het recht om geselecteerde items permanent te verwijderen uit de prullenmand of de prullenmand leeg te maken.

Ga als volgt te werk om items permanent uit de prullenmand te verwijderen:

1. Meld u aan bij de CMC.
2. Selecteer in het deelvenster *Beheren* op de CMC-startpagina *Prullenmand*.
3. Klik met de rechtermuisknop op het item dat u wilt verwijderen en selecteer *Verwijderen* in het contextmenu.
4. Selecteer *OK*.

U hebt nu een item verwijderd uit de prullenmand.

23.1.3 Automatisch opschonen voor prullenmand inschakelen

U kunt de prullenmand periodiek automatisch opschonen.

Ga als volgt te werk om de prullenmand automatisch op te schonen:

1. Meld u aan bij de CMC.
2. Selecteer in het deelvenster *Beheren* op de CMC-startpagina *Toepassingen*.
3. Selecteer op de pagina *Toepassingen* de toepassing *Prullenmand*.

   Het dialoogvenster *Eigenschappen: prullenmand* wordt geopend.

4. Selecteer het aankruisvakje en geef op hoe lang (in dagen) het systeem moet wachten voordat een verwijderd item automatisch wordt opgeschoond.
5. Kies *Opslaan en sluiten*.

U hebt nu automatisch opschonen voor de prullenmand ingeschakeld.

24 Controle

24.1 Overzicht

Met de controlevoorziening kunt u belangrijke gebeurtenissen bijhouden die zich voordoen op servers en in toepassingen, zodat u een beeld krijgt van de informatie die wordt geraadpleegd, de manier waarop deze informatie wordt geraadpleegd en gewijzigd, en de gebruikers die deze bewerkingen uitvoeren. Deze informatie wordt vastgelegd in de database Gegevensopslag voor controle. Zodra de gegevens zijn opgenomen in de controledatabase, kunt u naar wens aangepaste rapporten maken. U kunt naar voorbeeld-universes en -rapporten zoeken in de SAP Community http://community.sap.com/.

In dit hoofdstuk is een controleur een systeem dat verantwoordelijk is voor het registreren of opslaan van informatie over een gebeurtenis, en een controleobject is een systeem dat verantwoordelijk is voor het uitvoeren van een controlegebeurtenis. In sommige omstandigheden kan één systeem beide functies uitvoeren.

Hoe controleren werkt

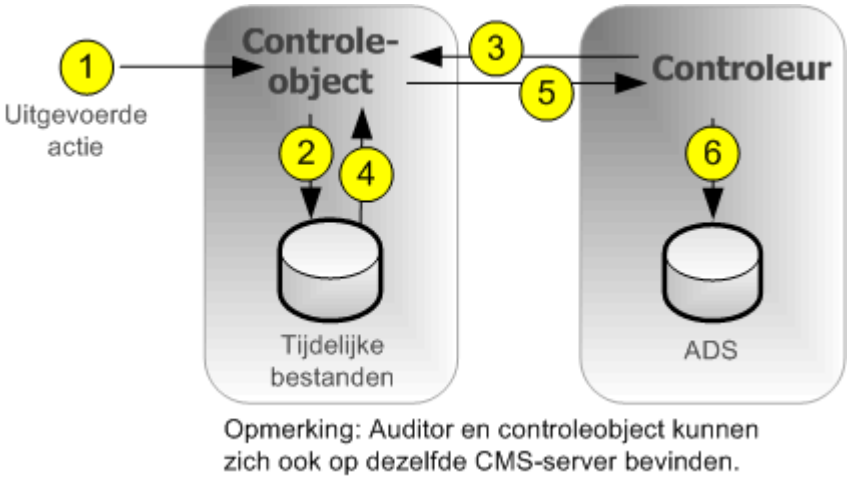
De CMS (Central Management Server) is de systeemcontroleur, terwijl elke server of toepassing die een controleerbare gebeurtenis activeert een controleobject is. Wanneer een gecontroleerde gebeurtenis wordt geactiveerd, genereert het controleobject een record en wordt deze opgeslagen in een lokaal tijdelijk bestand. De CMS communiceert regelmatig met de controleobjecten om deze records op te vragen en schrijft de gegevens naar de ADS.

De CMS bestuurt ook de synchronisatie van de controlegebeurtenissen die zich op verschillende computers voordoen. Voor elk controleobject wordt een tijdstempel ingesteld voor de geregistreerde controlegebeurtenissen. De CMS geeft regelmatig de systeemtijd door aan de controleobjecten om ervoor te zorgen dat de tijdstempels van de gebeurtenissen op de verschillende servers consistent zijn. De controleobjecten vergelijken deze tijd met hun interne klok. Als er verschillen bestaan, corrigeren ze de tijd die is geregistreerd voor opeenvolgende controlegebeurtenissen.

Afhankelijk van het type controleobject dat wordt gecontroleerd, volgt het systeem een van de volgende werkstromen bij het opslaan van de gebeurtenissen:

Server controleren

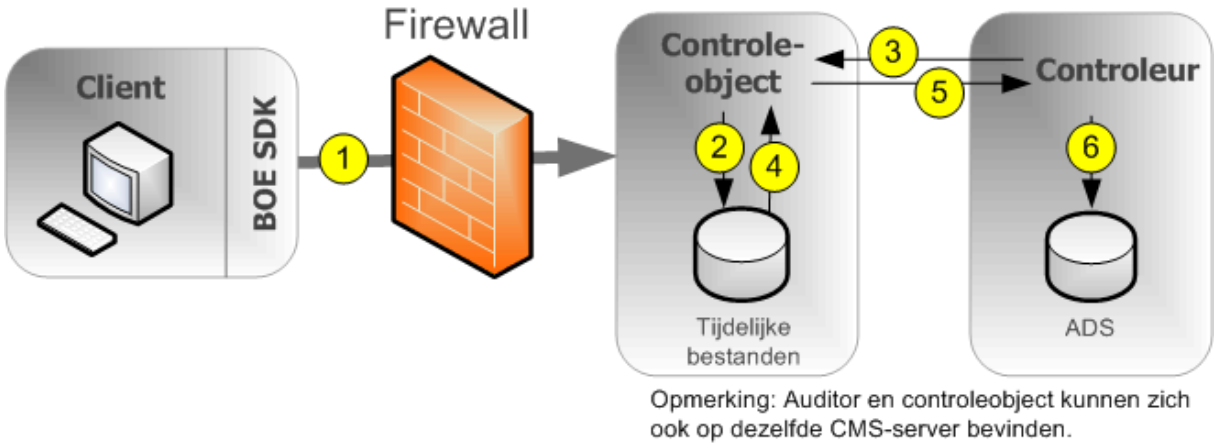
Voor gebeurtenissen die door de server zijn gegenereerd, kan de CMS als controleobject of als controleur optreden.



1. Er wordt een controleerbare gebeurtenis uitgevoerd door de server.
2. Het controleobject schrijft gebeurtenissen naar een tijdelijk bestand. Stappen 1 en 2 kunnen meermaals voor stap 3 voorkomen.
3. De controleur vraagt het controleobject geregeld op en vraagt een batch controlegebeurtenissen aan.
4. Het controleobject haalt de gebeurtenissen uit de tijdelijke bestanden op.
5. Het controleobject stuurt de gebeurtenissen door naar de controleur.
6. De controleur schrijft gebeurtenissen naar de ADS en waarschuwt het controleobject om de gebeurtenissen uit de tijdelijke bestanden te verwijderen.

Controle van clientaanmelding voor clients die verbinding maken via CORBA

Hiertoe behoren toepassingen zoals SAP BusinessObjects Web Intelligence



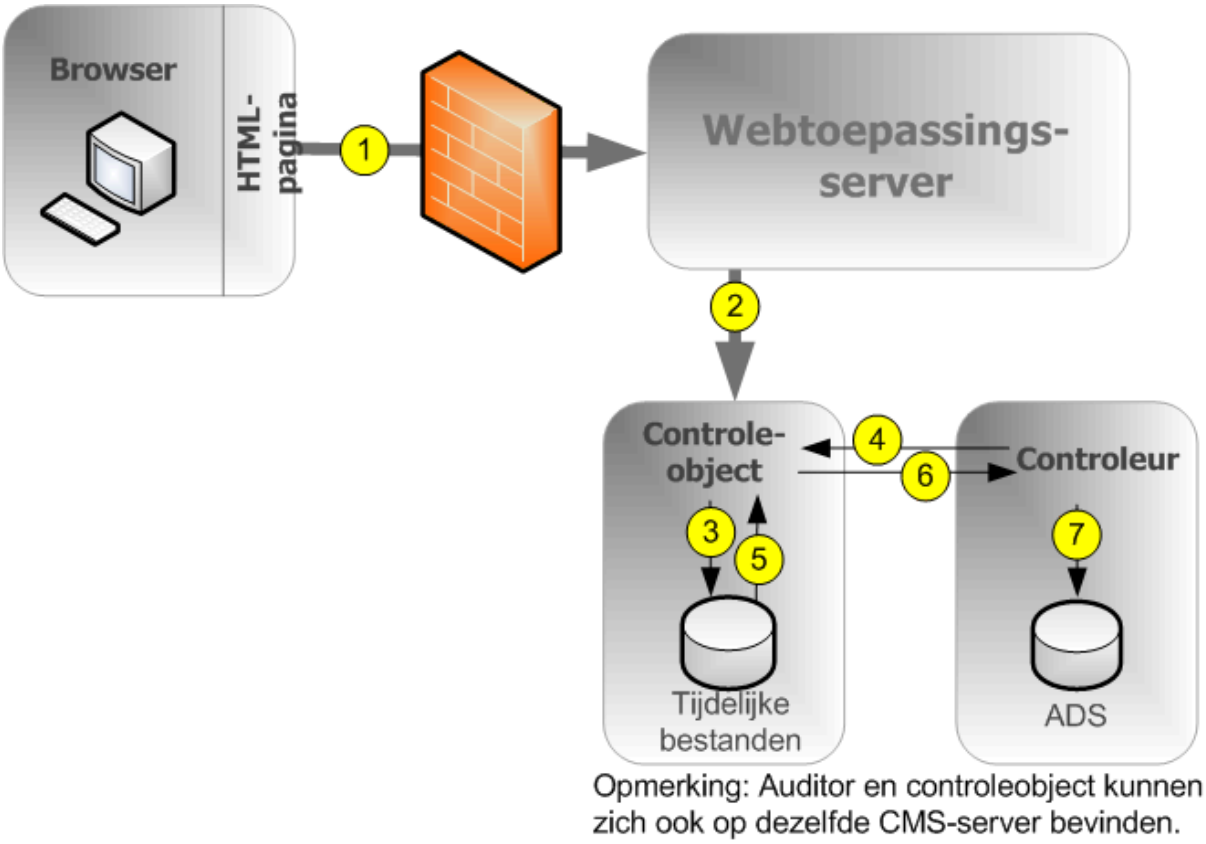
1. De client maakt verbinding met de CMS die fungeert als het controleobject. Het IP-adres en de computernaam van de client worden doorgestuurd en vervolgens door het controleobject gecontroleerd.

> **Opmerking**
>
> Er moet een poort geopend zijn in de firewall die zich vóór de client en CMS bevindt. Raadpleeg het hoofdstuk over beveiliging in de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over firewalls.

2. Het controleobject schrijft gebeurtenissen naar een tijdelijk bestand. Stappen 1 en 2 kunnen meermaals voorkomen vóór stap 3.
3. De controleur vraagt het controleobject geregeld op en vraagt een batch controlegebeurtenissen aan.
4. Het controleobject haalt de gebeurtenissen uit de tijdelijke bestanden op.
5. Het controleobject stuurt de gebeurtenissen door naar de controleur.
6. De controleur schrijft gebeurtenissen naar de ADS en waarschuwt het controleobject om de gebeurtenissen uit de tijdelijke bestanden te verwijderen.

Controle van clientaanmelding voor clients die verbinding maken via HTTP

Deze optie omvat onlinetoepassingen zoals BI-startpunt, Central Management Console en SAP BusinessObjects Web Intelligence.

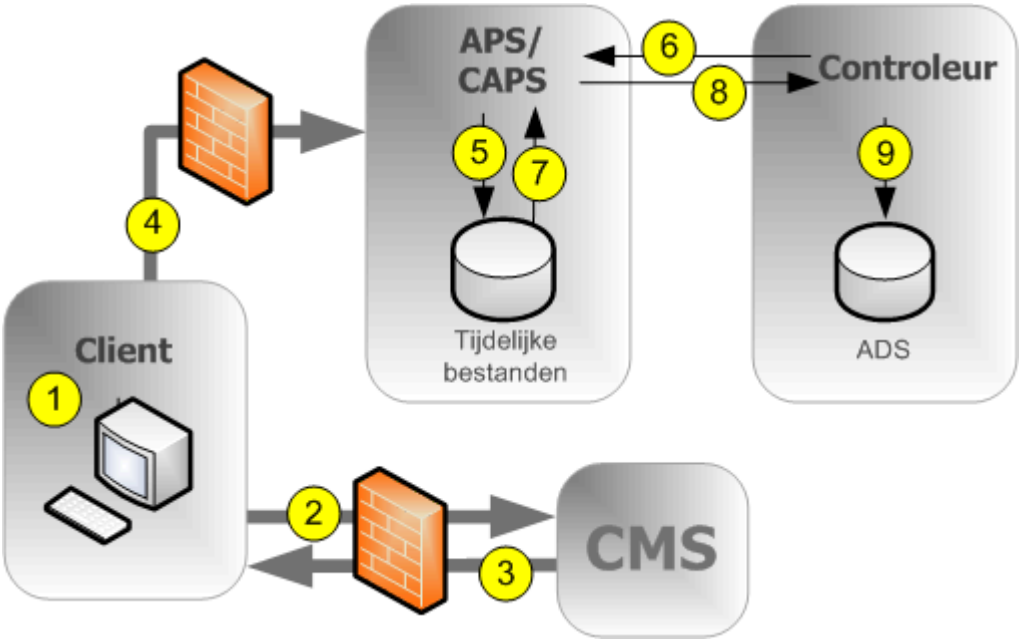


1. De browser maakt verbinding met de webtoepassingsserver, en aanmeldingsgegevens worden verzonden naar de webtoepassingsserver.
2. Via de SDK van het BI-platform wordt de aanmeldingsaanvraag samen met het IP-adres en de naam van de browsercomputer verzonden naar het controleobject (CMS).

3. Het controleobject schrijft gebeurtenissen naar een tijdelijk bestand. Stappen 1 tot 3 kunnen meermaals voor stap 4 voorkomen.
4. De controleur vraagt het controleobject geregeld op en vraagt een batch controlegebeurtenissen aan.
5. Het controleobject haalt de gebeurtenissen uit de tijdelijke bestanden op.
6. Het controleobject verzendt de gebeurtenissen naar de controleur.
7. De controleur schrijft gebeurtenissen naar de ADS en waarschuwt het controleobject om de gebeurtenissen uit de tijdelijke bestanden te verwijderen.

Controle die geen betrekking heeft op aanmelding voor clients die verbinding maken via CORBA

Deze werkstroom is van toepassing op de controle van SAP BusinessObjects Web Intelligence-gebeurtenissen wanneer u verbinding maakt via CORBA.



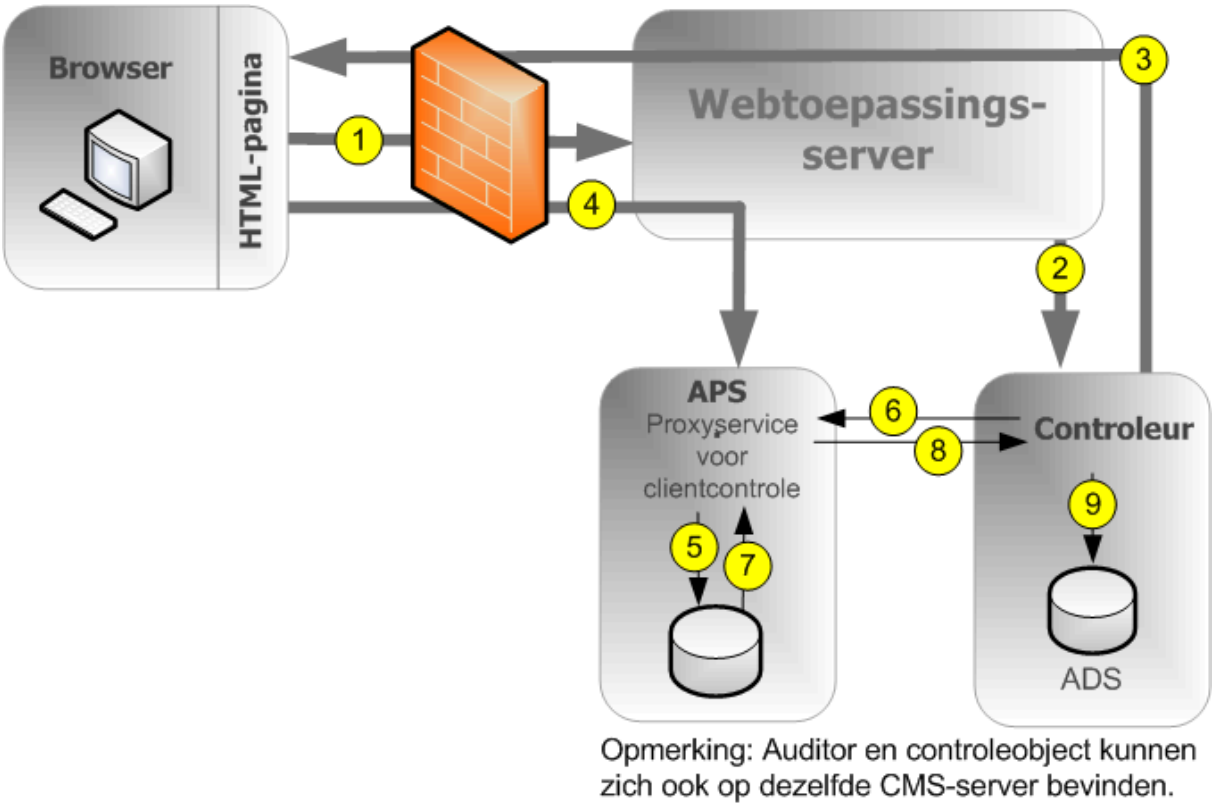
1. De gebruiker voert een bewerking uit die mogelijk wordt gecontroleerd.
2. De client maakt verbinding met de CMS om te controleren of de bewerking is geconfigureerd om te worden gecontroleerd.
3. Als de actie is ingesteld voor controle, geeft de CMS deze informatie door aan de client.
4. De client stuurt gebeurtenisgegevens naar de CAPS (Client Auditing Proxy Service), die wordt gehost op een Adaptive Processing Server.

> **Opmerking**
>
> Een poort in de firewall moet worden geopend tussen elke client en alle Adaptive Processing Servers die een CAPS hosten, en ook tussen elke client en de CMS. Raadpleeg het hoofdstuk over beveiliging in de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over firewalls.

5. De CAPS schrijft gebeurtenissen naar een tijdelijk bestand. Stappen 1 tot 5 kunnen meermaals voor stap 6 voorkomen.
6. De controleur vraagt de CAPS geregeld op en vraagt een batch controlegebeurtenissen aan.
7. De CAPS haalt de gebeurtenissen uit de tijdelijke bestanden op.
8. Gebeurtenisgegevens worden naar de controleur verzonden via de CAPS.
9. De controleur schrijft gebeurtenissen naar de ADS en waarschuwt de CAPS om de gebeurtenissen uit de tijdelijke bestanden te verwijderen.

Controle die geen betrekking heeft op aanmelding voor clients die verbinding maken via HTTP

Deze werkstroom is van toepassing op de controle van SAP BusinessObjects Web Intelligence-gebeurtenissen (behalve aanmeldingsgebeurtenissen) bij verbinding via HTTP.



1. De gebruiker start een controleerbare gebeurtenis. De clienttoepassing maakt verbinding met de webtoepassingsserver.
2. De webtoepassing controleert of de gebeurtenis is geconfigureerd om te worden gecontroleerd.

   > **Opmerking**
   >
   > In het diagram ziet u dat er contact wordt gemaakt met de CMS-controleur; voor deze gegevens kan echter contact worden gemaakt met elke CMS in de cluster.

3. De CMS retourneert de gegevens over de controleconfiguratie naar de toepassingsserver, die de gegevens weer terugstuurt naar de clienttoepassing.

4. Als de gebeurtenis is geconfigureerd voor controle, stuurt de client de gebeurtenisgegevens naar de webtoepassingsserver; deze stuurt de gegevens weer door naar de CAPS (Client Auditing Proxy Service), die op een APS (Adaptive Processing Server) wordt gehost.
5. De CAPS schrijft gebeurtenissen naar een tijdelijk bestand. Stappen 1 tot 5 kunnen meermaals voorkomen vóór stap 6.
6. De controleur vraagt de CAPS geregeld op en vraagt een batch controlegebeurtenissen aan.
7. De CAPS haalt de gebeurtenissen uit de tijdelijke bestanden op.
8. Gebeurtenisgegevens worden naar de controleur verzonden via de CAPS.
9. De controleur schrijft gebeurtenissen naar de ADS en waarschuwt de CAPS om de gebeurtenissen uit de tijdelijke bestanden te verwijderen.

Clients die controle ondersteunen

Controle wordt ondersteund door de volgende clienttoepassingen:

- Analysis-editie voor OLAP (AOLAP)
- BI-startpunt (BILP)
- Business View Manager (BVM)
- Central Configuration Manager (CCM)
- Central Management Console (CMC)
- OpenDocument
- Hulpprogramma voor informatieontwerp (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Hulpprogramma voor vertaalbeheer (TMT)
- Web Intelligence Rich Client (WIRC)
- Lumira Desktop Application (Discovery)
- Lumira Designer Application

> **Opmerking**
>
> Ten minste één exemplaar van CAPS moet worden uitgevoerd om controlegebeurtenissen van de bovenstaande clients te verzamelen.

Clients die hierboven niet worden vermeld, genereren gebeurtenissen niet rechtstreeks maar sommige acties die worden uitgevoerd door de servers als resultaat van bewerkingen van de clienttoepassing, kunnen worden gecontroleerd.

Controleconsistentie

In de meeste gevallen worden alle aangegeven systeemgebeurtenissen correct en consistent geregistreerd als de controlefunctie correct is geïnstalleerd, correct is geconfigureerd en is beveiligd, en als de juiste versies van alle clienttoepassingen worden gebruikt. Houd er echter rekening mee dat bepaalde systeem- en omgevingssituaties een negatieve invloed kunnen hebben op de controle.

Er treedt altijd vertraging op tussen het tijdstip waarop een gebeurtenis plaatsvindt en de uiteindelijke overdracht naar de ADS. Bepaalde omstandigheden kunnen deze vertragingen verhogen, bijvoorbeeld wanneer de CMS of de controledatabase niet beschikbaar is, of de netwerkverbinding verbroken is.

Als systeembeheerder probeert u de volgende situaties te voorkomen, omdat deze kunnen leiden tot onvolledige controlerecords:

- Een station waarop controlegegevens worden opgeslagen, bereikt de maximumcapaciteit. U moet zorgen dat er voldoende schijfruimte beschikbaar is voor uw controledatabase en gecontroleerde tijdelijke bestanden.
- Een server met controleobjecten wordt onjuist uit het netwerk verwijderd voordat alle controlegebeurtenissen zijn verzonden. Wanneer u een server uit het netwerk verwijdert, moet u ervoor zorgen dat er voldoende tijd beschikbaar is om controlegebeurtenissen naar de controledatabase te verzenden.
- Verwijderen of wijzigen van gecontroleerde tijdelijke bestanden.
- Een hardware- of schijffout.
- Een hostcomputer voor het controleobject of de auditor loopt vast.

Het kan ook voorkomen dat controlegebeurtenissen de CMS-auditor niet kunnen bereiken. Dit gebeurt in de volgende gevallen:

- Gebruikers met oudere clientversies.
- De verzending van controlegegevens wordt geblokkeerd door onjuist geconfigureerde firewalls.

> **Opmerking**
>
> Gebeurtenissen die worden gegenereerd door clienttoepassingen bevatten gegevens die van de clientzijde worden verzonden, met andere woorden buiten het vertrouwde gebied van het systeem. Daarom zijn deze gegevens onder bepaalde omstandigheden mogelijk niet zo betrouwbaar als gegevens die door de systeemservers worden geregistreerd.

> **Opmerking**
>
> Als u een server uit uw implementatie wilt verwijderen, moet u eerst die server uitschakelen, maar deze wel blijven uitvoeren en de verbinding behouden met uw netwerk totdat alle gebeurtenissen in de tijdelijke bestanden de kans hebben gehad te worden overgebracht naar de controledatabase. Het gegeven *Huidig aantal controlegebeurtenissen in wachtrij* van de server geeft aan hoeveel controlegebeurtenissen wachten op overdracht. Wanneer dit gegeven nul bereikt, kunt u de server stoppen. De locatie van de tijdelijke bestanden wordt gedefinieerd door de tijdelijke plaatsaanduiding `%DefaultAuditingDir%` voor dat knooppunt. Zie het hoofdstuk Serverbeheer voor meer informatie over tijdelijke plaatsaanduidingen.

> **Opmerking**
>
> Als u Clientcontrole gebruikt, is het raadzaam dat u een speciale Adaptive Processing Server maakt voor de proxyservice voor clientcontrole. Dit zorgt voor de beste systeemprestaties. Voer de CAPS om meer dan een APS uit om de fouttolerantie van uw systeem te verhogen.

Verwante koppelingen

Tijdelijke plaatsaanduidingen voor server en knooppunt [pagina 1211]

24.2 CMC-controlepagina

De pagina *Controle* in de CMC bevat de volgende gebieden:

- *Statusoverzicht*
- *Gebeurtenissen instellen*
- *Gebeurtenisdetails instellen*
- *Configuratie*

24.2.1 Controlestatus

Het *Statusoverzicht* van controle biedt u een gegevensset waarmee u uw controleconfiguratie kunt optimaliseren. Bovendien brengt het overzicht problemen naar voren die van invloed kunnen zijn op de integriteit van uw controlegegevens. Het statusoverzicht vindt u boven aan de pagina *Controle* in de Central Management Console.

Het overzicht geeft in de volgende gevallen ook waarschuwingen weer:

- De verbinding met de ADS-database is niet beschikbaar.
- Er is geen actieve of ingeschakelde proxyservice voor clientcontrole, wat het verzamelen van clientgebeurtenissen verhindert.
- Een controleobject bevat gebeurtenissen die niet kunnen worden opgehaald (de betrokken server of servers worden aangegeven). Dit komt meestal voort uit het onjuist stoppen of uitschakelen van een server zodat er nog gebeurtenissen in de tijdelijke bestanden staan.

> **Opmerking**
>
> De gegevens van het statusoverzicht worden met groen, geel of rood weergegeven om de status van de controlefunctie aan te geven.

Gegevens van controlestatus

Gegeven	Details
Laatste update van ADS op	De datum en tijd waarop de controle-CMS voor het laatst een polling heeft voltooid op de controleobjecten voor hun controlegebeurtenissen.
Thread-gebruik controleren	Het percentage van de pollingscyclus dat de controle-CMS heeft besteed aan het verzamelen van gegevens van de controleobjecten. De rest van de tijd is besteed aan rustpauzes tussen de polls.

Gegeven	Details
	Als deze waarde 100% is, wordt het getal in het geel weergegeven en dit betekent dat de controleur nog bezig is met het verzamelen van gegevens uit controleobjecten wanneer de volgende poll volgens de planning moet beginnen. Dit kan ertoe leiden dat de gebeurtenissen de ADS met vertraging bereiken. Als dit veelvuldig of aanhoudend gebeurt, is het raadzaam dat u uw implementatie bijwerkt zodat de ADS-database gegevens sneller kan ontvangen (met snellere netwerkverbindingen of krachtigere databasehardware bijvoorbeeld), of het aantal controlegebeurtenissen dat uw systeem volgt, verlaagt.
Duur van laatste pollingcyclus	Duur van de laatste pollingcyclus in seconden. Dit geeft de maximale vertraging aan waarmee gebeurtenisgegevens de ADS hebben bereikt gedurende de vorige pollingcyclus. • Als de duur minder dan 20 minuten (1200 seconden) bedraagt, wordt het getal weergegeven met een groene achtergrond. • Als de duur tussen de 20 minuten en 2 uur ligt (7200 seconden), wordt het weergegeven met een gele achtergrond. • Bij meer dan twee uur is de achtergrond rood. Als deze staat aanhoudt en u de vertraging te lang acht, is het raadzaam dat u uw implementatie bijwerkt zodat de ADS-database gegevens sneller kan ontvangen (met snellere netwerkverbindingen of krachtigere databasehardware bijvoorbeeld), of het aantal controlegebeurtenissen dat uw systeem volgt, verlaagd.
CMS-controleur	De naam van de CMS die momenteel als controleur dienst doet.
Naam van ADS-databaseverbinding	De naam van de databaseverbinding die momenteel wordt gebruikt door de controle-CMS om verbinding te maken met de ADS (Auditing Data Store). Voor SQL Anywhere, SQL Server en SAP HANA-servers is dit de naam van de ODBC-verbinding. Voor andere databasetypen is dit de databasenaam en verbindingspoort, gevolgd door de servernaam.
Gebruikersnaam voor ADS-database	De gebruikersnaam waarmee de controle-CMS zich aanmeldt bij de ADS-database.

24.2.2 Controlegebeurtenissen configureren

Via de CMC-controlepagina kunt u controle activeren en selecteren welke gebeurtenissen er binnen het volledige systeem gecontroleerd moeten worden.

Als u geen waarde hecht aan bepaalde gebeurtenissen of gebeurtenisdetails, kunt u deze uitgeschakeld laten voor betere systeemprestaties.

> **Opmerking**
>
> Controlegebeurtenissen worden naar de controledatabase in batchmodus gepusht in plaats van één gebeurtenis per keer. De batchgrootte is momenteel ingesteld op 1000 controlegebeurtenissen.

> **Opmerking**
>
> Als u de ADS-verbinding niet hebt geconfigureerd tijdens de installatie van het BI-platform, moet u een verbinding met de database tot stand brengen, voordat u uw controlegebeurtenissen configureert. Zonder verbinding worden de gebeurtenissen ook verzameld, maar wanneer de verbinding tot stand wordt gebracht, worden de gebeurtenissen naar de ADS geschreven. Als u controle wilt uitschakelen, moet het niveau op uit staan. Zie *Configuratie-instellingen van ADS*.

24.2.2.1 Controlegebeurtenissen configureren

Voer de volgende stappen uit om de controlegebeurtenissen te configureren:

1. Selecteer het tabblad *Controle* in de Central Management Console
   De pagina *Controle* wordt weergegeven.
2. Stel de schuifregelaar *Gebeurtenissen instellen* in op het gewenste controleniveau, waarbij elk controleniveau overeenkomt met een specifieke gegevenswaarde.
   - *Uit* - 1
   - *Minimaal* - 2
   - *Standaard* - 3
   - *Volledig* - 4
   - *Aangepast* - 0

   In de volgende tabel worden de vier verschillende instellingen voor de schuifregelaar weergegeven, evenals de gebeurtenissen die op elk niveau worden vastgelegd.

Controleniveau	Vastgelegde gebeurtenissen
Uit	Geen
Minimaal	• Aanmelden • Afmelden • Wijziging van rechten • Aangepast toegangsniveau gewijzigd • Wijziging van controle

Controleniveau	Vastgelegde gebeurtenissen
Standaard	*Minimale* gebeurtenissen, plus: • Weergeven • Vernieuwen • Aanwijzing • Maken • Verwijderen • Wijzigen • Opslaan • Zoeken • Bewerken • Uitvoeren • Leveren
Volledig	*Minimale* en *Standaard*gebeurtenissen plus: • Activeren • Analyse uitvoeren buiten analyseniveau • Pagina opgehaald • Configuratie van promotiebeheer • Terugzetten • Toevoegen aan VMS • Ophalen uit VMS • Inchecken in VMS • Uitchecken bij VMS • Exporteren naar VMS • VMS-vergrendeling • VMS-ontgrendeling • VMS verwijderen • Kubusverbinding • MDSAS-sessie **Opmerking** U kunt meer gebeurtenissen weergeven als de add-ons zijn geïnstalleerd.
Aangepast	U selecteert een aangepaste gegevensset.

Opmerking

Als de optie *Gebeurtenissen instellen* is ingesteld op *Standaard*, is de waarde voor *Controleniveau* 3.

Als de optie *Gebeurtenissen instellen* is ingesteld op *Uit*, wordt de waarde voor *Controleniveau* gewijzigd van 3 in 1.

3. Selecteer *Aangepast* en klik in de lijst onder de schuifregelaar *Gebeurtenissen instellen* op de gebeurtenissen die u wilt vastleggen.
4. Klik op de optionele details onder *Gebeurtenisdetails instellen* die u wilt vastleggen binnen de gebeurtenissen. Als u minder details vastlegt, worden de systeemprestaties verbeterd.

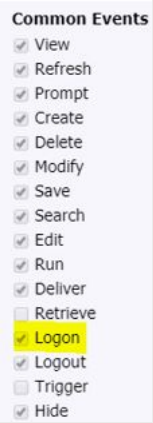
Detail	Beschrijving
Query	Indien ingesteld, wordt het gebeurtenisdetail *Query* (Detail-id 25) vastgelegd voor elke gebeurtenis die informatie opvraagt bij een database.
Details van mappad	Indien ingesteld, worden de volgende details vastgelegd: • *Pad naar objectmap (Detail-id 71)* • *Naam van hoofdmap (Detail-id 72)* • *Pad naar containermap (Detail-id 64)*
Details van rechten	Indien ingesteld, worden de volgende details vastgelegd: • *Recht toegevoegd (Detail-id 55)* • *Recht verwijderd (Detail-id 56)* • *Recht gewijzigd (Detail-id 57)*
Details van gebruikersgroep	Indien ingesteld, worden de volgende details vastgelegd: • *Naam van gebruikersgroep (Detail-id 16)* • *Id van gebruikersgroep (Detail-id 15)*
Details van eigenschapswaarde	Indien ingesteld, wordt het gebeurtenisdetail *Eigenschapswaarde* (Detail-id 29) vastgelegd, wanneer de eigenschappen van een object worden bijgewerkt. Dit wordt alleen gegenereerd voor CMC-, BI-startpunt- of SharePoint-gebeurtenissen.

5. Klik op *Opslaan*.

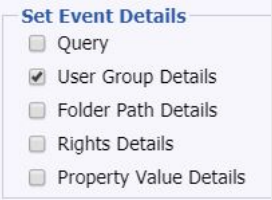
> **Opmerking**
>
> Voor clientcontrole duurt het, nadat de wijzigingen zijn aangebracht, twee minuten voordat het systeem gegevens gaat vastleggen voor nieuwe gebeurtenissen. Houd rekening met deze vertraging bij het implementeren van wijzigingen in het systeem.

24.2.2.2 Uitgebreide opname gebeurtenisdetails in tabel met controledetails

> **Opmerking**
>
> - U zou over voldoende kennis van CMC-controlepagina [pagina 893] moeten beschikken, met name *Algemene gebeurtenissen, Gebeurtenisdetails instellen, Details gebruikersgroep* en *Aanmelding*, om de onderstaande informatie te gebruiken.
> - *Aanmelding* is een gebeurtenis die details geeft over een gebruiker die de applicatie opent.



- *Details van gebruikersgroep* levert informatie over de gebruikersgroepen die voor elke gebeurtenis aan een gebruiker zijn gekoppeld.



De opname van details van de gebruikersgroep in de tabel AUDIT_EVENT_DETAIL is gedeeltelijk afhankelijk van de gegevens die zijn geselecteerd onder *Algemene gebeurtenissen* en *Gebeurtenisdetails instellen* op de pagina Controle. Neem bijvoorbeeld een scenario waarbij u *Aanmelding* hebt geselecteerd, maar niet de *details van gebruikersgroep* op de pagina *Controle*. In dit scenario worden de details van de gebruikersgroep nog steeds opgenomen voor de gebeurtenis *Aanmelding* in de tabel AUDIT_EVENT_DETAIL. Zie de onderstaande tabel voor meer informatie over dit gedrag in BI 4.2 Support Package 5.

Aanmelding	Details van gebruikersgroep	Gedrag
Geselecteerd	Geselecteerd	Details van gebruikersgroep worden opgenomen voor alle gebeurtenissen die zijn geselecteerd onder Algemene gebeurtenis.
Geselecteerd	Niet geselecteerd.	Details van gebruikersgroep worden alleen voor Aanmeldingsgebeurtenissen opgenomen.
Niet geselecteerd.	Niet geselecteerd.	Details van gebruikersgroep worden niet opgenomen.
Niet geselecteerd.	Geselecteerd	Details van gebruikersgroep worden opgenomen voor alle geselecteerde gebeurtenissen behalve Aanmeldingsgebeurtenissen.

24.2.3 Configuratie-instellingen van ADS (Auditing Data Store)

Als u geen controledatabase hebt ingesteld tijdens de installatie van het BI-platform, of als u de databaselocatie of instellingen wilt wijzigen, kunt u de volgende stappen uitvoeren om de verbinding met ADS te configureren.

Hier kunt u ook configureren hoe lang controlegebeurtenissen in de database worden bewaard.

Als u een upgrade hebt uitgevoerd voor een eerdere versie van SAP BusinessObjects Enterprise XI 3.x en versie 3.x van Business Objects Metadata Manager (BOMM) hebt geïnstalleerd, is het raadzaam de ADS te configureren voor gebruik met dezelfde database of tabelruimte als die van BOMM.

> **Opmerking**
>
> Als u een bestaande DB2 9.7-werkgroep als controledatabase gebruikt, zorg dan dat de database-account is geconfigureerd om een paginaformaat groter dan 8 kB te hebben.

24.2.3.1 De instellingen voor uw ADS-database configureren

1. Selecteer het tabblad *Controle* in de Central Management Console.
2. Selecteer in het gebied *Configuratie* onder de kop *ADS-database* het databasetype dat u hebt ingesteld voor uw controlegegevens.
3. Voer in het veld *Verbindingsnaam* de naam van de verbinding in die u hebt geconfigureerd voor de controledatabase.

Databasetype	Naam van verbinding
IBM DB2	servicenaam
Microsoft SQL Server	ODBC DSN
MySQL	`<serverhostname>,<port>,<databasename>`
Oracle	TNS-servicenaam
SAP HANA	ODBC DSN
SAP MaxDB	`<serverhostname>,<port>,<databasename>`
Sybase Adaptive Server Enterprise	servicenaam
Sybase SQL Anywhere	ODBC DSN

   a. Als u een Microsoft SQL-database met Windows-verificatie gebruikt, schakelt u de optie *Windows-verificatie* in.

4. In de velden *Gebruikersnaam* en *Wachtwoord* voert u de gebruikersnaam en het wachtwoord in die de controle-CMS moet gebruiken voor aanmelding bij de database.

5. In het veld *Gebeurtenissen verwijderen die ouder zijn dan (dagen)* voert u in hoeveel dagen de informatie in de database moet blijven staan. (Minimumwaarde 1, maximumwaarde 109.200).

> ⚠ Let op
>
> Gegevens ouder dan het hier ingestelde aantal dagen worden permanent uit de ADS verwijderd en kunnen niet worden hersteld. Als u records voor de lange termijn wilt behouden, is het raadzaam regelmatig records naar een archiefdatabase te verplaatsen.

6. Als de databaseverbinding wordt verbroken en u de controle-CMS handmatig weer met de database wilt verbinden, heft u de selectie van de optie *ADS automatisch opnieuw verbinden* op.

> ⓘ Opmerking
>
> Als deze optie niet geselecteerd is, moet u de verbinding met de ADS handmatig opnieuw tot stand brengen als deze verbroken wordt. Dit kunt u doen door de CMS opnieuw te starten of *ADS automatisch verbinden* in te schakelen. Gebeurtenissen worden vastgelegd en in tijdelijke mappen opgeslagen totdat de verbinding met de ADS opnieuw tot stand is gebracht.

7. Klik op *Opslaan*.
8. Start alle CMSs in het cluster opnieuw.

> ⓘ Opmerking
>
> In het *Statusoverzicht* boven aan de pagina ziet u de huidige ADS-waarden, die kunnen afwijken van de waarden in de sectie *ADS-database* tot u de CMS's opnieuw start.

24.3 Controlegebeurtenissen

In de volgende tabel worden alle controlegebeurtenissen in het systeem weergegeven en ontvangt u een korte beschrijven van elke gebeurtenis. Hieronder volgt een lijst met servicetypen die de gebeurtenissen maken.

Gebeurtenis	
Beschrijving van controlewijziging, en servers en clients die het gebeurtenistype genereren	De controle-instellingen van het systeem zijn aangepast. • Central Management-service
Maken	Er is een nieuw object aan het systeem toegevoegd. • Service voor BI-commentaar • Central Management-service • Crystal Reports-service voor weergave en wijziging • Desktop Intelligence • Information Engine-service • Beheer van levenscyclus • Web Intelligence • Algemene service van Web Intelligence

Gebeurtenis	
	• Beschrijving, en servers en clients die de Web Intelligence-kernservice genereren • Web Intelligence-verwerkingsservice
Kubusverbinding	Een bewerking met OLAP-kubusverbinding wordt uitgevoerd. • Multidimensionale analyseservice • Analysis-toepassingen
Aangepast toegangsniveau gewijzigd	Gegevens voor rechten zijn aangepast. • Central Management-service
Verwijderen	Een object is uit het systeem verwijderd. • Service voor BI-commentaar • Central Management-service • Service voor Beheer van levenscyclus
Leveren	Een object is naar een doel verzonden. • Planningsservice voor verificatie-update • Central Management-service • Planningsservice van Crystal Reports voor Enterprise • Planningsservice van Crystal Reports • Desktop Intelligence • Planningsservice voor doelbezorging • Planningsservice voor Platform zoeken • Planningsservice van test • Programmaplanningsservice • Planningsservice voor beveiligingsquery • Planningsservice voor importeren van gebruikers en groepen • Plannings- en publicatieservice van Web Intelligence
Analyse uitvoeren buiten analyseniveau	Een gebruiker van een Web Intelligence-document heeft een analyse op lager niveau uitgevoerd naar een detailniveau buiten de vooraf geladen gegevens van het rapport. • Web Intelligence • Web Intelligence-verwerkingsserver • Algemene services van Web Intelligence • Kernservices van Web Intelligence • Information Engine-service
Bewerken	De inhoud van een object is gewijzigd. • Toepassing BI-werkruimten • Desktop Intelligence • Information Engine-service • Web Intelligence

Gebeurtenis	
	• Algemene service van Web Intelligence • Web Intelligence-kernservice • Web Intelligence-verwerkingsservice
LCM-configuratie	De configuratiedetails van de console voor beheer van levenscyclus zijn gewijzigd. • Beheer van levenscyclus
Aanmelden	Een gebruiker meldt zich aan bij het systeem. • Central Management-service
Afmelden	Een gebruiker meldt zich af bij het systeem. • Central Management-service
Wijzigen	De bestandseigenschappen van een object zijn gewijzigd. • Web Intelligence • Beheer van levenscyclus • Central Management-service • Service voor BI-commentaar
MDSAS-sessie	Er wordt een bewerking met de Multidimensionale analyseservice uitgevoerd. • Multidimensionale analyseservice
Pagina opgehaald	Een SAP BusinessObjects Web Intelligence-client haalt extra informatie op uit de gegevensopslagruimte. • Web Intelligence-verwerkingsservice • Algemene services van Web Intelligence • Kernservices van Web Intelligence • Information Engine-service
Aanwijzing	Er is informatie ingevoerd voor een objectaanwijzing. • Crystal Reports-service voor opslaan in cache • Planningsservice van Crystal Reports voor Enterprise • Planningsservice van Crystal Reports • Desktop Intelligence • Information Engine-service • Live Office • Web Intelligence • Algemene service van Web Intelligence • Web Intelligence-kernservice • Web Intelligence-verwerkingsservice
Vernieuwen	De gegevens in een object zijn bijgewerkt aan de hand van de database op aanvraag van de gebruiker. • Crystal Reports-service voor opslaan in cache • Planningsservice van Crystal Reports voor Enterprise

Gebeurtenis	
	• Planningsservice van Crystal Reports • Desktop Intelligence • Information Engine-service • Live Office • Web Intelligence • Algemene service van Web Intelligence • Web Intelligence-kernservice • Web Intelligence-verwerkingsservice
Ophalen	Er wordt een object opgehaald uit de gegevensopslagruimte. • Central Management-service • Desktop Intelligence
Wijziging van rechten	De beveiligingsinformatie voor een gebruiker, groep of object wordt gewijzigd. • Central Management-service
Rollback	LifeCycle Manager wordt gebruikt om de vorige versie van een object te herstellen. • Beheer van levenscyclus
Uitvoeren	Er is een taak uitgevoerd. • Planningsservice voor verificatie-update • Planningsservice van Crystal Reports voor Enterprise • Planningsservice van Crystal Reports • Desktop Intelligence • Planningsservice voor doelbezorging • LCM-planningsservice • Beheer van levenscyclus • Planningsservice voor Platform zoeken • Planningsservice van test • Programmaplanningsservice • Planningsservice voor publicatie • Herhalingsservice • Planningsservice voor beveiligingsquery • Planningsservice voor importeren van gebruikers en groepen • Planningsservice voor Visueel verschil • Web Intelligence-service voor planning en publicatie
Opslaan	Een object wordt opgeslagen nadat dit gewijzigd of bijgewerkt is. • Analysis-editie voor OLAP • Crystal Reports-service voor opslaan in cache • Planningsservice van Crystal Reports voor Enterprise

Gebeurtenis	
	• Planningsservice van Crystal Reports • Crystal Reports-service voor weergave en wijziging • Desktop Intelligence • Information Engine-service • Beheer van levenscyclus • Multi-Dimensional Analysis-service • SAP BusinessObjects Mobile • Web Intelligence • Algemene service van Web Intelligence • Web Intelligence-kernservice • Web Intelligence-verwerkingsservice
Zoeken	Er wordt een zoekopdracht uitgevoerd. • Zoekservice • Explorer • Beheer van levenscyclus
Activeren	Een bestandsgebeurtenis is geactiveerd. • Gebeurtenisservice • Central Management-service
Weergeven	Een object wordt weergegeven • Analysis-toepassing • Analysis-editie voor OLAP • BI-startpunt • Toepassing BI-werkruimten • Service voor BI-commentaar • CMC • Crystal Reports-service voor opslaan in cache • Crystal Reports-service voor weergave en wijziging • Desktop Intelligence • Information Engine-service • Document openen • SAP BusinessObjects Mobile • Web Intelligence • Algemene service van Web Intelligence • Web Intelligence-kernservice • Web Intelligence-verwerkingsservice
Toevoegen aan VMS	Een object is toegevoegd aan het LCM-systeem voor versiebeheer. • Beheer van levenscyclus
Inchecken in VMS	Een object wordt ingecheckt in het LCM-systeem voor versiebeheer. • Beheer van levenscyclus

Gebeurtenis	
Uitchecken uit VMS	Een object wordt uitgecheckt uit het LCM-systeem voor versiebeheer. • Beheer van levenscyclus
Exporteren naar VMS	Een bron wordt geëxporteerd uit het VMS. • Beheer van levenscyclus
VMS-vergrendeling	Een bron in de VMS is vergrendeld. • Beheer van levenscyclus
VMS-ontgrendeling	Een bron in de VMS wordt ontgrendeld. • Beheer van levenscyclus
Ophalen uit VMS	Een object wordt opgehaald uit het LCM-systeem voor versiebeheer. • Beheer van levenscyclus
VMS verwijderen	Een object wordt verwijderd uit het LCM-systeem voor versiebeheer. • Beheer van levenscyclus

Gebeurtenissen op servicetype

Servicetype	Gebeurtenistypen gegenereerd
Analysis-toepassing	• Weergeven • Kubusverbinding
Planningsservice voor verificatie-update	• Leveren • Uitvoeren
Fiorified BI-startpunt	Weergeven
Service voor BI-commentaar	• Maken • Verwijderen • Weergeven • Wijzigen • Verbergen
Central Management Service	• Wijziging van controle • Maken • Aangepast toegangsniveau gewijzigd • Verwijderen • Leveren • Aanmelden

Servicetype	Gebeurtenistypen gegenereerd
	• Afmelden • Wijzigen • Ophalen • Wijziging van rechten • Activeren
Central Management Console	Weergeven
Planningsservice van Crystal Reports	• Leveren • Aanwijzing • Vernieuwen • Uitvoeren • Opslaan
Crystal Reports-service voor opslaan in cache	• Aanwijzing • Vernieuwen • Opslaan • Weergeven
Planningsservice van Crystal Reports voor Enterprise	• Leveren • Aanwijzing • Vernieuwen • Uitvoeren • Opslaan
Planningsservice van Crystal Reports	• Leveren • Aanwijzing • Vernieuwen • Uitvoeren • Opslaan
Crystal Reports-service voor weergave en wijziging	• Maken • Opslaan • Weergeven
Desktop Intelligence (client)	• Leveren • Aanwijzing • Ophalen • Uitvoeren
Desktop Intelligence-schedulerproces	• Leveren • Uitvoeren
Planningsservice voor doelbezorging	• Leveren • Uitvoeren
Gebeurtenisservice	Activeren

Servicetype	Gebeurtenistypen gegenereerd
Information Engine-service	• Maken • Analyse uitvoeren buiten analyseniveau • Bewerken • Opgehaalde pagina • Aanwijzing • Vernieuwen • Opslaan • Weergeven
LCM-planningsservice	Uitvoeren
LCM-service	• Maken • Verwijderen • LCM-configuratie • Wijzigen • Rollback • Uitvoeren • Opslaan • Toevoegen aan VMS • Inchecken in VMS • Uitchecken uit VMS • VMS verwijderen • Exporteren naar VMS • VMS-vergrendeling • Ophalen uit VMS • VMS-ontgrendeling • Zoeken
Live Office	• Aanwijzing • Vernieuwen
Multi-Dimensional Analysis-service	• Kubusverbinding • MDSAS-sessie • Opslaan
OpenDocument	Weergeven
Planningsservice voor Platform zoeken	• Leveren • Uitvoeren
Service Platform zoeken	Zoeken
Planningsservice van test	• Leveren • Uitvoeren
Programmaplanningsservice	• Leveren • Uitvoeren
Planningsservice voor publicatie	Uitvoeren

Servicetype	Gebeurtenistypen gegenereerd
Herhalingsservice	Uitvoeren
SAP BusinessObjects Design Studio versie 1.3 en later	• Aanmelden • Afmelden
Planningsservice voor beveiligingsquery	• Uitvoeren • Leveren
Planningsservice voor importeren van gebruikers en groepen	• Uitvoeren • Leveren
Planningsservice voor Visueel verschil	Uitvoeren
Web Intelligence-toepassing	• Maken • Analyse uitvoeren buiten analyseniveau • Bewerken • Wijzigen • Aanwijzing • Vernieuwen • Opslaan • Weergeven
Algemene service van Web Intelligence	• Maken • Analyse uitvoeren buiten analyseniveau • Bewerken • Opgehaalde pagina • Aanwijzing • Vernieuwen • Opslaan • Weergeven
Web Intelligence-kernservice	• Maken • Analyse uitvoeren buiten analyseniveau • Bewerken • Opgehaalde pagina • Aanwijzing • Vernieuwen • Opslaan • Weergeven
Web Intelligence-verwerkingsserver	• Maken • Analyse uitvoeren buiten analyseniveau • Bewerken • Pagina opgehaald • Aanwijzing • Vernieuwen • Opslaan

Servicetype	Gebeurtenistypen gegenereerd
	• Weergeven
Web Intelligence-service voor planning en publicatie	• Leveren • Uitvoeren

Gebeurteniseigenschappen en -details

Elke gebeurtenis die wordt vastgelegd door BI-platform, bevat een reeks gebeurteniseigenschappen en -details.

Gebeurteniseigenschappen worden altijd gegenereerd met een gebeurtenis, hoewel sommige mogelijk geen waarden hebben als de informatie niet van toepassing is op een bepaalde gebeurtenis. In de ADS worden gebeurteniseigenschappen opgenomen in de tabel waarin de gebeurtenis is opgeslagen, zodat deze kunnen worden gebruikt om gebeurtenissen te sorteren of te groeperen wanneer u rapporten maakt.

Gebeurtenisdetails bevatten extra informatie over de gebeurtenis die niet is opgenomen in de gebeurteniseigenschappen. Als een gebeurtenisdetail niet relevant is voor een bepaalde gebeurtenis, wordt dat detail niet gegenereerd. Er is een reeks algemene gebeurtenisdetails die gegenereerd kunnen worden voor alle gebeurtenistypen wanneer deze relevant zijn. Er zijn ook reeksen aanvullende gebeurtenisdetails die gegenereerd worden voor specifieke gebeurtenistypen. Aanwijzingsgebeurtenissen registreren bijvoorbeeld de ingevoerde waarden voor de aanwijzing in een gebeurtenisdetail, maar andere gebeurtenistypen genereren geen aanwijzingswaarden in gebeurtenisdetails. In de ADS worden details opgeslagen in een aparte tabel die aan de bovenliggende gebeurtenis is gekoppeld.

In sommige gevallen kunnen gebeurtenisdetails meerdere waarden bevatten. Deze details kunnen worden gegroepeerd met de bundel-id. Zie het verwante onderwerp voor meer informatie over bundel-id's.

Meertalige gegevens (zoals object- of mapnamen) worden vastgelegd in de standaardtaal voor de landinstelling van de controle-CMS.

Verwante informatie

Auditing Data Store Tables [pagina 1221]

24.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Opmerking**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Opmerking**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **Opmerking** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.

Event Property	Description
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

> **Opmerking**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.

Event Detail	ID	Description
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **Opmerking**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **Opmerking** For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. **Opmerking** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

Prompt

A value was entered for a prompt.

- Event Type ID: 1004

Event Detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for

Event Detail	ID	Description
		each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

Delete

User deleted an object.

- Event Type ID: 1006

Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event Detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.
Old Property Value	120	A user's old email address.
New Property Value	121	The same user's new email address.

Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable.

Search

A search was conducted.

- Event Type ID: 1009

Event Detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

Edit

User edited the content of an object.

- Event Type ID: 1010

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.

Event Detail	ID	Description
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment.
Account Name	45	This records one of the following:

Event Detail	ID	Description
		• For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful

- Event Type ID: 123
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "2" indicates a named-user license logon was successful

Event Detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded.
Authentication Type	122	Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3
User Type	123	Type of the user.
Session Count	125	Count of the session is recorded.
Tenant ID	126	The ID of the tenant is recorded.
Concurrent Tenant Session	127	The count of the concurrent session of the tenant is recorded.

Logout

A user logs off.

- Event Type ID: 1015

Event Detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

Trigger

A file event is triggered.

- Event Type ID: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

24.3.1.1 platformgebeurtenissen

De volgende gebeurtenissen zijn specifiek voor BI-platform.

Wijziging van rechten

Een recht of rechten voor een object is/zijn gewijzigd.

- Gebeurtenistype-id: 10003

Gebeurtenisdetail	Id	Beschrijving
Rechten toegevoegd	55	Het type recht dat is toegevoegd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`.
Rechten verwijderd	56	Het type recht dat is verwijderd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Rechten gewijzigd	57	Het type recht dat is gewijzigd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Principal	118	De id van een gebruiker voor wie of een gebruikersgroep (principal) waarvoor beveiligingsrechten zijn gewijzigd.
Principal-naam	119	De naam van een gebruiker of gebruikersgroep (principal) waarvoor beveiligingsrechten zijn gewijzigd.

Aangepast toegangsniveau gewijzigd

Een aangepast toegangsniveau is gewijzgd.

- Gebeurtenistype-id: 10004

Gebeurtenisdetail	Id	Beschrijving
Rechten toegevoegd	55	Het type recht dat is toegevoegd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
Rechten verwijderd	56	Het type recht dat is verwijderd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`.
Rechten gewijzigd	57	Het type recht dat is gewijzigd, het bereik van het nieuwe recht (welke objecten) en het objecttype waarop het is toegepast. De informatie wordt gestructureerd volgens het volgende voorbeeld: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`.
Principal	118	De id van een gebruiker voor wie of een gebruikersgroep (principal) waarvoor beveiligingsrechten zijn gewijzigd.

Wijziging van controle

De controle-instellingen van het systeem zijn gewijzigd.

- Gebeurtenistype-id: 10006

Gebeurtenisdetail	Id	Beschrijving
Gebeurtenistype-id	58	Registreert de id van het controlegebeurtenistype dat is in- of uitgeschakeld. Als meerdere

Gebeurtenisdetail	Id	Beschrijving
		gebeurtenistypen worden in- of uitgeschakeld in één actie, wordt een gebeurtenisdetail gegenereerd voor elk gebeurtenistype.
Actie	59	Registreert welke controlegebeurtenissen zijn in- of uitgeschakeld.
Nieuw controleniveau	60	Als het controleniveau van details wordt gewijzigd, wordt de nieuwe niveauinstelling geregistreerd (bijvoorbeeld uit, minimaal of standaard).
Oud controleniveau	61	Als het controleniveau van details wordt gewijzigd, wordt de vorige niveauinstelling geregistreerd (bijvoorbeeld uit, minimaal of standaard).
Controleoptie	62	Als een optioneel detail wordt in- of uitgeschakeld, wordt geregistreerd welk detail is gewijzigd en of het in- of uitgeschakeld is. Als meerdere details in één actie worden in- of uitgeschakeld, wordt een detailrecord gegenereerd voor elk gewijzigd detail.
ADS-verbinding	78	Als de verbinding met Gegevensopslag controleren wordt gewijzigd, worden hiermee de nieuwe verbindingsinstellingen geregistreerd met de volgende indeling: `DBType=Oracle,DBName=MyADS,Username=USR1,Password="*****",SSO=off,DBReconnect=on`. Alleen de gewijzigde details worden geregistreerd. Als bijvoorbeeld alleen de gebruikersnaam wordt bijgewerkt, wordt alleen `Gebruikersnaam="nieuw"` geregistreerd. **Opmerking** De wachtwoordgegevens worden in de database altijd verborgen met *.
Interval voor automatisch verwijderen	105	Dit detail registreert wijzigingen van het veld *Gebeurtenissen verwijderen die ouder zijn dan* op de pagina CMC controleren. Dit bepaalt hoeveel dagen controlegegevens worden bewaard in het ADS.

24.3.1.2 Commentaargebeurtenissen

De volgende rechten zijn specifiek van toepassing op het **BI-commentaar** in Business Intelligence-platform.

Opmerking toevoegen

Deze gebeurtenis wordt gegenereerd als u een nieuwe opmerking toevoegt, een dubbele opmerking invoert en als u massaal opmerkingen toevoegt. Als u een opmerking toevoegt, wordt alleen de id van bovenliggend document vastgelegd. Als u dubbele of massaal opmerkingen toevoegt, worden alle gebeurtenisdetails in de onderstaande tabel vastgelegd.

Gebeurtenistype-id: 11001

Gebeurtenisdetail	Id	Beschrijving
Bovenliggende document-id	12	De id van het object wordt vastgelegd.
Beschrijving	24	Aanvullende informatie in de gebeurtenis wordt vastgelegd.
Grootte	17	Grootte van het object (in bytes) dat onderwerp is van de gebeurtenis.
Bestandsnaam	18	De bestandsnaam van het object wordt vastgelegd.

Opmerking ophalen

De gebeurtenis wordt gegenereerd als u een opmerking bekijkt.

Gebeurtenistype-id: 11002

Gebeurtenisdetail	Id	Beschrijving
Bovenliggende document-id	12	De id van het object wordt vastgelegd.
Grootte	17	Grootte van het object (in bytes) dat onderwerp is van de gebeurtenis.

Opmerking wijzigen

De gebeurtenis wordt gegenereerd als u een bestaande opmerking bewerkt.

Gebeurtenistype-id: 11003

Gebeurtenisdetail	Id	Beschrijving
Bovenliggende document-id	12	De id van het object wordt vastgelegd.

Opmerking verwijderen

De gebeurtenis wordt gegenereerd als u een bestaande opmerking verwijdert.

Gebeurtenistype-id: 11004

Gebeurtenisdetail	Id	Beschrijving
Bovenliggende document-id	12	De id van het object wordt vastgelegd.

Opmerking verbergen

De gebeurtenis wordt gegenereerd als u een opmerking verbergt.

Gebeurtenistype-id: 11005

Gebeurtenisdetail	Id	Beschrijving
Bovenliggende document-id	12	De id van het object wordt vastgelegd.

24.3.1.3 SAP BusinessObjects Web Intelligence-gebeurtenissen

De volgende gebeurtenissen zijn specifiek voor het SAP BusinessObjects Web Intelligence-onderdeel.

Analyse uitvoeren buiten analyseniveau

Gebruiker heeft een analyse uitgevoerd buiten het analyseniveau van het rapport.

- Gebeurtenistype-id: 10201

Gebeurtenisdetail	Id	Beschrijving
Objectexemplaar	11	Registreert of de gebeurtenis het resultaat is van een geplande update of een gebruiker die het object weergeeft ('0' = resultaat van een gebruiker die het object weergeeft, '1' = resultaat van een geplande update van het object).
Aantal rijen	63	Het aantal rijen dat de databaseserver retourneert.
Query	25	Registreert de query die wordt gebruikt om de gegevens te vernieuwen (optioneel, ingesteld in CMC).
Naam van universeobject	31	De naam van de universe die het document gebruikt. Een exemplaar wordt geregistreerd voor elke universe die wordt geopend door het document.
Universe-id	32	De CUID van de universe die het document gebruikt. Een exemplaar wordt geregistreerd voor elke universe die wordt geopend door het document.

Pagina opgehaald

Pagina uit Web Intelligence-document is opgehaald.

- Gebeurtenistype-id: 10202

Gebeurtenisdetail	Id	Beschrijving
Naam WebIntelligence-rapport	10220	De naam van het WebIntelligence-document dat wordt bekeken, wordt geregistreerd.
Uitvoersoort	10221	De uitvoerindeling van het document dat wordt bekeken, bijvoorbeeld: • `xml.ro` voor WebIntelligence • `pdf` voor Adobe Acrobat • `xls` voor Microsoft Excel • `text/xml` indien onbekend
Paginanummer	10222	De naam van de WebIntelligence-rapportpagina die wordt bekeken, wordt geregistreerd. NB: • "0" wanneer het niet kan worden opgehaald (bijv. pdf)

Gebeurtenisdetail	Id	Beschrijving
		• "-1" in het geval van een fout

BW-statistiek

> **Opmerking**
>
> Deze controlegebeurtenissen worden rechtstreeks naar SAP BW verzonden. Ze worden hieronder ter referentie vermeld als Web Intelligence-gebeurtenissen, maar worden niet opgeslagen in de Auditing Data Store van het BI-platform. Ze zijn beschikbaar sinds 4.2 SP03.

Optie	Mogelijke waarden	Beschrijving

Lange naam
`sap.sal.bics.postBWstatistics`
Korte naam
`postBWstatistics`
Standaardwaarde: `false`
	`true`
	`false`
		Activeert de volgende BW-statistiekgebeurtenissen:
		• 20100: haalt kenmerkleden van BEx op
		• 20101: haalt resultaten van BEx-query op
		• 20102: dient BEx-variabelen in
		• 20103: opent een BEx-query via BICS API
		• 20104: synchroniseert met BW
		• 20105: stelt invoertekenreeks van variabele in

24.3.1.4 SAP BusinessObjects Analysis, editie voor OLAP-gebeurtenissen

MDSAS-sessie

Er wordt een MDAS-sessie uitgevoerd

- Gebeurtenistype-id: 10300
- Statussen:
  - "0" = Nieuwe sessie geopend.
  - "1" = Nieuwe sessie mislukt.
  - "2" = Bestaande sessie gesloten.

MDAS-kubusverbinding

Er wordt een kubusverbinding uitgevoerd.

- Gebeurtenistype-id: 10301
- Statussen:
  - "0" = Nieuwe verbinding geopend.
  - "1" = Nieuwe verbinding mislukt.
  - "2" = Bestaande verbinding gesloten.

Gebeurtenisdetail	Id	Beschrijving
Verbindings-id	94	Unieke id van de verbinding.
Verbindingsnaam	95	De naam van de verbinding.
Type provider	96	Het type provider voor de kubus.
Naam van kubus	97	De volledige naam van de kubus die wordt gebruikt.

24.3.1.5 Gebeurtenissen van console voor Promotiebeheer van SAP BusinessObjects

De volgende gebeurtenissen zijn uniek voor het onderdeel Promotiebeheer voor SAP BusinessObjects.

Algemene details van Hulpprogramma voor Promotiebeheer van SAP BusinessObjects

Alle gebeurtenissen voor Promotiebeheer bevatten de volgende extra gebeurtenisdetails.

Gebeurtenisdetail	Id	Beschrijving
Elementcluster	6	De CUID van de betrokken clusters wanneer het hulpprogramma voor promotiebeheer een bewerking uitvoert op objecten in verschillende clusters. Er wordt een gebeurtenisdetail gegenereerd voor elke betrokken cluster.
Elementopmerking	7	Aanvullende informatie over het object.
Primair element	8	Als het element een primair element is, wordt dit detail op '1' ingesteld; als het een afhankelijk element is, wordt het op '0' ingesteld.

Gebeurtenisdetail	Id	Beschrijving
Elementstatus	9	Als het bewerkingselement mislukt, wordt dit detail op '1' ingesteld, anders op '0'.
Bewerking	10	Beschrijft het type bewerking dat wordt uitgevoerd (bijvoorbeeld Toevoegen, Verwijderen of Wijzigen).

Configuratie van Hulpprogramma voor Promotiebeheer van SAP BusinessObjects

Configuratie van Promotiebeheer is gewijzigd.

- Gebeurtenistype-id: 10900

Gebeurtenisdetail	Id	Beschrijving
Configuratie	100	Een gebruiker bekijkt de configuratie van het hulpprogramma voor promotiebeheer. De configuratie wordt weergegeven als door komma's gescheiden waardeparen, bijvoorbeeld: instellingen ongedaan maken=ingeschakeld, poort=900.
Configuratie voor	101	Als de instellingen van het hulpprogramma voor promotiebeheer voor een object zijn gewijzigd, worden de vorige configuratie-instellingen vastgelegd. Gebruikt dezelfde indeling als Configuratie.
Configuratie na	102	Als de instellingen van het hulpprogramma voor promotiebeheer voor een object zijn gewijzigd, worden de nieuwe configuratie-instellingen vastgelegd. Gebruikt dezelfde indeling als Configuratie.
Type VMS	10900	De versie van het beheersysteem.

Terugzetten

Een object is teruggedraaid naar een vorige VMS-versie (Version Management System).

- Gebeurtenistype-ID: 10901

Toevoegen aan VMS

Er wordt een bron toegevoegd aan het VMS.

- Gebeurtenistype-ID: 10902

Gebeurtenisdetail	Id	Beschrijving
Versie	104	Registreert het versienummer van het document in het versiebeheersysteem.

Ophalen uit VMS

Een bron wordt opgehaald uit het VMS.

- Gebeurtenistype-ID: 10903

Gebeurtenisdetail	Id	Beschrijving
Verwijderd object herstellen	103	Geeft aan of een opgehaald object was verwijderd uit het systeem. '0' geeft aan dat het object niet was verwijderd; '1' geeft aan dat het object was verwijderd.
Versie	104	Registreert het versienummer van het document in het VMS.

Inchecken in VMS

Een bron wordt ingecheckt in het VMS.

- Gebeurtenistype-ID: 10904

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het VMS.

Uitchecken uit VMS

Een bron wordt uitgecheckt uit het VMS.

- Gebeurtenistype-ID: 10905

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het VMS.

Exporteren naar VMS

Een bron wordt geëxporteerd uit het VMS.

- Gebeurtenistype-ID: 10906

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het VMS.

VMS-vergrendeling

Een bron in het VMS is vergrendeld om te voorkomen dat gebruikers deze bewerken.

- Gebeurtenistype-ID: 10907

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het VMS.
Vergrendeld door	10901	De gebruikersnaam van de gebruiker die de actie heeft uitgevoerd.

VMS-ontgrendeling

Een bron in het VMS wordt ontgrendeld waardoor gebruikers deze kunnen bewerken.

- Gebeurtenistype-ID: 10908

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het VMS.
Ontgrendeld door	10902	De gebruikersnaam van de gebruiker die de actie heeft uitgevoerd.

VMS verwijderen

Een bron wordt verwijderd uit het VMS.

- Gebeurtenistype-ID: 10909

Gebeurtenisdetail	ID	Beschrijving
Versie	104	Registreert het versienummer van het document in het versiebeheersysteem.

25 Gebeurtenissen

25.1 Over gebeurtenissen

Gebeurtenissen zijn vergelijkbaar aan vlaggen of controlepunten die informatie bieden over gebeurtenissen of acties die op de server plaatsvinden. Plannen op basis van gebeurtenissen geeft u extra controle voor het plannen van objecten: u kunt gebeurtenissen zo instellen dat objecten alleen worden verwerkt nadat een bepaalde gebeurtenis heeft plaatsgevonden.

Hier is een lijst met gebeurtenissen die beschikbaar zijn op de CMC:

Crystal Reports-gebeurtenissen

Crystal Reports-gebeurtenissen activeren alleen een rapportuitvoering als het rapport dat op de gebeurtenis wacht al is gepland en klaar is om uitgevoerd te worden. Crystal Reports-gebeurtenissen kunnen worden gebaseerd op een nieuw bestand en rapporten kunnen worden gepland om te wachten op gebeurtenisactivering.

Aangepaste gebeurtenissen

Aangepaste gebeurtenissen worden ook wel "handmatige gebeurtenissen" genoemd. Elke aangepaste gebeurtenissen heeft twee eigenschappen: de naam van de gebeurtenis en de bijbehorende beschrijving. Aangepaste gebeurtenissen worden ook gebruikt om meldingen te activeren voor een postvak IN voor BI en e-mail-ID van een gebruiker. Met aangepaste gebeurtenissen kunt u ook objecten plannen op basis van gebeurtenisactivering door de vereiste voorwaarden in te stellen.

Toezichtgebeurtenissen

Toezichtgebeurtenissen zijn door het systeem gegenereerde gebeurtenissen die te maken hebben met de gezondheidsstatus van de service. Toezicht is een in de CMC ingebouwde toepasing waarmee beheerders de gezondheid van het systeem kunnen controleren. De belangrijkste aspecten van toezicht zijn controles en testen.

Controles maken het mogelijk om drempels voor meer dan 250 gegevens in te stellen in het systeem. U ontvangt een bericht als de ingestelde drempel wordt overschreden.

> Voorbeeld
>
> Als u een controle hebt die de door de uitvoer-FRS gebruikte schijfruimte controleert, wordt u ervan op de hoogte gesteld als het verbruik de opgegeven hoeveelheid schuifruimte bereikt.

Systeemgebeurtenissen

Er zijn twee typen systeemgebeurtenissen:

- **Bestandsgebeurtenissen**
  Bestandsgebeurtenissen zijn gebaseerd op een bestand op een locatie met een pad. Bijvoorbeeld: als een bestand op een van de serverpaden staat, kunt u rapporten uitvoeren door planning op basis van het pad van een bestand. Vanuit een zakelijk oogpunt, als de vereiste tabellen voor rapportage worden geladen op een maandelijkse/wekelijkse/dagelijkse basis, dan activeert het plaatsen van een tekstbestand op een pad, nadat de rapporten zijn geladen, een op een bestand gebaseerde systeemgebeurtenis.
- **Planninggebaseerde gebeurtenissen**
  Planninggebaseerde gebeurtenissen worden gebruikt om rapporten of BI-objecten op een bepaalde volgorde uit te voeren. Deze gebeurtenisdefinitie omvat drie acties: succes, mislukking en succes of mislukking. Dit is omdat de status van een object in uitvoering op elk moment in tijd een succes of een mislukking kan zijn.

Gebruikersberichten

Gebeurtenissen gebruikersberichten worden gebruikt door beheerders om BI-eindgebruikers die BI-startpunt gebruiken berichten te sturen over belangrijke gebeurtenissen. Beheerders kunnen geselecteerde gebruikers berichten sturen over kritieke meldingen en andere gerelateerde informatie op de geplande tijd (bijvoorbeeld systeemuitvaltijd). Het meldingsbericht verschijnt als een berichtpop-up in het BI-startpuntscherm als de gebruiker zich aanmeldt.

BW-gebeurtenissen

In het BW-systeem start de *gebeurtenis BOE starten*, een procestype in een BW-procesketen BW-gebeurtenissen voor het BI-platform. Elke BW-gebeurtenis omvat een gebeurtenisnaam en de bijbehorende beschrijving. BW-gebeurtenissen worden gebruikt voor het configureren van een op gebeurtenissen gebaseerd schema van rapporten die op een BW-gegevensbron worden gebaseerd. Een BW-systeem start een BW-gebeurtenis wanneer gegevens in het systeem worden gewijzigd. BW-gebeurtenissen kunnen ook meldingen activeren voor een postvak IN voor BI en e-mail-ID van een gebruiker.

25.1.1 Gebruikersberichten

Berichtgevingsfuncties maken het een beheerder mogelijk om meldingsberichten van de CMC naar de gebruiker te verzenden. Met behulp van deze functie kunnen beheerders geselecteerde gebruikers op de hoogte stellen van kritieke meldingen en andere gerelateerde informatie (bijvoorbeeld systeemuitvaltijd). Het meldingsbericht verschijnt als een berichtpop-up in de rechterbovenhoek van het BI-startpuntscherm als de gebruiker zich aanmeldt.

25.1.1.1 Een gebeurtenis berichtgeving maken

De gebeurtenis berichtgeving is een planbare invoegtoepassing. Bij het maken van een nieuwe gebeurtenis berichtgeving moet de beheerder de begin- en einddatum en -tijd opgeven. De Adaptive Job Server die verantwoordelijk is voor planning maakt een planningsexemplaar als de opgegeven begintijd van het bericht is bereikt. De AJS stuurt de melding dan naar het Postvak IN voor meldingen in het startpunt. Deze berichten worden weergegeven in de rechterbovenhoek van het BI-startpuntscherm.

Doe het volgende om een gebeurtenis berichtgeving te maken:

1. Meld u aan bij de CMC.
2. Selecteer *Gebeurtenissen* in het vervolgkeuzemenu op de CMC-startpagina.
3. Klik met de rechtermuisknop in het deelvenster *Gebeurtenissen* aan de linkerkant op *Gebruikersberichten* en navigeer naar *Nieuw* > *Nieuwe berichtgeving*.

   Het pop-upvenster *Nieuwe berichtgeving* wordt weergegeven.
4. Doe het volgende om een berichtgevingsmelding te plannen:
   a. Selecteer de vereiste tijdzone in het vervolgkeuzemenu *Tijdzone*.
   b. Stel de vereiste *Startdatum/-tijd* in.
   c. Stel de vereiste *Einddatum/-tijd* in.

   > **Opmerking**
   >
   > - De *eind*tijd kan niet eerder zijn dan de *start*tijd.
   > - Het verschil tussen de *start*- en *eind*tijd mag niet meer zijn dan 14 dagen.
   > - Onafhankelijk van de geselecteerde tijdzone mag de *start*tijd niet eerder zijn dan de CMS-servertijd. Als de *start*tijd eerder is dan de CMS-servertijd wordt de berichtgeving niet gestart.

   d. Voer in het vak *Titel berichtgeving* de titel van de berichtgeving in.

   > **Opmerking**
   >
   > De *Titel berichtgeving* kan niet meer dan 256 tekens lang zijn.

   e. Voer in het vak *Beschrijving* een geschikte beschrijving voor de berichtgeving in.

   > **Opmerking**
   >
   > De *Beschrijving* kan niet meer dan 1024 tekens lang zijn.

   > **Opmerking**
   >
   > U kunt ervoor kiezen om de berichtgeving naar het e-mailadres van de gebruiker te verzenden door het selectievakje *Dit bericht naar de e-mail-id van gebruiker sturen* te selecteren.
5. Selecteer *OK*.

U hebt nu een gebeurtenis berichtgeving gemaakt.

> **Opmerking**
>
> De tijdstippen van aanmaak en wijziging op de pagina 'Eigenschappen berichtgeving' geven de CMS-servertijd weer.

De beheerder kan de automatische pop-up van de berichtgevingsbanner in het BI-startpunt uitschakelen door het bestand `BIlaunchpad.properties` aan te passen en de polling uit te schakelen door het veld `Notification.enabled` in te stellen op `false`. Om berichtgevingspolling standaard in te schakelen moet de eigenschap `pinger.enabled` in het bestand `global.properties` ingeschakeld zijn. Als polling en pinger niet zijn ingeschakeld, wordt de berichtgevingspop-up alleen weergegevens als een gebruiker de pagina vernieuwt, zich voor de eerste keer aanmeldt of zich opnieuw aanmeldt terwijl het bericht actief is.

Polling vindt om de drie minuten plaats in het BI-startpunt.

25.1.1.2 Een berichtpubliek selecteren

Met berichtgevingsfuncties kunt u het vereiste publiek selecteren voor elk bericht dat u maakt.

Doe het volgende om het publiek voor een bericht te selecteren:

1. Klik met de rechtermuisknop op het bericht dat u hebt gemaakt en selecteer *Abonnees beheren* in het snelmenu.

   Het pop-upvenster *Abonnees beheren* wordt weergegeven.
2. Selecteer *Toevoegen* in het deelvenster *Abonneelijst*.

   Het pop-upvenster *Abonnees toevoegen* wordt weergegeven.
3. Selecteer de vereiste gebruiker/gebruikersgroepen die u bericht wilt sturen.
4. Selecteer *Standaardabonnement(en) toevoegen*.

   Het pop-upvenster *Abonnees toevoegen* verdwijnt.
5. Selecteer *Opslaan en sluiten* in het pop-upvenster *Abonnees beheren*.

U hebt nu het publiek voor een bericht geselecteerd.

ⓘ Opmerking

- U kunt de abonneelijst niet meer wijzigen nadat het bericht is verzonden.
- U kunt nu meldingen naar de OpenDocument-gebruikers verzenden.

25.1.1.3 Een gebeurtenis berichtgeving bewerken

Doe het volgende om een gebeurtenis berichtgeving te bewerken:

1. Meld u aan bij de CMC.
2. Selecteer *Gebeurtenissen* in het vervolgkeuzemenu op de CMC-startpagina.
3. Selecteer *Gebruikersberichten* in het deelvenster *Gebeurtenissen* aan de linkerkant.
4. Klik met de rechtermuisknop op het bericht dat u wilt bewerken en selecteer *Gebeurtenis bewerken* in het snelmenu.

   Het dialoogvenster *Gebeurtenis bewerken* verschijnt.

5. Bewerk de vereiste parameters van de gebeurtenis berichtgeving.

> **Opmerking**
>
> U kunt de volgende parameters van een gebeurtenis berichtgeving bewerken:
>
> - Tijdzone
> - Begindatum/tijd
> - Einddatum/tijd
> - Titel berichtgeving
> - Beschrijving
> - Abonnees beheren

6. Selecteer *OK*.

U hebt nu een gebeurtenis berichtgeving bewerkt.

> **Opmerking**
>
> Als u een gebeurtenis berichtgeving bewerkt door te navigeren naar *Gebeurtenissen* > *Gebruikersberichten* > *Eigenschappen* wordt de berichtgeving pas gestart als u *OK* selecteert op de pagina *Gebeurtenis bewerken*.

26 Platform zoeken

26.1 Hoe Platform zoeken werkt

Met Platform zoeken kunt u naar inhoud zoeken binnen de gegevensopslagruimte van BI-platform. De zoekresultaten worden ingedeeld in categorieën en geclassificeerd op basis van relevantie.

In deze versie van het BI-platform bevat Platform zoeken de volgende functies:

- Zoeken naar BI-platforminhoud.
- Een query stellen voor het maken van een document als er geen bestaand document gevonden kan worden.
- Continu en geplande indexering ondersteunen.
- Indexering in een geclusterde omgeving ondersteunen.
- Het niveau van indexering instellen en aanpassen.
- Geavanceerde configuratieopties voor zoeken bieden.
- Zoeken en indexeren in meerdere talen ondersteunen.
- Geavanceerde zoeksyntaxis bieden.
- Metagegevens, inhoud en dynamische facetten ondersteunen.
- Zelfherstel op basis van systeembelasting ondersteunen.

> **Opmerking**
>
> Als u migreert van de oudere versie naar een nieuwe versie, wordt de index niet gemigreerd.

26.1.1 SDK van Platform zoeken

Platform zoeken ondersteunt tevens een openbare SDK die functioneert als interface tussen de clienttoepassing en Platform zoeken. Het is algemeen beschikbaar om u te helpen bij het aanpassen van de zoekservice en deze te integreren met uw toepassing.

Wanneer een zoekopdrachtparameter via de clienttoepassing naar de SDK-laag wordt verzonden, wordt de opdrachtparameter door de SDK-laag naar een XML-gecodeerde indeling geconverteerd en vervolgens doorgestuurd naar de service voor Platform zoeken.

Zie de *Business Intelligence platform Java API-referentie* voor meer informatie over de API van Platform zoeken.

26.1.2 Geclusterde omgeving

Met Platform zoeken kan de belasting over meerdere knooppunten verdeeld worden in een geclusterde omgeving. De implementatie in een geclusterde omgeving optimaliseert systeembronnen en verbetert serverprestaties.

Platform zoeken biedt ondersteuning voor zowel horizontale als verticale clustervorming voor de functies Zoeken en Indexeren. Bij geclusterde omgevingen worden de prestaties van zoek- en indexeringsprocessen geoptimaliseerd.

Controleer deze SAP Note voor meer informatie over de configuratie van een indexlocatie voor Platform zoeken in een geclusterde omgeving.

Taakverdeling

Platform zoeken ondersteunt taakverdeling voor indexeren en zoeken. In een geclusterde omgeving kunnen indexeer- en zoekopdrachten worden uitgevoerd op meerdere knooppunten om zo de systeembelasting te verdelen. Elk knooppunt kan onafhankelijk inhoud indexeren en delta-indexen maken. Slechts één knooppunt in het cluster kan als hoofdindex dienen en de delta-indexen samenvoegen in de hoofdindex. Alle knooppunten hebben toegang tot de hoofdindex. Hierdoor zijn gelijktijdige zoekopdrachten mogelijk.

Failover

Dit betekent dat gebruikers kunnen blijven zoeken en indexeren zonder onderbreking. Wanneer een knooppunt in het cluster niet meer beschikbaar is door een technisch mankement of onderhoudsactiviteiten, worden de indexeer- en zoekopdrachten automatisch door een ander knooppunt overgenomen.

26.2 Platform zoeken instellen

26.2.1 OpenSearch implementeren

Platform zoeken ondersteunt de OpenSearch-standaard, waardoor de clienttoepassingen deze standaard of indeling kunnen gebruiken om met Platform zoeken te communiceren. OpenSearch wordt niet standaard geïnstalleerd met de SAP BusinessObjects Business Intelligence-suite, dus gebruikers moeten deze toepassing als een apart WAR-bestand `opensearch.war` handmatig implementeren op een toepassingsserver zoals Tomcat of met het hulpprogramma WDeploy. Dit bestand wordt door het installatieprogramma gekopieerd naar de map `<INSTALLATIEMAP>\warfiles\OpenSearch`.

> **Opmerking**
>
> Clientprogramma's moeten de OpenSearch-standaarden volgen om met Platform zoeken te communiceren.

> **Opmerking**
>
> Wanneer u het BI-platform installeert, wordt de Tomcat-toepassingsserver standaard geïnstalleerd.

26.2.1.1 Handmatig implementeren

Als u OpenSearch in een BI-platformomgeving wilt implementeren, voert u de volgende stappen uit:

1. Ga naar de volgende locatie: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Kopieer de OpenSearch-map naar `<INSTALLATIEMAP>\tomcat\webapps\`.
3. Wijzig de configuratieparameters in het bestand `\OpenSearch\WEB-INF\config.properties`:
   - CMS: de CMS-naam met poortnummer: `<CMS-naam>:<Poortnummer>`.
   - OpenDocURL: de URL van de OpenDocument-toepassing: `http://<tomcathost>:<connectorpoort>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   - Proxy.rpurl: de omgekeerde proxy-servernaam is verplicht als u omgekeerde proxy wilt gebruiken.
   - Proxy.opendoc.rpurl: de naam van de opendoc reverse proxy-server is verplicht als u de reverse proxy wilt gebruiken.
4. Start de Tomcat-toepassingsserver opnieuw voor het implementeren van OpenSearch.

26.2.1.2 Implementeren met WDeploy

Voor Windows worden opdrachten beschreven als `wdeploy.bat <parameters>`. Voor UNIX worden opdrachten beschreven als `wdeploy.sh <parameters>`.

1. Werk het bestand `config.<ApplicationServer>` bij, dat zich bevindt in `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf`, zodat het de vereiste parameters voor de webtoepassingsserver bevat (bijvoorbeeld installatiemap, exemplaarnaam, beheerderspoort, gebruikersnaam en wachtwoord van de beheerder).
2. Wijzig de volgende parameters in het bestand `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties` :
   a. Voor de parameter `CMS` voert u in: `<CMSnaam>:<Poort>`.
   b. Voor de parameter `OpenDocURL` voert u de URL van de OpenDocument-toepassing in.

      De URL moet zijn: `http://<WebApplicationServerHost>:<ConnectorPort>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   c. (Vereist voor omgekeerde proxy) Voor de parameter `Proxy.rpurl` voert u de naam in van de omgekeerde-proxyserver.
   d. (Vereist voor omgekeerde proxy) Voor de parameter `Proxy.opendoc.rpurl` voert u de naam in van de omgekeerde-proxyserver van de OpenDocument-toepassing.
3. Voer de opdracht `wdeploy.bat <WebApplicationServer> -Dapp_source_tree=<ParentFolderOpenSearchWebApp> -DAPP=OpenSearch deploy` uit `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy` uit.

Met de volgende opdracht wordt bijvoorbeeld OpenSearch geïmplementeerd op een WebSphere 7-webtoepassingsserver:

```
wdeploy.bat websphere7 -Dapp_source_tree="<InstallDir>\SAP BusinessObjects
Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

4. Start de webtoepassingsserver opnieuw.

26.2.2 Reverse proxy configureren

Voor het implementeren van webtoepassingen op een webtoepassingsserver die zich achter een reverse-proxyserver bevindt, configureert u de reverse-proxyserver voor het toewijzen van inkomende URL-verzoeken aan het juiste WAR-bestand.

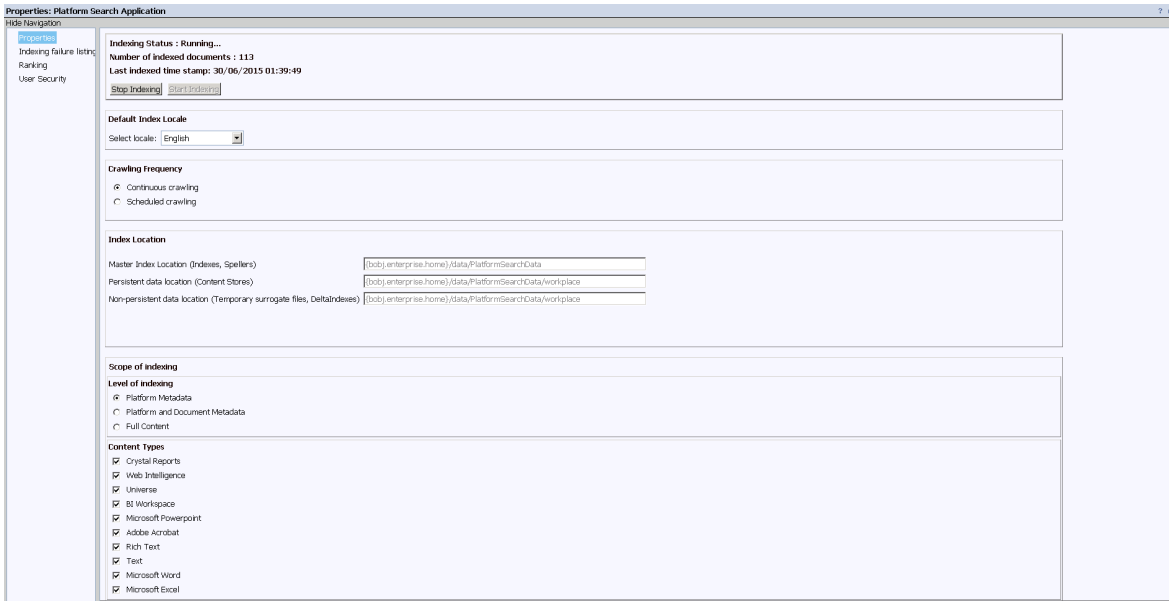
Voor het illustreren van de configuratiestappen gebruiken wij de reverse-proxyserver van Apache 2.2 als voorbeeld. De reverse-proxyserver van Apache 2.2 configureren voor OpenSearch:

1. Stel de reverse proxy in en breng de wijzigingen aan in het bestand `WEB-INF\config.properties` van OpenSearch.
2. Schakel de volgende contextparameters in en wijzig de waarden dienovereenkomstig.
   - `proxy.rpurl`: Dit is de URL van de reverse proxy voor OpenSearch (bijvoorbeeld `http://IPadresComputer/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: Dit is de URL van de reverse proxy voor Open Doc (bijvoorbeeld `http://IPadresComputer/RP/BOE/`).
3. Werk het bestand `httpd.conf` in de Apache Reverse Proxy-installatiemap bij met de volgende instellingen:
   - `ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat-host>:<Connectorpoort>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<Tomcat-host>:<Connectorpoort>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Start de Apache 2.2 Reverse-proxyserver opnieuw op.

26.2.3 Toepassingseigenschappen configureren in de CMC

Voer de volgende stappen uit om de toepassingseigenschappen van Platform zoeken te configureren:

1. Ga naar het beheergebied *Toepassingen* in de CMC.
2. Selecteer de *toepassing Platform zoeken*.
3. Klik op *Beheren* > *Eigenschappen*. Het dialoogvenster *Eigenschappen* wordt weergegeven.



4. Configureer de instellingen voor Platform zoeken:

Optie	Beschrijving
Zoekstatistieken	Platform zoeken biedt de volgende zoekstatistieken: • Indexeringsstatus: hiermee wordt de status van het indexeringsproces weergegeven. • Aantal geïndexeerde documenten: hiermee wordt het aantal documenten weergegeven dat is geïndexeerd. • Laatst geïndexeerde tijdstempel: hiermee wordt de tijdstempel weergegeven waarmee het document voor het laatst is geïndexeerd.
Indexeren stoppen/starten	Met de opties voor het starten of stoppen van de indexering kunt u het indexeringsproces starten of stoppen wanneer u wilt omschakelen van continu naar gepland verkennen, of voor onderhoudsdoeleinden. Klik op *Indexering stoppen* om het indexeren te stoppen.
Standaardindex van de landinstelling	Platform zoeken maakt gebruik van de landinstelling die in de CMC is opgegeven voor indexering van alle niet-gelokaliseerde BI-documenten. Nadat het document is gelokaliseerd, wordt de toepasselijke taalanalyse gebruikt voor indexering. Zoekopdrachten zijn gebaseerd op de productlandinstelling van de client, en het gewicht dat de productlandinstelling van de client heeft. U kunt het gewicht aanpassen in de eigenschappen van de CMC-configuratie.

Optie	Beschrijving
Frequentie voor verkennen	U kunt de volledige BI-platformgegevensopslagruimte indexeren aan de hand van de volgende opties: • Continu verkennen: met deze optie is indexering een continu proces waarbij de gegevensopslagruimte wordt geïndexeerd wanneer er een object wordt toegevoegd, gewijzigd of verwijderd. Zo kunt u de meest up-to-date inhoud van BI-platform bekijken en ermee werken. Met continu verkennen wordt de gegevensopslagruimte voortdurend bijgewerkt met de acties die u uitvoert. Deze optie is standaard ingesteld. Continu verkennen werkt zonder tussenkomst van de gebruiker en beperkt de tijd die het indexeren van een document in beslag neemt. • Gepland verkennen: met deze optie is indexering gebaseerd op een planning die is ingesteld met de opties in Planning. Voor meer informatie over het plannen van een object raadpleegt u de sectie *Een object plannen* van Platform zoeken in de *online-Help voor SAP BusinessObjects Business Intelligence-platform CMC*. **Opmerking** • Als u *Gepland verkennen* selecteert en het *Terugkeerpatroon* instelt op een andere optie dan *Nu*, geeft Platform zoeken de datum- en tijdstempel weer waarop het document wordt gepland om opnieuw te indexeren. • Als u *Gepland verkennen* selecteert, is de knop *Indexeren starten* ingeschakeld en de knop *Indexeren stoppen* uitgeschakeld. • Nadat de planning voltooid is, wordt de knop *Indexeren stoppen* ingeschakeld.

Optie	Beschrijving
Indexlocatie	De indexen worden opgeslagen in gedeelde mappen op de volgende locaties: • Hoofdindexlocatie (indexen en speller): de hoofd- en spellerindexen zijn opgeslagen op deze locatie. Tijdens een zoekactie worden de eerste resultaten opgehaald met de hoofdindex en worden de spellerindexen gebruikt om suggesties op te halen. In een geclusterde implementatie van BI-platform moet deze locatie een gedeelde bestandssysteem zijn dat toegankelijk is vanuit alle knoppunten in het cluster. • Permanente gegevenslocatie (inhoudsopslag): de inhoudsopslag bevindt zich op deze locatie. Deze is gemaakt op basis van de hoofdindexlocatie en blijft ermee gesynchroniseerd. De inhoudsopslag wordt gebruikt om facetten te genereren en de eerste treffers te verwerken die via de locatie van de hoofdindex zijn gegenereerd. In een geclusterde BI-platformimplementatie wordt bij elk knooppunt een inhoudsopslag gegenereerd. De permanente gegevenslocatie is de enige indexlocatie waar de geclusterde omgeving invloed op heeft, omdat de inhoudsopslagmappen zich hier bevinden. Als een computer één zoekservice heeft, is er ook maar één locatie voor inhoudsopslag. Bijvoorbeeld {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam>\ContentStores. Als een geclusterde omgeving echter meerdere zoekservices bevat, heeft elke zoekservice één eigen locatie voor inhoudsopslag. Als er bijvoorbeeld twee exemplaren van een server worden uitgevoerd, zijn de locaties van de inhoudsopslag als volgt: 1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam>\ContentStores. 2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Servernaam 1>\ContentStores. • Niet-permanente gegevenslocatie (tijdelijke bestanden, delta-indexen): op deze locatie worden delta-indexen gemaakt en tijdelijk opgeslagen voordat deze worden samengevoegd met de hoofdindex. De indexen op deze locatie worden verwijderd wanneer ze zijn samengevoegd met de hoofdindex. Daarnaast worden surrogaatbestanden (uitvoer van de extractors) op deze locatie gemaakt en tijdelijk opgeslagen totdat ze geconverteerd worden in delta-indexen. **Opmerking** • Hoofdindexlocatie moet een gedeelde locatie zijn. • U moet op *Indexeren stoppen* klikken om de indexlocatie aan te passen. • Als u een indexlocatie aanpast, kopieert u de inhoud naar een nieuwe locatie, omdat de indexeringsgegevens anders verloren gaan. • De indexbestanden kunnen mogelijk persoonlijke en vertrouwelijke informatie opslaan, met name wanneer u ervoor kiest om documentinhoud te indexeren. U moet alleen een systeemgebruiker toestemming geven voor toegang tot de gedeelde map en u moet de gedeelde mappen in een versleutelde omgeving opslaan om diefstal van gegevens te vermijden.

Optie	Beschrijving

Indexeringsniveau	U kunt op de volgende manieren de inhoud die u wilt zoeken, afstemmen op het indexeringsniveau:
	• Metagegevens van platform: er wordt alleen een index gemaakt van de metagegevens van het platform, zoals titels, trefwoorden en beschrijvingen van documenten. Standaard is deze optie geselecteerd.
	• Metagegevens van platform en documenten: in deze index zijn de metagegevens van platform en documenten inbegrepen. De metagegevens van het document bestaan onder meer uit de aanmaakdatum, de wijzigingsdatum en de naam van de auteur.
	• Volledige inhoud: in deze index zijn de metagegevens van platform en documenten inbegrepen, evenals andere inhoud zoals:
	  • De eigenlijke inhoud van het document
	  • De inhoud van aanwijzingen en zoeklijsten
	  • Diagrammen, grafieken en labels
	Opmerking
	Volledig indexeren van de inhoud wordt niet ondersteund voor Analysis Office- en Lumira-documenten. Alleen het indexeren van de metagegevens wordt ondersteund voor Analysis Office- en Lumira-documenten.
	Opmerking
	Wanneer u het indexeringsniveau aanpast, wordt de indexering geïnitialiseerd om de volledige BI-platformgegevensopslagruimte te vernieuwen.

Optie	Beschrijving
Inhoudstypen	U kunt de volgende inhoudstypen selecteren voor indexering: • Crystal Reports • Web Intelligence • Universe • BI-werkruimte • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • RTF-tekst • Tekst • Microsoft Word • Microsoft Excel Het inhoudtypefilter is niet van toepassing op indexering van platformmetagegevens. Onafhankelijk van de inhoudtypen die u selecteert, vindt het indexeren van platformmetagegevens plaats voor alle ondersteunde objecttypen, en de zoekresultaten in BI-startpunt geven alle objecten voor het trefwoord gerelateerd aan platformmetagegevens als resultaat. Het inhoudstypefilter is relevant voor het indexeren van documentmetagegevens (documentauteur, documentkoptekst, documentvoettekst enz.) en het indexeren van inhoud (grafieken, diagrammen, tabel bij een rapport). Op basis van het indexeerniveau en de inhoudstypen die u selecteert, worden de documentmetagegevens en de inhoud voor de geselecteerde objecttypen uit de gegevensopslagruimte door platform zoeken geïndexeerd. Alleen die objecten worden in de zoekresultaten van het BI-startpunt weergegeven bij het zoeken naar het trefwoord gerelateerd aan documentmetagegevens en -inhoud.
Index opnieuw maken	Met deze optie wordt de bestaande index verwijderd en wordt de gehele gegevensopslagruimte opnieuw geïndexeerd. U kunt de optie *Index opnieuw maken* selecteren ongeacht of indexering actief is of is gestopt. De bestaande index wordt verwijderd wanneer u u wijzigingen op de eigenschappenpagina opslaat. Als indexering momenteel is gestopt, begint het opnieuw maken van de index pas wanneer u indexering opnieuw start. Als u niet wilt dat Platform zoeken de documenten opnieuw indexeert, moet u de selectie van *Index opnieuw maken* opheffen voordat u op de knop *Indexering starten* klikt.

Optie	Beschrijving
Documenten die zijn uitgesloten van indexering	De optie *Documenten die zijn uitgesloten van indexering* sluit documenten van indexering uit. U wilt bijvoorbeeld niet dat zeer grote Crystal Reports-rapporten doorzoekbaar worden gemaakt, omdat de resources van de Report Application Server anders overbelast raken. Zo wilt u waarschijnlijk ook niet dat publicaties met honderden aangepaste rapporten worden geïndexeerd. Door bepaalde documenten uit te sluiten, kunt u voorkomen dat ze worden geopend door Platform zoeken. Vergeet niet dat een document dat al geïndexeerd is voordat het in deze groep werd geplaatst, mogelijk nog steeds doorzocht kan worden. U moet de index opnieuw maken om ervoor te zorgen dat documenten in de groep *Documenten die zijn uitgesloten van indexering* niet doorzocht kunnen worden. Alleen de beheerdersaccount heeft standaard volledige toegang tot de optie *Documenten die zijn uitgesloten van indexering*. Andere gebruikers met de volgende rechten kunnen alleen documenten toevoegen aan de groep *Documenten die zijn uitgesloten van indexering*: • Weergave- en bewerkingsrechten voor de categorie • Het document rechtstreeks bewerken
Andere configuratie - exemplaar overslaan	Exemplaren van documenten worden standaard geselecteerd voor indexering. Dit zorgt voor een grotere index, die meer schijfruimte gebruikt. De map "Lucene-indexengine" in de map PlatformSearchData wordt enorm groot door de indexering van een zeer groot aantal exemplaren in de gegevensopslagruimte. Als er miljoenen (of meer) documenten zijn en veel van deze documenten ook nog eens een groot aantal bestaande exemplaren hebben (naast geplande exemplaren die regelmatig worden gegenereerd) in het systeem, wordt de map "Lucene-indexengine" te groot, zelfs als het indexeringsniveau wordt ingesteld op "Metagegevens platform". Met de functie Exemplaar overslaan bij zoeken platform kunt u de indexering van exemplaren besturen door via het selectievakje onder 'Andere configuratie - exemplaar overslaan' op de pagina Eigenschappen zoektoepassing platform in CMC in- of uit te schakelen. **Opmerking** • Als u Exemplaar overslaan in- of uitschakelt, moet u de Adaptive Processing Server voor zoeken platform opnieuw starten. Deze wijziging beïnvloedt alle indexeringsniveaus. • Als u Exemplaar overslaan wijzigt en de wijzigingen wilt toepassen op alle bestaande exemplaren (d.w.z. selecteren voor indexering), moet u de index opnieuw maken.

Optie	Beschrijving
Objecten die zijn uitgesloten van indexering	De optie *Objecten die zijn uitgesloten van indexering* sluit objecten van indexering uit. U wilt bijvoorbeeld niet dat bepaalde objecten doorzoekbaar worden gemaakt, omdat de resources van de Report Application Server anders overbelast raken. Door bepaalde objecten uit te sluiten, kunt u voorkomen dat ze worden geopend door Platform zoeken. Vergeet niet dat een object dat al geïndexeerd is voordat het in deze groep werd geplaatst, mogelijk nog steeds doorzocht kan worden. U moet de index opnieuw maken om ervoor te zorgen dat objecten in de groep *Objecten die zijn uitgesloten van indexering* niet doorzocht kunnen worden. Lijst met objecten die kunnen worden uitgesloten van indexering: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • RTF • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • Profiel • Gebeurtenis • Discussies • InformationDesigner • MDAnalysis • Publicatie • Niet-specifiek • Analytisch • Hyperlink • Programma • pQuery • DSL.MetaDataFile • Sneltoets • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

Optie	Beschrijving
	• VISI.Lums • VISILums • Gebruiker • Gebruikersgroep

5. Klik op *Opslaan en sluiten*.

> **Opmerking**
>
> Als een gebruiker de optie *Index opnieuw maken* niet selecteert en het indexeringsniveau wijzigt of extractors selecteert of deselecteert, wordt de index incrementeel bijgewerkt zonder de bestaande index te verwijderen.

26.3 Werken met Platform zoeken

26.3.1 Inhoud indexeren in de CMS-gegevensopslagruimte

Indexering is een continu proces waarbij de onderstaande opeenvolgende taken worden uitgevoerd:

1. Verkennen: verkennen is een proces waarbij de CMS-gegevensopslagruimte wordt gecontroleerd om gepubliceerde, bewerkte of verwijderde objecten te identificeren. Dit kan op twee manieren worden uitgevoerd: continu of gepland.
   Raadpleeg het onderwerp *Toepassingseigenschappen configureren* in de verwante onderwerpen voor meer informatie over continu en gepland zoeken.
2. Uitpakken: hierbij worden de extractors aangeroepen op basis van het documenttype. Voor elk documenttype in de gegevensopslagruimte is er een toegewezen extractor. Nieuwe documenttypen kunnen doorzoekbaar worden gemaakt door nieuwe extractorplug-ins te definiëren. Al deze extractors zijn schaalbaar genoeg om inhoud uit grote documenten met veel records uit te pakken.
   De volgende extractors worden ondersteund:
   - Extractor van metagegevens
   - Crystal Reports-extracto
   - Web Intelligence-extractor
   - Universe-extractor
   - Agnostische extractors (MS Office 2003 en 2007, en PDF-documenten)

   Raadpleeg het onderwerp *Doorzoekbare inhoudtypen* in verwante onderwerpen voor meer informatie over documenttypen die doorzocht kunnen worden.
3. Indexeren: hierbij wordt alle uitgepakte inhoud geïndexeerd via een bibliotheek van een derde partij, genaamd Apache Lucene Engine. De duur van dit proces varieert afhankelijk van het aantal objecten dat zich in het systeem bevindt, plus de grootte en het type documenten.
   Voor het uitvoeren van indexering moeten de voglende servers actief en ingeschakeld zijn:
   - IFRS (Input File Repository Server)
   - OFRS (Output File Repository Server)

- Central Management Server (CMS)
- De APS (Adaptive Processing Server) die de service Platform zoeken host

Als het objecttype is geselecteerd als Web Intelligence- of Crystal Reports-rapport, moet de overeenkomstige Web Intelligence-verwerkingsserver of Crystal Reports-toepassingsserver actief en ingeschakeld zijn voor de respectievelijk geselecteerde objecttypen.

4. Inhoudsopslag: de inhoudsopslag bevat gegevens zoals de id, cuid, naam, soort en het exemplaar dat geëxtraheerd is uit de hoofdindex in een gemakkelijk leesbare indeling. Hiermee wordt het zoekproces bespoedigd.

Verwante informatie

Toepassingseigenschappen configureren in de CMC [pagina 940]
Doorzoekbare inhoudstypen [pagina 951]

26.3.2 Lijst met fouten bij indexering

De lijst met fouten bij indexering geeft een lijst met documenten die niet konden worden geïndexeerd. Bij Platform zoeken worden drie indexeringspogingen gedaan. Als een document niet geïndexeerd kan worden, wordt het weergegeven in de lijst met indexeringsfouten.

U kunt de lijst met fouten bij indexering als volgt weergeven:

1. Ga naar het beheergebied Toepassingen in de CMC.
2. Selecteer de *toepassing Platform zoeken*.
3. Kies *Acties > Lijst met fouten bij indexering*.

   In het dialoogvenster van de toepassing Platform Zoeken wordt een lijst weergegeven met documenten en de volgende details:
   - Titel: hier wordt de titel weergegeven van het document dat niet kon worden geïndexeerd.
   - Type: hier worden de naam van het documenttype, zoals Crystal Reports en Web Intelligence, en de locatie van het document weergegeven.
   - Fouttype: hier worden de foutcode en de reden waarom het document niet kon worden geïndexeerd weergegeven. Klik op de hyperlink Meer info om meer te weten te komen over de stapeltracering van de oorzaak van de fout.
   - Tijdstip van laatste poging: hier wordt het tijdstempel weergegeven van de laatste poging tot indexering van een document.

26.3.3 Door resultaten zoeken

26.3.3.1 Voor het zoeken

26.3.3.1.1 Voorgestelde query'

Bij het gebruik van Platform zoeken kan het zijn dat de gebruiker niet op zoek is naar een bepaald object, maar naar het antwoord op een specifieke vraag. Antwoorden op deze vragen zijn mogelijk beschikbaar in rapporten in de gegevensopslagruimte van het BI-platform.

Platform zoeken analyseert de structuur van universes en bestaande rapporten in uw gegevensopslagruimte en vergelijkt deze informatie met de zoektermen die door de gebruiker zijn opgegeven voor het suggereren van nieuwe SAP BusinessObjects Web Intelligence-query's waarmee gebruikers de antwoorden op hun vragen kunnen vinden.

Voor het maken van potentiële rapporten laat Platform zoeken de woorden in alle universes overeenkomen voor dimensie, meetwaarde, voorwaarde en filterwaarde.

Platform zoeken gaat op zoek naar overeenkomsten in de volgende informatie over universes of bestaande Web Intelligence-documenten:

- Meetwaarden in universes waarin zich woorden bevinden die overeenkomen met woorden in de zoekreeks. Als een meetwaarde overeenkomt met een van de zoektermen, wordt deze meetwaarde in het resulterende Web intelligence-document gebruikt.
- Dimensienamen in universes die overeenkomen met woorden in de zoekreeks.
  Als een dimensienaam overeenkomt met een van de zoektermen, wordt de informatie over deze dimensie door het resulterende Web Intelligence-document geanalyseerd.
- Met behulp van queryfilters kunt u de gegevens in het document uitlichten. Deze queryfilters worden gegenereerd doordat de zoekreeks wordt geanalyseerd.
  - Als de naam van een universevoorwaarde overeenkomt met een van de zoektermen, wordt de voorwaarde als filter gebruikt.
  - Als er veldwaarden in bestaande Web Intelligence-documenten voorkomen waarvan de namen overeenkomen met zoektermen, wordt er vanuit de dimensie van het historische rapport met de overeenkomende waarde een filter gemaakt, met 'gelijk aan' als de voorwaardelijke operator.

Als Platform zoeken zoveel overeenkomsten heeft gevonden dat het resulterende document twee resultaatvelden en een filter bevat, is de query gereed om te worden uitgevoerd. In dat geval kan de gebruiker klikken om het volledige rapport weer te geven.

Als er niet voldoende overeenkomsten tussen universes en het document zijn gevonden, kunt u de query bewerken alvorens deze uit te voeren.

Als de zoekreeks in meerdere universes wordt gevonden of als hetzelfde woord twee verschillende overeenkomsten geeft, zoals in de naam van een dimensie en als filterwaarde, stelt Platform zoeken meerdere query's voor.

26.3.3.1.2 Doorzoekbare inhoudstypen

De inhoud die naar BI-platform wordt gepubliceerd, kan worden doorzocht met Platform zoeken. Hierna volgt een overzicht van de objecttypen met hun bijbehorende geïndexeerde inhoud:

Objecttype	Geïndexeerde inhoud
Crystal Reports 2020	Titel, beschrijving, selectieformule, opgeslagen gegevens, tekstvelden in secties, parameterwaarden en subrapporten.
Web Intelligence-documenten	Titel, beschrijving, naam van de universe-filters die in het rapport worden gebruikt, opgeslagen gegevens, constanten in de filtervoorwaarde die lokaal zijn gedefinieerd in het rapport, naam van de universe-meetwaarden die in het rapport worden gebruikt, naam van de universe-objecten die in het rapport worden gebruikt, gegevens in de recordset en statische tekst in cellen.
Microsoft Excel-documenten (2003 en 2007)	Gegevens in alle niet-lege cellen, velden op de overzichtspagina van de documenteigenschappen (titel, onderwerp, auteur, bedrijf, categorie, trefwoorden en opmerkingen) en tekst in kop- en voettekst van het document. Voor cellen waarin berekeningen of formules worden gebruikt, kan worden gezocht naar de waarde na de evaluatie. Voor getal- of datum/tijd-waarden kan worden gezocht in de onbewerkte gegevens.
Microsoft Word-documenten (2003 en 2007)	Tekst in alle alinea's en tabellen, velden op de overzichtspagina van de documenteigenschappen (titel, onderwerp, auteur, bedrijf, categorie, trefwoorden en opmerkingen), tekst in documentkop- en voetteksten en numerieke tekst.
RTF-, PDF-, PPT- en TXT-bestanden	Alle tekst in deze bestanden kan worden doorzocht.
LCMJob, ObjectPackage, webservicequery (QaaWS), profiel, discussies, InformationDesigner, widgets voor SAP BusinessObjects BI-platform, MDAnalysis, publicaties, analyse en hyperlink	Inhoud van metagegevens kan worden doorzocht.
Gebeurtenissen	Alle gebeurtenissen zoals aangepaste gebeurtenissen, systeemgebeurtenissen, Crystal Reports-gebeurtenissen en Toezichtgebeurtenissen zijn doorzoekbaar. Als een gebeurtenis verbonden wordt met een bron, maakt Platform zoeken de bron zichtbaar samen met de gebeurtenis. **Opmerking** Platform zoeken ondersteunt gebeurtenissen voor Crystal Reports voor Enterprise.

Objecttype	Geïndexeerde inhoud

BI-werkruimte	• De titel, beschrijving en inhoud van de volgende BIW-modules worden geïndexeerd:
	  • Tekstmodule
	  • Webpaginamodule
	  • Navigatielijstmodule
	  • Viewermodule
	• De titel en beschrijving van een samengestelde module wordt geïndexeerd.
	• Alleen de titel van een werkruimtesjabloonmodule wordt geïndexeerd.
	• In het geval van een groepsmodule worden de titel en metagegevens van de modules erin geïndexeerd.
	• De titel, beschrijving en CUID van InfoObject-modules in BIW worden geïndexeerd.
	  Opmerking
	  Aangezien alleen de titel en beschrijving van een ingesloten InfoObject-module worden geïndexeerd, worden geen referenties naar de ingesloten module geretourneerd wanneer naar de InfoObject-inhoud wordt gezocht. Als bijvoorbeeld een CR in BIW wordt ingevoegd, worden de titel en beschrijving geïndexeerd. Bij het zoeken naar de inhoud van de CR worden geen referenties naar de ingesloten module geretourneerd.
	• Als een BIW meerdere tabbladen en subtabbladen bevat, worden de titel en inhoud van elk (sub)tabblad geïndexeerd.

CR Next Gen	Titel, beschrijving, selectieformule, opgeslagen gegevens, tekstvelden in secties, parameterwaarden en subrapporten. De volgende objecten in een CR Next Gen-rapport worden niet ondersteund: • Kruistabelrapport • Extractie van diagramgegevens • Extractie van afbeeldingen en bijbehorende metagegevens • Ingesloten OLE (bijvoorbeeld een Word-document ingesloten in CR) Bovendien is het niet mogelijk om gegevens per pagina uit een CR Next Gen-rapport te lezen.

Objecttype	Geïndexeerde inhoud
Universe	Inhoud van gegevens kan worden doorzocht. **Opmerking** De optie voor universe-indexering is standaard ingeschakeld. Als u merkt dat het veel tijd kost om query's uit te voeren die door Platform zoeken worden gebruikt om universe-inhoud te indexeren, waardoor de prestaties van de databaseserver verslechteren, is het raadzaam de optie voor universe-indexering uit te schakelen in de CMC (Central Management Console). Een voorbeeld van een query die Platform zoeken gebruikt terwijl universe-inhoud wordt geïndexeerd, is `Select distinct SampleColumnName from SampleTableName LIMIT 1000`. Volg deze stappen om universe-indexering uit te schakelen: 1. Meld u aan bij de CMC (Central Management Console). 2. Kies *Toepassingen*. 3. Navigeer naar Toepassing voor Platform zoeken en kies *Eigenschappen*. 4. Navigeer naar inhoudstypen en hef selectie van *Universe* op. 5. Kies *Opslaan en sluiten*.
Lumira-document	Alleen de inhoud van metagegevens kan worden doorzocht.
Analysis voor Office-document	Alleen de inhoud van metagegevens kan worden doorzocht.

Opmerking

De maximumgrootte die wordt ondersteund voor niet-specifieke documenten (MS Office 2003- en 2007- en PDF-documenten) is 15 MB.

26.3.3.2 Zoeken

Wanneer een gebruiker naar een trefwoord zoekt in BI-startpunt of een andere toepassing die gebruikmaakt van de SDK van Platform zoeken, wordt de hoofdindex doorzocht op de zoektermen. Op basis van de weergaverechten van de gebruiker geeft de zoekmachine alleen documenten weer waarvoor de gebruiker toegangsrechten heeft.

Opmerking

Wanneer een zoekopdracht wordt uitgevoerd in de CMC in een omgeving met een grote CMS-database, kan de zoekopdracht mislukken. Lees voor meer informatie SAP Note 2156647 Zoeken in de CMC gaat traag of levert geen resultaten op.

26.3.3.3 Na het zoeken

26.3.3.3.1 Facetten

Met Platform zoeken worden de zoekresultaten verfijnd doordat deze worden ingedeeld in categorieën of facetten van gelijksoortige objecttypen en worden geclassificeerd op basis van het aantal keer dat de categorie voorkomt in de resultaten voor de zoekterm. Met facetten kunt u eenvoudig naar het juiste resultaat navigeren.

Platform zoeken genereert facetten uit de InfoObject-metagegevens, en de metagegevens en inhoud van het document. Alleen de facetten waarvan meer dan twee documenten overeenkomen met een opgegeven query, worden weergegeven. Facetten worden dynamisch opgehaald op basis van de documenten die overeenkomen met de zoekquery en worden gesorteerd op het aantal documenten.

Documenten worden gegroepeerd in de volgende algemene facetten of categorieën:

- Persoonlijk of openbaar (zoals HR, Corporate en Finance): dit is gebaseerd op de categorieën van documenten voor BI-platform.
- Documenttype: dit is gebaseerd op het documenttype zoals Web Intelligence, Crystal Reports, Microsoft Word (2003 en 2007) en Microsoft Excel (2003 en 2007).
- Universe en Verbindingen: dit is gebaseerd op de inhoudsbron.
- Datum: dit betreft de datum van de laatste vernieuwing: (jaar, kwartaal en maand).
- Tijd: dit betreft de tijd van de laatste vernieuwing, bijvoorbeeld 24 uur of vorige week.
- Auteur: dit is de naam van de gebruiker die het document heeft gemaakt.

> ⓘ Opmerking
>
> Wanneer u met de landinstelling Hebreeuws of Arabisch werkt, worden in het zoekresultaat geen facetten weergegeven als u inhoudsobjecten zoekt in het BI-startpunt.

26.3.3.3.2 De classificatie van zoekresultaten normaliseren

Bij de classificatie van een document houdt Platform zoeken rekening met de plaats waar de betreffende term voorkomt. De inhoud wordt in de volgende categorieën gegroepeerd op basis va hoe de inhoud voorkomt in het document:

1. Metagegevens van platform
2. Metagegevens van document
3. Metagegevens van inhoud
4. Inhoud

U kunt het gewicht voor deze categorieën aanpassen in de CMC.

26.3.3.3.2.1 Gewicht aanpassen voor de classificatie van zoekresultaten

Met Platform zoeken kunt u gewicht geven aan de inhoud die gegroepeerd wordt in categorieën op basis van hoe de inhoud voorkomt in het document: door een hogere waarde voor de gewenste categorie in te stellen kunt u hiervoor sneller zoekresultaten ophalen.

Ga als volgt te werk om het gewicht in te stellen:

1. Klik in het gebied *Beheren* van de CMC op *Toepassingen*.
2. Open de *toepassing Platform zoeken*.
3. Kies *Classificatie*.

   De gewichten van verschillende inhoudscategorieën zoals Metagegevens van platform, Metagegevens van document, Metagegevens van inhoud en Inhoud worden weergegeven. De *Landinstelling van gebruiker* is de landinstelling die in de voorkeuren van BI-startpunt is ingesteld.
4. Stel de gewichten in volgens uw vereisten.
5. Kies *Opslaan*.

Als u in een upgradescenario classificatie wilt toepassen op documenten die al zijn geïndexeerd, moet u de index opnieuw maken. Raadpleeg de informatie over het opnieuw maken van de index in de sectie Toepassingseigenschappen configureren in de CMC [pagina 940] voor meer details.

26.3.3.3.3 Ondersteuning voor meerdere talen

Platform zoeken biedt ondersteuning voor meerdere talen om inhoud te indexeren, zoekresultaten op te halen en suggesties in uw gewenste taal weer te geven. Voor indexering van alle niet-gelokaliseerde BI-platformdocumenten wordt de landinstelling gebruikt die in de *Standaardindex van de landinstelling* in de CMC is ingesteld.

Zodra het InfoObject is gelokaliseerd, gebruikt Platform zoeken de taalanalysefunctie om het document te indexeren.

De zoekfunctie is gebaseerd op de landinstelling die is ingesteld in de productlandinstellingen van de client. Platform zoeken geeft meer gewicht aan de productlandinstellingen van de client bij het ophalen van zoekresultaten. U kunt de gewichten configureren in de CMC.

26.3.3.3.4 Suggesties

Platform zoeken geeft suggesties voor onjuist gespelde zoekquery's. Als de oorspronkelijke query geen resultaten oplevert, stelt Platform zoeken de meest waarschijnlijke termen voor op basis van de geïndexeerde inhoud.

Suggesties worden weergegeven als trefwoorden met hyperlink. Klik op een hyperlink om een lijst weer te geven van documenten die het trefwoord bevatten en die kunnen overeenkomen met de oorspronkelijke query. Deze suggesties worden bepaald volgens algoritmen op basis van verschillende objectieve factoren.

Als er meerdere termen zijn die met de oorspronkelijke opdracht overeen kunnen komen, biedt Platform zoeken een top drie met suggesties in de taal die is ingesteld als *Standaardindex van de landinstelling* in de CMC.

> **Opmerking**
>
> Platform zoeken genereert in de volgende gevalleen geen suggesties:
>
> - als de zoekquery's minder dan drie letters bevatten
> - voor een toegewezen zoekopdracht, zoals Type: Crystal Reports-rapport
> - voor universe-metagegevens en -inhoud
> - Voor multibyte-talen, zoals Chinees, Japans en Koreaans

26.4 Platform zoeken integreren met SAP NetWeaver Enterprise Search

SAP NetWeaver Enterprise Search 7.20 en hoger kan de zoekservice gebruiken op basis van OpenSearch (RSS en ATOM). Hiermee kunnen zoekaanvragen gedelegeerd worden naar externe serviceprovidersystemen voor zoekopdrachten. In dit geval is OpenSearch de serviceprovider, SAP NetWeaver Enterprise Search is de gebruiker van de zoekresultaten en SAP BusinessObjects Platform Search is de serviceprovider voor zoekopdrachten.

Als een gebruiker een zoekaanvraag indient, stuurt SAP NetWeaver Search deze aanvragen direct door naar de OpenSearch-provider. De provider beantwoordt de zoekaanvraag en stuurt het antwoord terug naar SAP NetWeaver Enterprise Search. Het antwoord wordt vervolgens samengevoegd met de resultaten die worden ontvangen van de andere zoekobjectconnectors, tot een zoekresultaat dat in de gebruikersinterface wordt weergegeven.

Als u SAP NetWeaver Enterprise Search en Platform zoeken wilt integreren, moet u de volgende stappen uitvoeren:

1. Maak een connector in SAP NetWeaver Enterprise Search.
2. Importeer de rol van een gebruiker in het BI-platform.

26.4.1 Een connector maken in SAP NetWeaver Enterprise Search

U kunt een zoekobjectconnector van het type OpenSearch gebruiken voor de integratie van externe zoekproviders die een zoekfunctie bieden welke beschikbaar is via OpenSearch.

Voor het maken van een connector in SAP NetWeaver Enterprise Search gelden de volgende vereisten:

1. De URL van de OpenSearch-beschrijvingsservice.
2. De OpenSearch-beschrijvingsservice mag alleen beschikbaar zijn in de RSS- of ATOM-indeling.

Voer de volgende stappen uit om een connector in SAP NetWeaver Enterprise Search te maken:

1. Start de Beheercockpit en kies Maken.
2. Selecteer OpenSearch als het type zoekobjectconnector.
3. Kies *Volgende*.
4. Voer de URL van de OpenSearch-provider in voor de OpenSearch-beschrijvingsservice.
5. Selecteer een van de volgende verificatie-instellingen om de URL van de beschrijvingsservice te starten:
   - Geen verificatie: er vindt geen verificatie plaats.
   - SAP-verificatieticket: deze gebruiker wordt gebruikt voor verificatie via eenmalige aanmelding.
   - Gebruiker/wachtwoord: er wordt een vooraf gedefinieerd wachtwoord gebruikt voor verificatie.
6. Selecteer Zoek-URL starten in de OpenSearch URL-instellingen.
   De OpenSearch-beschrijvingsservice wordt vervolgens gevalideerd voor een geschikte zoekservice. Het systeem voert automatisch een waarde in voor het sjabloon voor URL zoeken, en de bijbehorende beschrijving.
7. Selecteer een van de volgende verificatie-instellingen om de connector in te stellen:
   - Geen verificatie: er vindt geen verificatie plaats.
   - SAP-verificatieticket: deze gebruiker wordt gebruikt voor verificatie via eenmalige aanmelding.
   - Gebruiker/wachtwoord: er wordt een vooraf gedefinieerd wachtwoord gebruikt voor verificatie.
8. Kies *Volgende*.
   Er wordt een samenvattend dialoogvenster weergegeven met de waarden die zijn ingevoerd voor deze zoekobjectconnector.
9. Kies *Vorige* om de instellingen aan te passen of *Annuleren* om alle ingevoerde gegevens te negeren.
10. Kies *Voltooien* om de instellingen op te slaan.

26.4.2 De rol van een gebruiker in het BI-platform importeren

Voer de volgende stappen ut om de rol van een gebruiker in het BI-platform te importeren:

> **Opmerking**
>
> De beheerder moet gebruikersdetails, systeeminformatie, informatie over de toepassingshost en gebruikersreferenties hebben.

1. Ga naar het gedeelte *Verificatie* van de CMC.
2. Kies *SAP*.
3. Voer het volgende in op het tabblad *Machtigingssystemen*:
   - Systeem
   - Client
   - Toepassingsserver
   - Systeemnummer
   - Gebruikersnaam
   - Wachtwoord
   - Taal

4. Kies *Bijwerken*.
5. Kies het tabblad *Rol importeren* en importeer gebruikersrollen.
6. Kies *Bijwerken*.
7. Kies *Beheren* > *Gebruikersbeveiliging* in de CMC om de juiste gebruikersrechten toe te wijzen.

26.5 Zoeken in resultaten uit SAP NetWeaver Enterprise Search

Voer de volgende stappen uit om de zoekresultaten van SAP NetWeaver Enterprise Search te doorzoeken:

1. Meld u aan bij de toepassing SAP NetWeaver Enterprise Search.
2. Kies *Geavanceerd zoeken*.
3. Selecteer de connector die gemaakt is voor Platform Zoeken.
4. Zoek op een trefwoord.

   Geconsolideerde resultaten voor het trefwoord bevatten het resultaat van Platform zoeken als er een treffer is voor het trefwoord.

26.6 Controle

Alle gebeurtenissen van de zoekaanvragen die zijn verzonden door een clienttoepassing die de service Platform zoeken gebruikt, alsook het zoekantwoord, worden gecontroleerd. Voor Platform zoeken wordt de controle geïmplementeerd op het serviceniveau.

De service Platform zoeken moet worden uitgevoerd met een Proxyservice voor clientcontrole op dezelfde server om controlegebeurtenissen te kunnen versturen.

Er is één gebeurtenistype-id 1009 voor Platform zoeken en vier d-types van gebeurtenisdetail specifiek voor Platform zoeken:

- Keyword search (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

Naast bovengenoemde gebeurtenisdetails zijn er een aantal standaardgebeurtenisdetails, zoals sessionCuid en userCuid, die ondersteund worden voor elke controle in elke BI-platformmodule.

De werking van controle in Platform zoeken wordt hieronder uitgelegd aan de hand van een voorbeeld.

Als u naar een trefwoord zoals Verkoop zoekt, kan het totaalaantal zoekresultaten 5 zijn. In dit geval worden de volgende gebeurtenissen gecontroleerd:

- Gebeurtenistype-id 1009
- Gebeurtenisdetailtype-id 19 met waarde 'sales'

- Gebeurtenisdetailtype-id 63 met waarde 5
- Sessie-cuid
- Gebruikers-cuid
- Status met waarde 0 (successtatus)
- Starttijd
- Duur
- Object-id met waarde 0 aangezien dit controle op de servicezijde is

Wanneer facetten gegenereerd worden en u een of meer facetten selecteert, worden de volgende gebeurtenissen gecontroleerd:

- Gebeurtenistype-id 1009
- Gebeurtenisdetailtype-id 19 met waarde 'sales'
- Gebeurtenisdetailtype-id 63 met waarde 5
- Gebeurtenisdetailtype-id 20 met een door komma's gescheiden facetreeks
- Sessie-cuid
- Gebruikers-cuid
- Status met waarde 0 (successtatus)
- Starttijd
- Duur
- Object-id met waarde 0 aangezien dit controle op de servicezijde is

Als er een uitzondering bij het zoeken optreedt vanwege een ongeldige invoer zoals *"a", worden de volgende gebeurtenisdetails gecontroleerd:

- Gebeurtenistype-id 1009
- Gebeurtenisdetailtype-id 19 met waarde 'sales'
- Gebeurtenisdetailtype-id 63 met waarde 0
- Gebeurtenisdetailtype-id 1 met uitzonderingsbericht
- Sessie-cuid
- Gebruikers-cuid
- Status met waarde 1 (mislukkingsstatus)
- Starttijd
- Duur
- Object-id met waarde 0 aangezien dit controle op de servicezijde is

26.7 Problemen oplossen

26.7.1 Zelfherstel

Platform zoeken heeft nu een eigen mechanimse voor zelfherstel. Het geheugengebruik van de zoekservice wordt constant in de gaten gehouden en indexering wordt automatisch gestopt wanneer het geheugengebruik de drempelwaarde overschrijdt. De service wordt automatisch hervat wanneer het geheugengebruik weer tot een aanvaardbaar niveau is gezakt. Gebruikers kunnen tijdens dit proces blijven zoeken, maar gedurende een

bepaalde tijd niet indexeren. Platform zoeken configureert standaard het aantal documenten dat geïndexeerd kan worden bij elk exemplaar gebaseerd op het documenttype. Het indexeren wordt gestart gebaseerd op de systeembronnen zoals CPU en geheugen.

26.7.2 Scenario's van problemen

Deze sectie voorziet in stapsgewijze oplossingen voor een breed scala aan problemen die kunnen optreden bij het ophalen van zoekresultaten met Platform zoeken.

Kan zoekresultaten niet ophalen uit het onlangs toegevoegde document dat het trefwoord bevat

- Controleer of Platform zoeken het documenttype van het ingediende document ondersteunt. Als het documenttype niet ondersteund wordt, wordt het document niet geïndexeerd.
  Raadpleeg het onderwerp *Doorzoekbare inhoudstypen* in de hieronder vermelde verwante onderwerpen voor meer informatie over ondersteunde documenttypen.
- Controleer de optie die geselecteerd is voor *Frequentie zoeken*. Als de *Frequentie voor verkennen* is ingesteld op *Continu verkennen*, worden documenten direct geselecteerd voor indexering. Als de *Frequentie voor verkennen* is ingesteld op *Gepland verkennen*, wordt indexering alleen uitgevoerd tijdens de geplande periode.
  Voor meer informatie over de *Frequentie voor verkennen* raadpleegt u het onderwerp *Toepassingseigenschappen configureren* in de hieronder vermelde verwante onderwerpen.
- Controleer de lijst met fouten bij indexering om te verifiëren of het document succesvol geïndexeerd is. Als het document in deze lijst wordt weergegeven, moet u het wijzigen en opnieuw indienen zodat Platform zoeken het document gebruikt voor indexering.

  > **Opmerking**
  >
  > U kunt het document wijzigen door een veld toe te voegen of te verwijderen en het dan opnieuw op te slaan. Hiermee wordt de tijdstempel van het document bijgewerkt in de gegevensopslagruimte van het BI-platform en wordt het opnieuw indexeren van het document gestart.

  Zie het onderwerp *Lijst met fouten bij indexering* in de hieronder vermelde verwante onderwerpen voor meer informatie over documenten die niet geïndexeerd kunnen worden.
- Controleer Adaptive Processing Server-traceringslogboeken voor meer informatie over de indexeringsfout.
  1. Ga naar de map `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\logging\`, die het APS-traceringslogboek met een GLF-extensie bevat.
  2. Open het traceringslogbestand en zoek naar het document SI_ID dat geïndexeerd moet worden.

     > **Opmerking**
     >
     > U kunt het document SI_ID vinden in de documenteigenschappen.

Kan Crystal Reports-documenten niet ophalen

Met Platform zoeken wordt alleen Crystal Reports-inhoud voor Crystal Reports 2020 2020 geïndexeerd. Er wordt geen inhoud voor Crystal Reports voor Enterprise geïndexeerd.

Voor Crystal Reports voor Enterprise kunt u echter zoeken naar de metagegevens van een document zoals titel, beschrijving en trefwoord, die documenteigenschappen zijn.

Als het document indexeerbare inhoud bevat, moet u dezelfde procedure volgen als in de bovengenoemde sectie *Kan zoekresultaten niet ophalen uit het onlangs toegevoegde document dat het trefwoord bevat*.

De toepassing SAP NetWeaver Enterprise Search kan geen resultaten ophalen uit de gegevensopslagruimte van het BI-platform

- Controleer of Platform zoeken de zoekresultaten ophaalt met het BI-startpunt om te achterhalen of het probleem veroorzaakt wordt door de integratie van Platform zoeken en SAP NetWeaver Enterprise Search.
- Controleer of OpenSearch correct geïmplementeerd is op de webtoepassingsserver. De specifieke stappen voor het valideren van de OpenSearch-implementatie zijn afhankelijk van het type webtoepassingsserver dat wordt gebruikt.
- Controleer of de connector juist gemaakt of geconfigureerd is in de SAP NetWeaver Enterprise Search-configuratie. U moet de juiste connector voor SAP NetWeaver Enterprise Search gebruiken om de resultaten van Platform zoeken te federeren.
- Controleer of de communicatie tussen de computers met respectievelijk SAP NetWeaver Enterprise Search en BI-platform correct verloopt. In geval van netwerkproblemen in een gedistribueerde omgeving kan SAP NetWeaver Enterprise Search de resultaten mogelijk niet federeren.
- Controleer of SAP NetWeaver Enterprise Search-gebruikers aan het BI-platform worden toegevoegd met de juiste rechten. Ga naar het gebied *Verificatie* van de CMC en selecteer *SAP* om de gebruikersrechten te valideren.

Verwante informatie

Lijst met fouten bij indexering [pagina 949]
Toepassingseigenschappen configureren in de CMC [pagina 940]
Doorzoekbare inhoudstypen [pagina 951]

27 Federatie

27.1 Federatie

Federatie is een niet-sitegebonden herhalingsfunctie voor gebruik van meerdere BI-platformimplementaties in een internationale omgeving.

Van inhoud die in de ene BI-platformimplementatie wordt gemaakt en beheerd, kan op gezette tijden een kopie worden gemaakt naar andere BI-platformimplementaties op verschillende geografische locaties. U kunt herhalingstaken in één richting en in twee richtingen uitvoeren.

Federatie biedt de volgende voordelen:

- Het netwerkverkeer beperken
- Inhoud op één locatie maken en beheren
- Prestaties verhogen voor eindgebruikers

Wanneer u inhoud herhaalt met Federatie, kunt u het volgende doen:

- Het beheer van meerdere implementaties vereenvoudigen
- Een consistent rechtenbeleid instellen voor bedrijven met meerdere vestigingen
- Sneller informatie verkrijgen en rapporten verwerken op externe locaties waar de gegevens zijn opgeslagen
- Tijd besparen doordat lokale en verspreide gegevens sneller worden opgehaald
- Inhoud uit meerdere implementaties synchroniseren zonder aangepaste code te schrijven

Federatie is een functie die gebruikers in staat stelt te werken met afzonderlijke beveiligingsmodellen, levenscycli, test- en implementatietijden, en verschillende bedrijfseigenaars en beheerders. U kunt bijvoorbeeld beheerdersfuncties delegeren waardoor de beheerder van een verkooptoepassing geen wijzigingen kan aanbrengen in een toepassing voor personeelszaken.

Zoals in de tabel hieronder wordt beschreven, kunt u verschillende objecten herhalen met Federatie.

Categorie	Objecttypen die kunnen worden herhaald	Opmerkingen
Business Views-weergaven	Business View-beheer, DataConnection, Zoeklijsten, Gegevensbasis enzovoort	Alle objecten worden ondersteund, maar niet allemaal op individueel niveau.
Rapporten	Crystal Reports, Web Intelligence en Dashboard Design	Full Client-invoegtoepassing en sjablonen worden ondersteund.
Externe objecten	Excel-, PDF-, PowerPoint-, Word-, TXT-, RTF- en Shockwave-bestanden	
Gebruikers	Gebruikers, groepen, Postvakken IN, Favorieten en persoonlijke categorie	
Business Intelligence-platform	Mappen, gebeurtenissen, categorieën, agenda's, toegangsniveaus, hyperlinks, snelkoppelingen, programma's,	

Categorie	Objecttypen die kunnen worden herhaald	Opmerkingen
	profielen, objectpakketten, niet-specifieke objecten	
Universe	Universe, verbindingen en universe-overbelasting	

In de volgende scenario's vindt u twee voorbeelden waarin wordt gedemonstreerd hoe uw organisatie kan profiteren van federatie.

Scenario 1: winkel (gecentraliseerd ontwerp)

De winkelketen ACME wil elke maand een verkooprapport naar alle vestigingen verzenden via herhaling in één richting. De beheerder op de oorspronkelijke locatie maakt een rapport dat de beheerders op elke doellocaties herhalen en opnieuw uitvoeren tegen de desbetreffende opslagdatabase.

> → Tip
>
> Gelokaliseerde exemplaren kunnen worden teruggestuurd naar de oorspronkelijke locatie, waar de herhaalde informatie van elk object wordt beheerd. Hier worden onder andere het juiste logo en de databaseverbindingsgegevens toegepast.

Scenario 2: planning op afstand (gedistribueerde toegang)

De gegevens bevinden zich op de oorspronkelijke locatie. Uitstaande herhalingstaken worden verzonden naar de oorspronkelijke locatie waar ze worden uitgevoerd. Voltooide herhalingstaken worden teruggestuurd naar de doellocaties waar ze worden weergegeven. De gegevens van een rapport zijn bijvoorbeeld niet beschikbaar op de doellocatie, maar de gebruiker kan de rapporten configureren voor uitvoering op de oorspronkelijke locatie voordat het voltooide rapport wordt teruggestuurd naar de doellocatie.

27.2 Federatieterminologie

De volgende woordenlijst bevat nieuwe terminologie die in samenhang met Federatie wordt gebruikt en handig kan zijn bij het werken met Federatie.

BI-toepassing	De logische groepering van verwante BI-inhoud (Business Intelligence) met een specifiek doel en een specifieke doelgroep. Een BI-toepassing is geen object. In een implementatie van BI-platform kunnen meerdere BI-toepassingen worden beheerd. Elke BI-toepassing kan een eigen beveiligingsmodel, levenscyclus, tijdlijn voor tests en implementatie, en eigen eigenaars en beheerders hebben.
Doellocatie	Een BI-platformsysteem waarmee herhaalde inhoud van BI-platform van een oorspronkelijke site wordt opgehaald.
Lokaal	Het lokale systeem waarmee een gebruiker of beheerder verbinding heeft. De beheerder van een doellocatie bijvoorbeeld, is “lokaal” op de doellocatie.
Lokaal uitgevoerde, voltooide exemplaren	Exemplaren die op de doellocatie worden verwerkt en vervolgens worden teruggestuurd naar de oorspronkelijke locatie.

Meerdere oorspronkelijke locaties	Meerdere locaties kunnen dienst doen als oorspronkelijke locatie. Veel ontwikkelcentra bijvoorbeeld, beschikken over meerdere oorspronkelijke locaties. Per herhaling kan echter slechts één oorspronkelijke locatie worden opgegeven.
Herhaling in één richting	Objecten worden uitsluitend in één richting herhaald: van de oorspronkelijke locatie naar de doellocatie. Wijzigingen die op de doellocatie worden aangebracht, blijven uitsluitend op de doellocatie.
Oorspronkelijke locatie	BI-platformsysteem waarvan de inhoud afkomstig is.
Extern	Een systeem dat voor een gebruiker niet lokaal is. Zo is de oorspronkelijke locatie een "externe" locatie voor gebruikers en beheerders op de doellocatie.
Externe verbinding	Een object dat gegevens bevat die worden gebruikt voor het tot stand brengen van verbinding met een implementatie van BI-platform, zoals gebruikersnaam en wachtwoord, CMS-naam, URI van de webservice en opschoningsopties.
Externe planning	Planningsaanvragen die van de doellocatie naar de oorspronkelijke locatie worden gestuurd. Rapporten op de doellocatie kunnen extern worden gepland, waarbij het rapportexemplaar voor verwerking wordt teruggestuurd naar de oorspronkelijke locatie. Het verwerkte exemplaar wordt vervolgens naar de doellocatie geretourneerd.
Herhaling	Het proces waarbij inhoud van het ene BI-platformsysteem naar het andere wordt gekopieerd.
Herhalingstaak	Een object dat gegevens bevat over herhalingsplanning, welke inhoud moet worden herhaald en eventueel speciale voorwaarden die tijdens de herhaling moeten worden uitgevoerd.
Herhalingslijst	Een lijst van de objecten die moeten worden herhaald. Een herhalingslijst verwijst naar andere inhoud, zoals gebruikers, groepen, rapporten, enzovoort in de implementatie van BI-platform die samen moet worden herhaald.
Herhalingsobject	Een object dat van een oorspronkelijke locatie naar een doellocatie wordt herhaald. Alle herhaalde objecten op een doellocatie worden gemarkeerd met het herhalingspictogram. Als er een conflict is, worden objecten gemarkeerd met het conflictpictogram.
Herhalingspakket	Het herhalingspakket wordt tijdens de overdracht gemaakt en bevat de objecten van een herhalingstaak. Het kan alle objecten bevatten die in de herhalingslijst zijn gedefinieerd, zoals het geval is in een snel wijzigende omgeving of bij de eerste herhaling. Het kan ook een deelverzameling van de herhalingslijst bevatten als de objecten minder vaak worden gewijzigd dan in de planning van de herhalingstaak. Het herhalingspakket wordt geïmplementeerd als BIAR-bestand (BI Application Resource).
Herhaling vernieuwen	Alle objecten in een herhalingslijst worden vernieuwd, ongeacht de laatst gewijzigde versie.
Herhaling in twee richtingen	Identiek aan herhaling in één richting, met het verschil dat wijzigingen in dit geval in beide richtingen worden verzonden. Wijzigingen in de oorspronkelijke locatie worden herhaald naar elke doellocatie. Wijzigingen en nieuwe objecten in een doellocatie worden verzonden naar de oorspronkelijke locatie.

27.3 Beveiligingsrechten beheren

Federatie herhaalt inhoud van de ene implementatie naar de andere. Hiervoor is samenwerking met andere beheerders nodig, dus moet u weten hoe de beveiliging werkt voordat u Federatie gebruikt.

Beheerders van de afzonderlijke implementaties moeten onderling overleggen voordat de functie Federatie wordt ingeschakeld. Nadat de inhoud is herhaald, kunnen beheerders inhoud wijzigen.

Voor het uitvoeren van bepaalde taken zijn specifieke rechten voor de oorspronkelijke implementatie en de doelimplementatie vereist:

- Vereiste rechten op de oorspronkelijke locatie
- Vereiste rechten op de doellocatie
- Vereiste rechten voor objecten specifiek voor Federatie
- Scenario's in federatie

> → Tip
>
> Lees dit hoofdstuk aandachtig door voordat u Federatie inschakelt.

27.3.1 Vereiste rechten op de oorspronkelijke locatie

In dit gedeelte wordt beschreven welke acties op de oorspronkelijke locatie kunnen worden uitgevoerd en welke rechten de gebruikersaccount die verbinding maakt met de oorspronkelijke locatie daarvoor nodig heeft. Dit is de account die u hebt opgegeven in het externe verbindingsobject op de doellocatie.

Actie	Beschrijving	Vereiste rechten
Herhaling in één richting	Hiermee worden gegevens uitsluitend herhaald van de oorspronkelijke locatie naar de doellocatie. ⓘ Opmerking De rechten “Weergeven” en “Herhalen” zijn vereist voor alle objecten die worden herhaald, inclusief objecten die automatisch worden herhaald op basis van afhankelijkheidsberekeningen.	• De rechten “Weergeven” en “Herhalen” voor alle objecten die u wilt herhalen • Het recht “Weergeven” voor de herhalingslijst
Herhaling in beide richtingen	Hiermee wordt van de oorspronkelijke locatie naar de doellocatie herhaald en van de doellocatie naar de oorspronkelijke locatie.	• De rechten “Weergeven” en “Herhalen” voor alle objecten die u wilt herhalen • Het recht “Weergeven” voor de herhalingslijst • Het recht “Rechten wijzigen” voor gebruikersobjecten,

Actie	Beschrijving	Vereiste rechten
		voor herhaling van wachtwoordwijzigingen
Planning	Hiermee wordt externe planning toegestaan op de oorspronkelijke locatie vanaf de doellocatie.	• Het recht “Planning” voor alle objecten die u extern wilt plannen

Verwante informatie

Vereiste rechten op de doellocatie [pagina 966]

27.3.2 Vereiste rechten op de doellocatie

In dit gedeelte wordt beschreven welke acties op de doellocatie kunnen worden uitgevoerd en welke rechten de gebruikersaccount die de herhalingstaak uitvoert daarvoor nodig heeft. Dit is de account van de gebruiker die de herhalingstaak maakt.

> ⓘ Opmerking
>
> Net als andere objecten die kunnen worden gepland, kunt u ook herhalingstaken namens iemand anders plannen.

Actie	Beschrijving	Vereiste rechten
Alle objecten	Objecten herhalen ongeacht herhaling in één of twee richtingen.	• De rechten “Weergeven”, “Toevoegen”, “Bewerken” en “Rechten wijzigen” voor alle objecten. • Het recht “Gebruikerswachtwoord aanpassen” voor alle gebruikersobjecten
Eerste herhaling	De eerste keer dat de herhalingstaak wordt uitgevoerd, bestaat er nog geen object op de doellocatie. De gebruikersaccount die de herhalingstaak uitvoert, moet daarom rechten voor alle mappen op het hoogste niveau hebben en voor de objecten waaraan inhoud wordt toegevoegd.	• De rechten “Weergeven”, “Toevoegen”, “Bewerken” en “Rechten wijzigen” voor alle mappen op het hoogste niveau en standaardobjecten.

Verwante informatie

Vereiste rechten op de oorspronkelijke locatie [pagina 965]

27.3.3 Rechten specifiek voor Federatie

Deze sectie biedt informatie over scenario's die specifiek zijn voor Federatie.

Actie	Beschrijving	Vereiste rechten
Objecten opschonen	Met het opschonen van objecten worden objecten uit de doellocatie verwijderd.	• De account waaronder de herhalingstaak wordt uitgevoerd, vereist het recht "Verwijderen" voor alle objecten die mogelijk worden verwijderd.
Opschoning voor bepaalde objecten uitschakelen	Objecten die vanaf de oorspronkelijke locatie worden herhaald en op de oorspronkelijke locatie worden verwijderd, wilt u mogelijk niet verwijderen op de doellocatie. U kunt dit bewerkstelligen met behulp van rechten. Kies deze optie bijvoorbeeld wanneer gebruikers op de doellocatie een object gaan gebruiken, onafhankelijk van de gebruikers op de oorspronkelijke locatie. Stel dat u een herhaalde universe hebt op basis waarvan gebruikers op de doellocatie hun eigen lokale rapporten maken. Als deze universe op de oorspronkelijke locatie wordt verwijderd, wilt u de universe mogelijk niet verwijderen op de doellocatie.	• Weiger het recht "Verwijderen" van de gebruikersaccount waaronder de herhalingstaak wordt uitgevoerd voor de objecten die u wilt behouden.
Herhaling in beide richtingen zonder wijzigingen op de oorspronkelijke locatie	In sommige gevallen zult u de optie 'Herhaling in beide richtingen' hebben ingeschakeld, maar wilt u bepaalde objecten op de oorspronkelijke locatie niet wijzigen, zelfs niet als deze wel worden gewijzigd op de doellocatie. Een reden hiervoor kan zijn dat het een speciaal object betreft dat alleen mag worden gewijzigd door gebruikers op de oorspronkelijke locatie. Of u wilt de optie voor externe planning inschakelen, maar wilt de	• Weiger het recht "Bewerken" van de gebruikersaccount voor het verbinden in het externe verbindingsobject.

Actie	Beschrijving	Vereiste rechten
	wijzigingen niet overdragen naar de oorspronkelijke locatie. **Opmerking** Voor Externe planning kunt u een taak maken die alleen objecten voor externe planning verwerkt. In dit geval worden hogerliggende objecten toch herhaald, inclusief het rapport, de map met het rapport en de map boven die map. Alle wijzigingen op de doellocatie worden herhaald naar de oorspronkelijke locatie en alle wijzigingen op de oorspronkelijke locatie worden herhaald naar de doellocatie.	

27.3.4 Beveiliging voor een object herhalen

Als u de beveiligingsrechten voor een object wilt behouden, moet u gelijktijdig zowel het object als de bijbehorende gebruiker of groep repliceren. Als u dit niet doet, moeten de gebruiker of groep al zijn gedefinieerd op de locatie waarnaar u repliceert en moeten zij unieke CUID's op elke locatie hebben.

Als een object zonder bijbehorende gebruiker of groep wordt gerepliceerd, of als de gebruiker of groep niet reeds bestaan op de locatie waarnaar u repliceert, verliezen zij hun rechten.

Voorbeeld

Groep A en groep B beschikken over rechten voor object A. Groep A heeft het recht “Weergeven” en groep B heeft “Weergave weigeren”. Als met de herhalingstaak alleen groep A en object A worden herhaald, heeft object A op de doellocatie alleen het recht “Weergeven” voor de bijbehorende groep A.

Wanneer u een object herhaalt, bestaat er een beveiligingsrisico als u niet alle groepen herhaalt die expliciete rechten voor dat object hebben. Het voorbeeld hierboven geeft een mogelijk beveiligingsrisico weer. Als gebruiker A lid is van zowel groep A als groep B, heeft deze gebruiker niet het recht om object A weer te geven op de oorspronkelijke locatie. Gebruiker A wordt echter wel naar de doellocatie herhaald, omdat hij/zij lid is van beide groepen. Nadat gebruiker A naar de doellocatie is herhaald, heeft hij/zij wel het recht object A weer te geven op de doellocatie, maar niet het recht om object A weer te geven op de oorspronkelijke locatie, omdat groep B niet is herhaald.

Objecten waarin wordt verwezen naar andere objecten die zich niet in een herhalingstaak bevinden of die nog zich nog niet op de doellocatie bevinden, worden in een logbestand weergegeven. Het logbestand geeft aan dat het object verwees naar een object dat niet is herhaald en deze verwijzing heeft gewist.

De beveiliging van een object voor een bepaalde gebruiker of groep wordt alleen herhaald van de oorspronkelijke locatie naar de doellocatie. U kunt beveiliging instellen voor herhaalde objecten op de doellocatie, maar deze instellingen worden niet herhaald naar de oorspronkelijke locatie.

27.3.5 Beveiliging herhalen met toegangsniveaus

Voor behoud moeten rechten gedefinieerd worden op toegangsniveaus. Het object, de gebruiker of de groep moet gelijktijdig met het toegangsniveau worden herhaald of al voorkomen op de locatie waarnaar u herhaalt.

Objecten waarmee expliciete rechten worden toegekend aan een gebruiker of groep die geen deel uitmaakt van de herhalingstaak of zich nog niet op de doellocatie bevindt, worden in het logboekbestand vermeld. Hierin ziet u dat het object rechten heeft toegekend die niet zijn herhaald en dat de rechten zijn opgeheven.

Desgewenst kunt u automatische herhaling definiëren voor "toegangsniveaus" die zijn ingesteld voor een geïmporteerd object. Deze optie is alleen beschikbaar in de herhalingslijst.

> ⓘ Opmerking
>
> Standaardtoegangsniveaus worden niet herhaald, maar verwijzingen blijven behouden.

27.4 Opties voor herhalingstype en herhalingsmodus

Afhankelijk van het herhalingstype en de herhalingsmodus die u hebt geselecteerd, kunt u een van de vier verschillende opties voor herhalingstaken maken:

- Herhaling in één richting,
- Herhaling in beide richtingen,
- Vernieuwen vanaf oorsprong
- of Vernieuwen vanaf doel.

27.4.1 Herhaling in één richting

Met deze optie kunt u de inhoud in slechts één richting herhalen: van de oorspronkelijke locatie naar de doellocatie. Wijzigingen die u aanbrengt in objecten die zich op de oorspronkelijke locatie en in de herhalinglijst bevinden, worden naar de doellocatie verzonden. De wijzigingen die in objecten op de doellocatie zijn aangebracht, worden echter niet terug naar de oorspronkelijke locatie verzonden.

Herhaling in één richting is ideaal voor implementaties met één centrale implementatie van BI-platform waar objecten worden gemaakt, gewijzigd en beheerd. Voor andere implementaties wordt de inhoud van de centrale implementatie gebruikt.

Als u herhaling in één richting wilt, selecteert u de volgende opties:

- Herhalingstype = Herhaling in één richting

- Herhalingsmodus = Normale herhaling

27.4.2 Herhaling in beide richtingen

Met deze optie kunt u de inhoud in beide richtingen herhalen: van de oorspronkelijke locatie naar de doellocatie en omgekeerd. Alle wijzigingen in objecten op de oorspronkelijke locatie worden herhaald naar de doellocaties en alle wijzigingen in objecten op de doellocatie worden herhaald naar de oorspronkelijke locatie.

> ⓘ Opmerking
>
> Schakel de optie Herhaling in beide richtingen in voor externe planning en als u lokaal uitgevoerde exemplaren weer wilt herhalen naar de oorspronkelijke locatie.

Als u meerdere implementaties van BI-platform hebt waar inhoud op beide locaties wordt gemaakt, gewijzigd en beheerd, is de optie Herhaling in beide richtingen het meest efficiënt. Met deze optie kunt u de verschillende implementaties ook synchroon houden.

Als u herhaling in beide richtingen wilt, selecteert u de volgende opties:

- Herhalingstype = Herhaling in beide richtingen
- Herhalingsmodus = Normale herhaling

Verwante informatie

Externe planning en lokaal uitgevoerde exemplaren [pagina 995]

27.4.3 Vernieuwen vanaf oorsprong of Vernieuwen vanaf doel

Wanneer u inhoud herhaalt met de optie Herhaling in één richting of de optie Herhaling in beide richtingen, worden de objecten op de herhalingslijst naar een doellocatie herhaald. Mogelijk worden echter niet alle objecten herhaald elke keer dat de herhalingstaak wordt uitgevoerd.

Federatie beschikt over een optimaliseringssysteem waarmee herhalingstaken sneller kunnen worden uitgevoerd. Dit systeem bepaalt aan de hand van de versie en het tijdstempel van een object of het na de laatste herhaling is gewijzigd. Deze controle wordt uitgevoerd op objecten die zijn geselecteerd in de herhalingslijst en op objecten die tijdens de afhankelijkheidscontrole zijn herhaald.

In bepaalde gevallen kan het echter voorkomen dat objecten worden genegeerd door het optimaliseringssysteem, waardoor ze niet worden herhaald. In deze gevallen kunt u de opties “Vernieuwen vanaf oorsprong” en “Vernieuwen vanaf doel” gebruiken om de herhalingstaak te dwingen inhoud, en de bijbehorende afhankelijkheden, te herhalen, ongeacht hun tijdstempel.

Met de optie Vernieuwen vanaf oorsprong wordt alleen inhoud verzonden vanaf de oorspronkelijke locatie naar de doellocatie. Met de optie Vernieuwen vanaf doel wordt alleen inhoud verzonden vanaf de doellocaties naar de oorspronkelijke locatie.

Voorbeeld

De volgende drie voorbeelden bevatten scenario's met de opties “Vernieuwen vanaf oorsprong” en “Vernieuwen vanaf doel”, waarbij bepaalde objecten worden overgeslagen vanwege de optimalisering.

Scenario 1: objecten waarin zich andere objecten bevinden, worden toegevoegd aan een gebied dat wordt herhaald.

Map A wordt herhaald van de oorspronkelijke locatie naar de doellocatie. De map bevindt zich nu op beide locaties. Een gebruiker verplaatst of kopieert map B met daarin rapport B naar map A op de oorspronkelijke locatie. Bij de eerstvolgende herhaling wordt door Federatie gedetecteerd dat het tijdstempel van map B is gewijzigd en wordt deze map naar de doellocatie herhaald. Het tijdstempel van rapport B is echter niet gewijzigd. Bij een normale herhaling in één richting of in beide richtingen wordt het rapport daarom overgeslagen.

U kunt ervoor zorgen dat de inhoud van map B correct wordt herhaald door één herhalingstaak met de optie “Vernieuwen vanaf oorsprong” uit te voeren. Hierna wordt de herhaling van deze map correct uitgevoerd bij normale herhaling in één richting of in beide richtingen. Als dit voorbeeld wordt omgedraaid en de map naar de doellocatie wordt verplaatst of gekopieerd, gebruikt u “Vernieuwen vanaf doel”.

Scenario 2: nieuwe objecten worden toegevoegd met LifeCycle Manager of vanaf de BIAR-opdrachtregel.

Objecten die u toevoegt aan een gebied dat met LifeCycle Manager of vanaf de BIAR-opdrachtregel wordt herhaald, worden bij normale herhaling in één richting of in beide richtingen mogelijk genegeerd. De oorzaak hiervan is dat de interne klok van het bronsysteem en het doelsysteem mogelijk niet synchroon lopen bij het gebruik van LifeCycle Manager of de BIAR-opdrachtregel.

> ⓘ Opmerking
>
> Na het importeren van nieuwe objecten in een gebied dat op de oorspronkelijke locatie wordt herhaald, is het daarom raadzaam om een herhalingstaak uit te voeren met de optie “Vernieuwen vanaf oorsprong”. Na het importeren van nieuwe objecten in een gebied dat op de doellocatie wordt herhaald, is het daarom raadzaam om een herhalingstaak uit te voeren met de optie “Vernieuwen vanaf doel”.

Scenario 3: tussen geplande herhalingsopdrachten in.

Als u objecten toevoegt aan een gebied dat wordt herhaald en niet kunt wachten tot de volgende herhaling, kunt u gebruikmaken van de opties “Vernieuwen vanaf oorsprong” en “Vernieuwen vanaf doel”. Door het gebied waaraan objecten zijn toegevoegd te selecteren, kunt u inhoud snel herhalen.

> ⓘ Opmerking
>
> Dit scenario kan bij lange herhalingslijsten tijdrovend zijn en frequent gebruik van deze optie wordt dan ook niet aangeraden. Het is bijvoorbeeld niet nodig om elk uur een herhalingstaak met de optie Vernieuwen vanaf oorsprong of Vernieuwen vanaf doel uit te voeren. Gebruik deze opties uitsluitend voor herhalingstaken die u “meteen” uitvoert en bij planning met grote intervallen.

> ⓘ Opmerking
>
> In bepaalde gevallen kunt u geen gebruikmaken van conflictoplossing, zoals bij “Vernieuwen vanaf oorsprong”: de optie Doellocatie wint is geblokkeerd of “Vernieuwen vanaf doel”: de optie Oorspronkelijke locatie wint is geblokkeerd.

27.5 Externe gebruikers en groepen herhalen

In Federatie kunt u gebruikers en groepen van andere platforms herhalen, met name van Active Directory en LDAP.

> → Tip
>
> Neem deze sectie door als u deze typen gebruikers en groepen of hun persoonlijke inhoud wilt plannen, zoals favoriete mappen of Postvakken IN.

Gebruikers en groepen toewijzen

1. Wijs de gebruikers en groepen op de oorspronkelijke locatie toe, zodat deze in Federatie juist worden herhaald.
2. Herhaal de toegewezen gebruikers en groepen naar de doellocatie.

> ⓘ Opmerking
>
> Wijs gebruikers en groepen niet afzonderlijk toe op de doellocatie. Als u dit doet, zullen hun CUID's op de doellocatie en de oorspronkelijke locatie van elkaar verschillen en kan Federatie de gebruikers of groepen niet met elkaar in overeenstemming brengen.

Voorbeeld

De beheerder wijst groep A toe aan gebruiker A op de oorspronkelijke locatie en de doellocaties. Groep A en gebruiker A krijgen verschillende CUID's op de oorspronkelijke locatie en de doellocaties. Tijdens de herhaling kan Federatie ze niet met elkaar in verband brengen, waardoor groep A of gebruiker A vanwege een aliasconflict niet wordt herhaald.

> ⓘ Opmerking
>
> Voordat u gebruikers en groepen van derden herhaalt, moet de doellocatie zijn ingesteld voor gebruik van Active Directory- of LDAP-verificatie. U moet de doellocatie ook instellen voor gebruik van Active Directory of LDAP, zodat deze locatie kan communiceren met de directoryserver of domeincontroller.

> ⓘ Opmerking
>
> Wanneer u een AD- of LDAP-groep de eerste keer hebt herhaald, kunnen gebruikers in deze groep zich pas aanmelden als het AD-/LDAP-groepsdiagram is vernieuwd. Dit gebeurt automatisch, ongeveer om de 15 minuten. Als u het AD-/LDAP-groepsdiagram handmatig wilt vernieuwen, gaat u naar de pagina *Verificatie* van de CMC, dubbelklikt u op *Windows AD* of *LDAP* en klikt u vervolgens op *Bijwerken*.

> **Opmerking**
>
> wees voorzichtig met replicatie van groepen van andere platforms. Wanneer u nieuwe gebruikers toevoegt aan de groep op de directoryserver, kunnen zij zich op beide locaties aanmelden. Dit beveiligingsprobleem van de Active Directory- en LDAP-verificatie is onafhankelijk van Federatie.
>
> Als u zich afzonderlijk aanmeldt op de oorspronkelijke locatie en de doellocatie of als het groeplidmaatschap op beide locaties wordt bijgewerkt met de knop Bijwerken op de verificatiepagina van de CMC, wordt op beide locaties een gebruikersaccount gemaakt. De accounts zullen dan verschillende CUID's hebben, waardoor de herhaling niet correct kan worden uitgevoerd door Federatie.
>
> Het is belangrijk dat u de account op één locatie maakt en vervolgens herhaalt naar de andere locatie.

27.6 Universes en universeverbindingen herhalen

Wanneer u Federatie gebruikt om universes te herhalen tussen implementaties van BI-platform is het belangrijk dat u dit van tevoren te plannen. Een universe-object kan niet werken zonder een onderliggende universe-verbinding.

Universeverbindingsobjecten bevatten informatie die nodig is voor het maken van verbinding met een rapportdatabase. Universe-verbindingsobjecten moeten geldige informatie bevatten en het tot stand brengen van een databaseverbinding toestaan om correct te kunnen werken.

> **Opmerking**
>
> Als u herhaling in beide richtingen gebruikt en een universe van de oorspronkelijke locatie herhaalt zonder de bijbehorende universe-verbinding naar de doellocatie, wordt bij daaropvolgende herhalingen de koppeling tussen de bron van de universe en de universe-verbinding op de bron mogelijk overschreven of verwijderd. Als u dit wilt voorkomen, moet u de universeverbindingen altijd herhalen met de universes.

Selecteer altijd de volgende opties wanneer u de herhalingslijst met de universes maakt of wijzigt om ervoor te zorgen dat afhankelijke universe-verbindingen worden herhaald met de universes:

- *Verbindingen voor geselecteerde universes opnemen*
- *Vereiste universes voor geselecteerde universes opnemen*

> **Opmerking**
>
> Als de koppeling van een universe met de universeverbinding is overschreven of verwijderd, opent u de universe in Universe Designer en wijzigt u de verbindingsgegevens onder *Bestand* > *Parameters*.

In de volgende twee voorbeelden wordt aangegeven hoe universes en de gerelateerde universeverbindingen worden herhaald.

Voorbeeld

Wanneer u universes en universe-verbindingen herhaalt, moet u contoleren of de verbindingsomgeving op de oorspronkelijke locatie overeenkomt met de verbindingsomgeving op de doellocatie.

Als voor de universe-verbinding bijvoorbeeld de ODBC-verbinding “TestODBC” wordt gebruikt, moet er een correct geconfigureerde ODBC-verbinding met de naam “TestODBC” beschikbaar zijn in de doelomgeving. The ODBC-verbinding kan worden omgezet in dezelfde of een andere database. De schema's van de databases moeten gelijk zijn om ervoor te zorgen dat er geen verbindingsproblemen optreden in universes waarvoor deze verbinding wordt gebruikt.

Voorbeeld

Als voor de herhaalde universe op de doellocatie een andere database moet worden gebruikt dan voor de universe op de oorspronkelijke locatie, herhaalt u de universe-verbinding, maar moeten de verbindingsgegevens op de doellocatie naar de gewenste database wijzen.

Als voor de universe-verbinding op de oorspronkelijke locatie bijvoorbeeld de ODBC-verbinding “Test” wordt gebruikt die verwijst naar “DatabaseA”, moet de ODBC-verbinding op de doellocatie ook de naam “Test” hebben, maar moet deze verwijzen naar “DatabaseB”.

27.7 Herhalingslijsten beheren

Herhalingslijsten bevatten inhoud, zoals gebruikers, groepen en rapporten in de BI-platformimplementatie, die samen kunnen worden herhaald. Vanuit de CMC kunt u herhalingslijsten openen.

Van typen inhoud die kunnen worden herhaald, vindt u een uitleg in de onderstaande tabel.

Categorie	Ondersteunde objecten
Gegevensopslagobjecten	Objecten als Business Views-weergaven, gegevensverbindingen, zoeklijsten, gegevensverzamelingen, enzovoort. **Opmerking** Alle objecten worden ondersteund, maar niet allemaal op individueel niveau.
Rapporten	Crystal Reports-rapporten, Web Intelligence-documenten en Dashboard-objecten. **Opmerking** Full Client-invoegtoepassing en sjablonen worden ondersteund.

Categorie	Ondersteunde objecten
Externe objecten	Excel-, PDF-, PowerPoint-, Word-, TXT-, RTF- en Shockwave-bestanden.
Gebruikers	Gebruikers, groepen, Postvakken IN, Favorieten en persoonlijke categorie.
Business Intelligence-platform	Mappen, gebeurtenissen, categorieën, agenda's, aangepaste rollen, hyperlinks, snelkoppelingen, programma's, profielen, objectpakketten, niet-specifieke objecten.
Universes	Universes, verbindingen, universe-overload.

ⓘ Opmerking

De volgende objecten moeten worden gemaakt op de oorspronkelijke locatie en vervolgens worden herhaald naar de doellocatie. Als u deze objecten echter op de doellocatie maakt en ze vervolgens naar de oorspronkelijke locatie herhaalt, functioneren ze op de oorspronkelijke locatie niet naar behoren.

- Business Views-weergaven
- Business Element-items
- Gegevensverzamelingen
- Gegevensverbindingen
- Zoeklijst
- Universe-overloads

27.7.1 Herhalingslijsten maken

De herhalingslijsten bevinden zich in het gebied Herhalingslijsten van de CMC. U kunt herhalingslijsten ordenen in de mappen en submappen die u maakt.

27.7.1.1 Een map voor een herhalingslijst maken

1. Ga naar het gebied *Herhalingslijsten* in de CMC.
2. Klik op *Herhalingslijsten*.
3. Klik op *Beheren* > *Nieuw* > *Map*.
   Het dialoogvenster *Map maken* verschijnt.
4. Typ een mapnaam en klik op *OK*.
   U kunt nu herhalingslijsten maken in deze map.

27.7.1.2 Een herhalingslijst maken

1. Ga naar het gebied *Herhalingslijsten* in de CMC.
2. Selecteer de map waarin u uw nieuwe herhalingslijst wilt opslaan.
3. Klik op *Beheren* > *Nieuw* > *Nieuwe herhalingslijst*.
   Het dialoogvenster *Nieuwe herhalingslijst* wordt weergegeven.
4. Typ een naam en een beschrijving voor de herhalingslijst.
5. Klik op de koppeling *Eigenschappen van herhalingslijst* voor geavanceerde opties.

   Hiermee kunt u aangeven welke afhankelijkheden automatisch worden herhaald van de oorspronkelijke locatie naar de doellocatie.
6. Selecteer de vereiste opties volgens de beschrijving in de tabel.

Afhankelijkheidsopties voor objecten	Definitie
Persoonlijke mappen voor geselecteerde gebruikers opnemen	De persoonlijke mappen van de geselecteerde gebruiker en de inhoud van de mappen worden herhaald.
Persoonlijke categorieën voor geselecteerde gebruikers opnemen	De persoonlijke categorieën van de geselecteerde gebruiker herhalen.
Universes voor geselecteerde rapporten opnemen	Universes waarvan geselecteerde rapportobjecten afhankelijk zijn, worden herhaald.
Leden van geselecteerde gebruikersgroepen opnemen	Gebruikers die zich in een geselecteerde groep bevinden, worden herhaald.
Universes opnemen die vereist zijn door geselecteerde universes	Hiermee worden universes die afhankelijk zijn van andere universes herhaald.
Postvakken IN voor geselecteerde gebruikers opnemen	Het Postvak IN van de geselecteerde gebruiker en de inhoud van het postvak worden herhaald.
Gebruikersgroepen voor geselecteerde universes opnemen	De gebruikersgroepen die aan een universe-overload zijn gekoppeld, worden herhaald.
Toegangsniveaus opnemen die voor geselecteerde objecten zijn ingesteld	Toegangsniveaus die voor geselecteerde objecten zijn gedefinieerd, worden herhaald.
Documenten voor geselecteerde categorieën opnemen	Hiermee worden documenten, zoals Word, Excel en PDF, die deel uitmaken van geselecteerde categorieën, herhaald.
Profielen voor geselecteerde gebruikers en gebruikersgroepen opnemen	Profielen die zijn gekoppeld aan geselecteerde gebruikers of groepen, worden herhaald.
Verbindingen opnemen die door geselecteerde universes worden gebruikt	Universeverbindingsobjecten die door geselecteerde objecten worden gebruikt, worden herhaald.

> **Opmerking**
>
> Bepaalde objecten in BI-platform zijn afhankelijk van andere objecten. Een Web Intelligence-document is voor structuur en inhoud bijvoorbeeld afhankelijk van de onderliggende universe. Als u een Web Intelligence-document herhaalt maar de bijbehorende universe niet selecteert, wordt herhaling niet uitgevoerd op de doellocatie, tenzij de universe daar al was herhaald. Als u echter *Universes voor geselecteerde rapporten opnemen* inschakelt, herhaalt Federatie automatisch de universes waarvan het rapport afhankelijk is.

7. Klik op *Volgende*.
8. Selecteer een of meer objecten om aan uw herhalingslijst toe te voegen.
   - Gebruik de pijlknoppen om objecten toe te voegen aan of te verwijderen uit de map *Beschikbare objecten*.
   - Of klik op *Gegevensopslagobjecten* onder *Alle herhalen* om alle Business View-objecten, Business Elements-items, Data Foundation-objecten, Data Connection-objecten, zoeklijstobjecten en gegevensopslagobjecten te herhalen, inclusief rapportafbeeldingen en functies.

   > **Opmerking**
   >
   > Het is niet mogelijk om mappen op het hoogste niveau in de map *Beschikbare objecten* te herhalen.

9. Klik op *Opslaan en sluiten*.

27.7.2 Herhalingslijsten wijzigen

Nadat u een herhalingslijst hebt gemaakt, kunt u de bijbehorende eigenschappen of objecten wijzigen.

27.7.2.1 Eigenschappen in een herhalingslijst wijzigen

1. Ga naar het gebied *Herhalingslijsten* in de CMC.
2. Selecteer de *herhalingslijst* die u wilt wijzigen.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Algemene eigenschappen* wordt weergegeven.
4. Wijzig de titel en de beschrijving. In het geopende dialoogvenster *Algemene eigenschappen* kunt u ook andere elementen van de geselecteerde herhalingslijst aanpassen.
5. Als u de afhankelijkheidsopties wilt wijzigen, klikt u op *Eigenschappen van herhalingslijst* in de navigatielijst.
6. Klik op *Opslaan en sluiten*.

Verwante informatie

Herhalingslijsten maken [pagina 975]

27.7.2.2 Objecten in een herhalingslijst wijzigen

1. Ga naar het gebied *Herhalingslijsten* in de CMC.
2. Selecteer een *herhalingslijst*.
3. Klik op *Acties* > *Herhalingslijst beheren*.

Het dialoogvenster *Herhalingslijst beheren* verschijnt en bevat een lijst met objecten die in de herhalingslijst zijn opgenomen.

4. Voeg objecten toe of verwijder objecten naar wens.
5. Klik op *Opslaan en sluiten*.

Verwante informatie

Herhalingslijsten maken [pagina 975]

27.8 Externe verbindingen beheren

Externe verbindingsobjecten bevatten de vereiste gegevens voor het maken van een verbinding met een externe BI-platformimplementatie.

> **Opmerking**
>
> Het externe verbindingsobject wordt gemaakt in een BI-platformimplementatie op een doelsite. De externe verbinding is de oorspronkelijke locatie.

U kunt externe verbindingen weergeven in het gebied *Federatie* van de CMC.

27.8.1 Externe verbindingen maken

In Federatie wordt een externe verbinding met een externe BI-platformimplementatie verbonden. Als u een verbinding tot stand wilt brengen met de oorspronkelijke locatie waarop de inhoud zich bevindt die u wilt herhalen, moet u eerst een externe verbinding op de doellocatie maken.

U kunt mappen en submappen maken om uw externe verbindingen te ordenen.

27.8.1.1 Een map maken voor externe verbinding

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op *Externe verbindingen*.
3. Klik op *Beheren* > *Nieuw* > *Map*.
   Het dialoogvenster *Map maken* verschijnt.
4. Typ een mapnaam en klik op *OK*.
   U kunt nu externe verbindingen maken in deze map.

27.8.1.2 Een externe verbinding maken

Als u verbinding wilt maken met een externe BI-platformimplementatie, moet u een externe verbinding maken in Federatie.

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op *Externe verbindingen*.
3. Klik op *Beheren* > *Nieuw* > *Nieuwe externe verbinding*.
   Het dialoogvenster *Nieuwe externe systeemverbinding* verschijnt.
4. Geef een naam, beschrijving en verwante velden op:

> **Opmerking**
>
> Alle velden zijn verplicht, met uitzondering van "Beschrijving" en "Beperk het aantal opschoningsobjecten tot".

Veld	Beschrijving
Titel	De naam van het externe verbindingsobject.
Beschrijving	Een beschrijving van het externe verbindingsobject. (Optioneel)
URI van webservice op extern systeem	URL naar Federatie-webservices, die automatisch wordt geïmplementeerd op de Java-toepassingsserver. U kunt alle Federatie-webservices in het BI-platform gebruiken, ongeacht of deze zich op de oorspronkelijke locatie, op de doellocatie of in een andere implementatie bevinden. Gebruik deze notatie: `http://<toepassing_uwserver_computernaam>:<poort>/dswsbobje`. Voorbeeld: `http://<mijncomputer.mijndomein.com>:<8080>/dswsbobje`
Externe systeem-CMS	De naam van de CMS waarmee u verbinding wilt maken en die toegankelijk is via Federatie-webservices. Deze wordt beschouwd als de CMS van de oorspronkelijke locatie. Dit is de indeling: `CMS_Naam:poort`. Voorbeeld: `<mymachine>:6400` **Opmerking** Als u de standaardpoort 6400 gebruikt, is het opgeven van de poort optioneel.

Veld	Beschrijving
Gebruikersnaam	De gebruikersnaam die wordt gebruikt om verbinding te maken met de oorspronkelijke locatie. **Opmerking** Zorg ervoor dat de gebruikersnaam die u gebruikt weergaverechten heeft voor de herhalingslijst op de oorspronkelijke locatie van de implementatie.
Wachtwoord	Het wachtwoord van de gebruikersaccount waarmee u verbinding maakt met de oorspronkelijke locatie.
Verificatie	Het type accountverificatie voor de verbinding met de oorspronkelijke locatie. Mogelijke opties zijn: Enterprise, AD of LDAP.
Opschoningsfrequentie (in uren)	De frequentie waarmee herhalingstaken voor deze externe verbinding objecten moeten opschonen. Geef uitsluitend positieve gehele getallen op. De eenheid is uren. De standaardwaarde is 24.
Beperk het aantal opschoningsobjecten tot	Het aantal objecten dat door een herhalingstaak wordt opgeschoond. (Optioneel)

5. Klik op *OK*.

27.8.2 Externe verbindingen wijzigen

Nadat u een externe verbinding hebt gemaakt, kunt u de eigenschappen en beveiligingsopties ervan wijzigen.

Een externe verbinding wijzigen:

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op *Externe verbindingen*.
3. Dubbelklik op de externe verbinding die u wilt wijzigen.
   Het dialoogvenster *Verbindingseigenschappen* verschijnt. U kunt de volgende eigenschappen wijzigen:
   - *Titel*
   - *Beschrijving*
   - *URI van webservice op extern systeem*
   - *Externe systeem-CMS*
   - *Gebruikersnaam*
   - *Wachtwoord*
   - *Verificatie*
   - *Opschoningsfrequentie (in uren)*
   - *Beperk het aantal opschoningsobjecten tot*
4. Geef uw wijzigingen op.
5. Klik op *Opslaan en sluiten*.

27.9 Herhalingstaken beheren

Een herhalingstaak is een type object dat wordt uitgevoerd volgens een planning en wordt gebruikt om inhoud te herhalen tussen twee BI-platformimplementaties in federatie.

> **Opmerking**
>
> Herhaalde objecten op een doellocatie worden gemarkeerd met het herhalingspictogram. Als er een conflict optreedt, wordt een object gemarkeerd met het conflictpictogram zoals weergegeven: .

U kunt een lijst met herhalingstaken weergeven in de map *Externe verbinding* in het gebied *Federatie* van de CMC.

27.9.1 Herhalingstaken maken

Een herhalingstaak is vereist om inhoud tussen twee BI-platformimplementaties in federatie te herhalen. Elke herhalingstaak moet slechts één externe verbinding en één herhalingslijst hebben.

27.9.1.1 Een herhalingstaak maken

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op *Externe verbindingen*.
3. Selecteer een *externe verbinding* voor de nieuwe herhalingstaak.

   > **Let op**
   >
   > De CMC moet verbinding kunnen maken met webservices in de URI van de externe verbinding, zodat de wizard kan worden voortgezet.

4. Klik op *Beheren* > *Nieuw* > *Nieuwe herhalingstaak*.
   Het dialoogvenster *Nieuwe herhalingstaak* wordt weergegeven.
5. Typ een naam en een beschrijving voor de herhalingstaak.
6. Klik op *Volgende*.
   Er wordt een lijst weergegeven met beschikbare herhalingslijsten op de oorspronkelijke locatie.
7. Selecteer de *herhalingslijst* die u wilt gebruiken voor uw herhalingstaak.
8. Klik op *Volgende*.
9. Selecteer configuratieopties zoals beschreven in de onderstaande tabel.

Optie	Beschrijving
Opschonen van objecten op doel inschakelen	Waar het oorspronkelijke object op de oorspronkelijke locatie is verwijderd, worden herhaalde objecten

Optie	Beschrijving
	op de doellocatie gedwongen verwijderd door de herhalingstaak. **Opmerking** Bij het opschonen worden er geen objecten verwijderd die zijn herhaald op basis van afhankelijkheden noch objecten die in de herhalingslijst zijn geselecteerd.
Herhaling in één richting	Objecten worden alleen van de oorspronkelijke locatie naar de doellocatie herhaald. Wijzigingen die na de herhaling worden aangebracht in het object op de oorspronkelijke locatie, worden herhaald naar de doelocatie. Wijzigingen op de doellocatie worden echter niet herhaald naar de oorspronkelijke locatie.
Herhaling in twee richtingen	Objecten worden herhaald in beide richtingen: van de oorspronkelijke locatie naar de doellocatie en van de doellocatie naar de oorspronkelijke locatie. Wijzigingen die na de herhaling worden aangebracht in deze objecten op een locatie, worden automatisch herhaald op de andere locatie.
Oorspronkelijke site heeft voorrang	Wanneer er een conflict tussen een object op de oorspronkelijke locatie en de herhaalde versie op de doellocatie wordt gedetecteerd, geniet de versie op de oorspronkelijke locatie de voorkeur.
Geen automatische conflictoplossing	Er wordt geen actie ondernomen om gedetecteerde conflicten op te lossen.
Doellocatie heeft voorrang (Alleen beschikbaar bij herhaling in twee richtingen)	Wanneer er een conflict tussen een object op de oorspronkelijke locatie en de herhaalde versie op de doellocatie wordt gedetecteerd, geniet de versie op de doellocatie de voorkeur.
Normale herhaling	De herhalingstaak wordt op de normale wijze uitgevoerd.
Vernieuwen vanaf oorsprong	Alle inhoud van de oorspronkelijke locatie wordt naar de doellocatie herhaald, ongeacht of de inhoud is gewijzigd. U kunt de gehele herhalingslijst herhalen of slechts een deel ervan.
Vernieuwen vanaf doel (Alleen beschikbaar bij herhaling in twee richtingen)	Alle inhoud van de doellocatie wordt naar de oorspronkelijke locatie herhaald, ongeacht of de inhoud is gewijzigd. U kunt de gehele herhalingslijst herhalen of slechts een deel ervan.
Alle objecten herhalen (Alleen beschikbaar bij herhaling in twee richtingen)	De gehele herhalingslijst wordt herhaald. **Opmerking** Hiermee wordt de meest volledige herhaling uitgevoerd; deze bewerking neemt echter de meeste tijd in beslag.

Optie	Beschrijving
Externe planningen herhalen (Alleen beschikbaar bij herhaling in twee richtingen)	Externe exemplaren in behandeling worden herhaald van de doellocatie naar de oorspronkelijke locatie en voltooide exemplaren van de oorspronkelijke locatie worden herhaald naar de doellocatie.
Documentsjablonen herhalen	Alle objecten die geen exemplaren zijn (lokaal uitgevoerd of rapporten die zijn geselecteerd voor externe planning), worden herhaald. Deze bestaat uit gebruikers, groepen, mappen, rapporten, enzovoort.
Lokaal uitgevoerde, voltooide exemplaren herhalen	Voltooide exemplaren worden alleen van de doellocatie naar de oorspronkelijke locatie herhaald.

10. Klik op *OK*.

27.9.2 Herhalingstaken plannen

Nadat u eenmaal een herhalingstaak hebt gedefinieerd, kunt u plannen dat deze eenmaal of regelmatig wordt uitgevoerd. U kunt ook meerdere herhalingstaken op één doellocatie vanaf één oorspronkelijke locatie plannen.

> **Opmerking**
>
> Als u meerdere herhalingstaken op één doellocatie plant, kan er door slechts één herhalingstaak tegelijk verbinding worden gemaakt met de oorspronkelijke locatie. Andere herhalingstaken die verbinding proberen te maken, krijgen de status In behandeling en behouden deze totdat automatische verbinding met de oorspronkelijke locatie mogelijk is.

27.9.2.1 Een herhalingstaak plannen

1. Ga naar het gebied *Federatie* in de CMC.
2. Selecteer de *herhalingstaak* die u wilt plannen.
3. Klik op *Acties* > *Planningen*.
4. Selecteer de gewenste planningsopties.

27.9.3 Herhalingstaken wijzigen

Nadat u een herhalingstaak hebt gemaakt in Federatie, kunt u de eigenschappen ervan wijzigen.

27.9.3.1 Een herhalingstaak wijzigen

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op de map *Externe verbindingen*.
3. Selecteer de *externe verbinding* waarin de gewenste *herhalingstaak* zich bevindt.
4. Selecteer de *herhalingstaak* die u wilt wijzigen.
5. Klik op *Beheren* > *Objecteigenschappen beheren*.
6. Bekijk en bewerk de *eigenschappen*, *planning*, *geschiedenis*, *herhalingslijst* en *gebruikersbeveiliging*, indien noodzakelijk.

Secties	Beschrijving
Eigenschappen	De naam, beschrijving en andere algemene eigenschappen en opties van de herhalingstaak wijzigen.
Planning	Een terugkerende planning instellen voor de herhalingstaak.
Geschiedenis	Alle exemplaren van de herhalingstaak weergeven en beheren.
Herhalingslijst	De geselecteerde herhalingslijst wijzigen.
Gebruikersbeveiliging	De rechten voor de herhalingstaak instellen.

27.9.4 Een logboek weergeven na uitvoering van een herhalingstaak

Elke keer als u een herhalingstaak uitvoert, wordt door de functie Federatie automatisch een logboekbestand gemaakt op de doellocatie. Voor de logboekbestanden worden XML 1.1-standaarden gebruikt en is een webbrowser vereist die XML 1.1 ondersteunt.

Een herhalingslogboekbestand weergeven:

1. Ga naar het gebied *Federatie* in de CMC.
2. Klik op *Alle herhalingstaken*.
3. Selecteer een *herhalingstaak* in de lijst.
4. Klik op *Eigenschappen*.
   De *eigenschappenpagina* van de herhalingstaak wordt weergegeven.
5. Klik op *Geschiedenis*.
6. Klik op de *Exemplaartijd* van het logboekbestand om voltooide herhalingstaken weer te geven of klik op de status *Mislukt* als u een logboekbestand met mislukte herhalingstaken wilt weergeven.
7. Selecteer het gewenste exemplaar om het logboekbestand weer te geven.
   Het logboekbestand wordt gegenereerd in de XML-indeling en met behulp van een XSL-formulier worden de gegevens geconverteerd naar een HTML-pagina.

   U kunt het XML-logboekbestand weergeven vanaf de computer met de SIA (Server Intelligence Agent) waarin de Adaptive Job Server zich bevindt. U vindt het logboekbestand op de volgende locatie:

- Onder Windows: `<Installatiemap>\SAP BusinessObjects XI 4.0\logging`.
- Onder Unix: `<Installatiemap>/sap_bobj/logging`

27.10 Opschoning van objecten beheren

In Federatie moet u gedurende het gehele herhalingsproces objecten opschonen om er zeker van te zijn dat alle objecten die u op de oorspronkelijke locatie verwijdert, ook op de doellocaties worden verwijderd.

Voor het opschonen van objecten zijn twee elementen nodig: een externe verbinding en een herhalingstaak. Een extern verbindingsobject definieert algemene opschoningsopties en de herhalingstaak voert de opschoning uit na het verstrijken van het interval.

27.10.1 Een object opschonen

Afzonderlijke herhalingstaken waarvoor dezelfde externe verbinding wordt gebruikt, werken samen tijdens het opschonen van objecten. Dit betekent dat uw herhalingstaak objecten in de eigen herhalingslijst opschoont, maar ook de objecten in andere herhalingslijsten die dezelfde externe verbinding gebruiken. Een externe verbinding wordt alleen als identiek beschouwd als het bovenliggende element van de herhalingstaak hetzelfde externe verbindingsobject is.

Voorbeeld

Met herhalingstaak A en B worden object A en B herhaald. Beide objecten worden vanuit dezelfde oorspronkelijke locatie herhaald en gebruiken dezelfde externe verbinding. Als object B op de oorspronkelijke locatie wordt verwijderd, detecteert herhalingstaak A dat object B is verwijderd. Hoewel het object wordt herhaald door herhalingstaak B, wordt object B ook verwijderd van de doellocatie. Wanneer herhalingstaak B wordt uitgevoerd, is het opschonen van objecten niet meer nodig.

> ⓘ Opmerking
>
> Alleen de objecten op de doellocatie worden bij het opschonen van objecten verwijderd. Wanneer u een object op de oorspronkelijke locatie verwijdert dat onderdeel is van een herhalingstaak, wordt het object ook op de doellocatie verwijderd. Als een object op de doellocatie wordt verwijderd, wordt dit object bij het opschonen van objecten niet verwijderd op de oorspronkelijke locatie, zelfs niet als een herhalingstaak in beide richtingen wordt uitgevoerd.
>
> Objecten die uit de herhalingslijst zijn verwijderd, worden niet verwijderd van de doellocatie. Voor het correct verwijderen van een object dat in een herhalingslijst vermeld wordt, moet u het zowel op de doellocatie als op de oorspronkelijke locatie verwijderen. Objecten die via afhankelijkheidsberekeningen zijn herhaald, worden niet verwijderd.

27.10.2 Limieten voor het opschonen van objecten

In het object Externe verbinding kunt u het aantal objecten definiëren dat in een herhalingstaak gelijktijdig moet worden opgeschoond. Federatie detecteert automatisch waar het opschonen eindigt. De volgende keer dat u een herhalingstaak uitvoert, wordt hierdoor de volgende opschoning gestart vanaf dit punt.

> → Tip
>
> Als u een herhalingstaak sneller wilt voltooien, kunt u het aantal objecten dat moet worden opgeschoond verkleinen.

Voorbeeld

Met herhalingstaak A en B worden object A en B herhaald. Beide objecten worden vanaf dezelfde oorspronkelijke locatie herhaald en gebruiken dezelfde externe verbinding.

Wanneer op de oorspronkelijke locatie object B wordt verwijderd en de limiet voor opschoningsobjecten is ingesteld op 1, wordt op het moment dat herhalingstaak A opnieuw wordt uitgevoerd, gecontroleerd of object A is verwijderd. Object B wordt niet gecontroleerd en ook niet verwijderd.

Vervolgens wordt herhalingstaak B uitgevoerd en wordt het opschonen van objecten gestart op het punt waar herhalingstaak A is geëindigd. Bij deze herhalingstaak wordt wel gecontroleerd of object B is verwijderd en wordt het object van de doellocatie verwijderd. U vindt deze optie op het tabblad Eigenschappen van het object Externe verbinding: “Beperk het aantal opschoningsobjecten tot:”.

> ⓘ Opmerking
>
> Als u deze optie niet selecteert, wordt er door alle herhalingstaken die deze externe verbinding gebruiken, gecontroleerd welke objecten moeten worden opgeschoond.

27.10.3 Frequentie voor het opschonen van objecten

In het veld “Opschoningsfrequentie” voor de externe verbinding kunt u instellen hoe vaak objecten bij een herhalingstaak moeten worden opgeschoond.

> ⓘ Opmerking
>
> Geef een positief geheel getal op; dit getal staat voor het aantal uren dat moet worden gewacht voordat de volgende opschoning wordt uitgevoerd.

Voorbeeld

Met herhalingstaak A en B worden object A en B herhaald. Beide objecten worden vanaf dezelfde oorspronkelijke locatie herhaald en gebruiken dezelfde externe verbinding.

Als object B van de oorspronkelijke locatie is verwijderd en alle volgende voorwaarden waar zijn, wordt door de herhalingstaak gecontroleerd of object A is verwijderd.

- De objectlimiet is 1
- De opschoningsfrequentie is 150 uur
- Herhalingstaak A wordt als volgende taak uitgevoerd

Omdat de objectlimiet 1 is, wordt object B niet gecontroleerd of verwijderd op de doellocatie.

De volgende opschoning vindt plaats 150 uur nadat de eerste controle door herhalingstaak A is uitgevoerd. Hoewel de herhalingstaken A en B vele malen binnen die 150 uur kunnen worden uitgevoerd, voert geen van beide een opschoning uit. Na de 150 uur voert de eerstvolgende herhalingstaak de opschoning uit. Dan wordt vastgesteld dat object B op de oorspronkelijke locatie is verwijderd en wordt dit object vervolgens ook op de doellocatie verwijderd.

Opties in- en uitschakelen

Bij elke herhalingstaak kan een opschoning worden uitgevoerd. Gebruik de optie "Opschonen van objecten op doel inschakelen" om aan te geven of bij een herhalingstaak objecten moeten worden opgeschoond. Wanneer u dringende herhalingstaken hebt, kunt u het opschonen van objecten ook overslaan zodat de taken zo snel mogelijk worden uitgevoerd. Schakel hiertoe Objecten opschonen uit.

Verwante informatie

Limieten voor het opschonen van objecten [pagina 986]

27.11 Conflictopsporing en -oplossing beheren

Bij Federatie kan een conflict ontstaan wanneer de eigenschappen van een object op zowel de oorspronkelijke locatie als de doellocatie worden gewijzigd. Eigenschappen op zowel het bovenste niveau als geneste eigenschappen van een object worden gecontroleerd op conflicten. Er kan bijvoorbeeld een conflict ontstaan als een rapport of de naam van een rapport op zowel de oorspronkelijke locatie als de doellocatie wordt gewijzigd.

In sommige gevallen ontstaat geen conflict. Bijvoorbeeld als de naam van een rapport wordt gewijzigd op de oorspronkelijke locatie en de beschrijving van de herhaalde versie wordt gewijzigd op de doellocatie, worden de wijzigingen samengevoegd en ontstaat er geen conflict.

27.11.1 Conflicten als gevolg van herhaling in één richting oplossen

Bij herhaling in één richting zijn er twee opties voor conflictoplossing.

Oorspronkelijke site heeft voorrang

Wanneer een conflict ontstaat bij herhaling in één richting, heeft het object van de oorspronkelijke locatie voorrang. Wijzigingen in objecten op doellocaties worden overschreven door de gegevens op de oorspronkelijke locatie. Als een rapport bijvoorbeeld zowel op de oorspronkelijke locatie als op de doellocatie wordt gewijzigd, wordt na de volgende herhalingstaak de wijziging op de doellocatie overschreven door de versie van de oorspronkelijke locatie.

> ⓘ Opmerking
>
> Aangezien het conflict automatisch is opgelost, wordt het niet in het logboekbestand geregistreerd en wordt het object niet vermeld in de lijst met conflicterende objecten.

Geen automatische conflictoplossing

Wanneer zich een conflict voordoet en u "Geen automatische conflictoplossing" hebt geselecteerd, wordt het conflict niet opgelost, wordt er geen logboekbestand gegenereerd en wordt het object niet vermeld in de lijst met conflicterende objecten.

Beheerders kunnen in het gebied Federatie van de CMC een lijst ophalen met alle herhaalde objecten waarin een conflict is ontstaan. Objecten waarin een conflict is ontstaan, worden gegroepeerd door de externe verbinding waarmee de verbinding met de oorspronkelijke locatie tot stand is gebracht. Als u deze lijsten wilt ophalen, gaat u naar de map Herhalingsfouten in het gebied Federatie van de CMC en selecteert u de gewenste externe verbinding. Alle herhaalde objecten op een doellocatie worden gemarkeerd met het herhalingspictogram. Als er een conflict is, worden objecten gemarkeerd met het conflictpictogram. Er wordt ook een waarschuwingsbericht op de *eigenschappenpagina* weergegeven.

> ⓘ Opmerking
>
> Wanneer een herhalingstaak die gebruikmaakt van een externe verbinding is voltooid, wordt de lijst bijgewerkt. Deze lijst bevat alle conflicterende objecten voor alle herhalingstaken die gebruikmaken van de desbetreffende externe verbinding.

> ⓘ Opmerking
>
> Gebruikers die toegang hebben tot de CMC en de herhalingstaken, kunnen het XML-logboek raadplegen; dit wordt in de map voor logboekbestanden opgeslagen. Met een objectpictogram van een doellocatie wordt een conflict aangeduid. Tijdens de verwerking wordt er een conflictlogboek gemaakt.

Ahmed wijzigt rapport A op de oorspronkelijke locatie. Marian wijzigt de herhaalde versie van het rapport op de doellocatie. De volgende keer dat de herhalingstaak wordt uitgevoerd, ontstaat er een conflict in het rapport omdat dit op beide locaties is gewijzigd en het conflict niet automatisch wordt opgelost.

Het rapport op de doellocatie blijft behouden en de wijzigingen in het rapport op de oorspronkelijke locatie worden niet herhaald. Alle volgende replicatietaken worden op dezelfde manier verwerkt, totdat dit conflict is opgelost. Wijzigingen in het rapport op de oorspronkelijke locatie worden niet herhaald, totdat het conflict handmatig is opgelost.

> **Opmerking**
>
> In dit geval wordt het object niet herhaald. Ook wijzigingen die geen conflict veroorzaken, worden niet herhaald.

Er zijn drie opties voor het handmatig oplossen van een conflict:

1. Maak een herhalingstaak waarmee alleen de conflicterende objecten worden herhaald. Deze taak moet gebruikmaken van dezelfde externe verbinding en herhalingslijst.
   Als u de wijzigingen op de oorspronkelijke locatie wilt behouden, maakt u een herhalingstaak. Stel de herhalingsmodus vervolgens in op "Vernieuwen vanaf oorsprong" en Automatische conflictoplossing op "Oorspronkelijke site heeft voorrang".
   Als u de wijzigingen op de doellocatie wilt behouden, maakt u een herhalingstaak met Herhalingstype = "Herhaling in beide richtingen", Herhalingsmodus = "Vernieuwen vanaf doel" en Automatische conflictoplossing = "Doelsite heeft voorrang".

   > **Opmerking**
   >
   > Stel in de herhalingsmodus "Vernieuwen vanaf oorsprong" of "Vernieuwen vanaf doel" in om alleen de conflicterende objecten in de herhalingslijst te selecteren. Op deze manier worden andere objecten niet herhaald. Plan vervolgens wanneer de herhalingstaak moet worden uitgevoerd; de geselecteerde objecten worden herhaald en het conflict wordt opgelost zoals aangegeven.

2. Maak een herhalingstaak waarmee alleen de conflicterende objecten worden herhaald. Deze taak moet gebruikmaken van dezelfde externe verbinding. In tegenstelling tot hetgeen het geval is bij optie 1, kunt u echter een nieuwe herhalingslijst maken op de oorspronkelijke locatie. Gebruik alleen de conflicterende objecten en maak een nieuwe herhalingstaak voor deze specifieke herhalingslijst.
   Als u de wijzigingen op de oorspronkelijke locatie wilt behouden, stelt u Automatische conflictoplossing in op "Oorspronkelijke site heeft voorrang".
   Als u de wijzigingen op de doellocatie wilt behouden, stelt u Automatische conflictoplossing in op "Doelsite heeft voorrang" en Herhalingstype op "Herhaling in beide richtingen".
3. Voor herhaling in één richting kunt u alleen het object op de doellocatie verwijderen. De volgende keer dat de herhalingstaak wordt uitgevoerd, wordt het object van de oorspronkelijke locatie herhaald naar de doellocatie.

   > **Opmerking**
   >
   > Wees voorzichtig bij het verwijderen van objecten, omdat andere objecten die hiervan afhankelijk zijn, hierdoor mogelijk worden verwijderd, uitgeschakeld of niet meer zijn beveiligd. Optie 1 en 2 worden aanbevolen.

27.11.2 Conflicten als gevolg van replicatie in twee richtingen oplossen

Bij herhaling in beide richtingen zijn er drie opties voor conflictoplossing:

- Oorspronkelijke site heeft voorrang
- Doelsite heeft voorrang
- Geen automatische conflictoplossing

Oorspronkelijke site heeft voorrang

Wanneer een conflict ontstaat, krijgt de oorspronkelijke locatie voorrang en worden de wijzigingen op de doellocatie overschreven.

Voorbeeld

Lidy wijzigt de naam van een rapport in Rapport A. Stefan wijzigt de naam van de herhaalde rapportversie op de doellocatie in Rapport B. Wanneer de volgende herhalingstaak wordt uitgevoerd, wordt de herhaalde versie op de doellocatie omgezet in Rapport A.

Er wordt geen conflict geregistreerd in het logboekbestand en het object wordt niet vermeld in de lijst met conflicterende objecten, omdat het conflict is opgelost conform de instellingen van de gebruiker op de oorspronkelijke locatie.

Doelsite heeft voorrang

Wanneer er een conflict ontstaat, blijven de wijzigingen op de doellocatie intact en worden alle wijzigingen herhaald naar de oorspronkelijke locatie.

Voorbeeld

Karel wijzigt de naam van een rapport in Rapport A. Peter wijzigt de naam van de herhaalde rapportversie op de doellocatie in Rapport B. Wanneer de herhalingstaak wordt uitgevoerd, wordt er een conflict gedetecteerd. De naam van het doelrapport blijft Rapport B.

Bij herhaling in beide richtingen worden de wijzigingen ook herhaald naar de oorspronkelijke locatie. In dit scenario wordt de oorspronkelijke locatie bijgewerkt en wordt de naam van het bijbehorende rapport gewijzigd in Rapport B. Er wordt geen conflict in het logboekbestand geregistreerd en het object wordt niet vermeld in de lijst met conflicterende objecten, omdat het conflict is opgelost conform de instellingen van de gebruiker.

Geen automatische conflictoplossing

Wanneer “Geen automatische conflictoplossing” is geselecteerd, worden conflicten niet opgelost. Het conflict wordt geregistreerd in een logboek en kan handmatig door de beheerder worden opgelost.

> ⓘ Opmerking
>
> Met een objectpictogram wordt aangegeven dat er een conflict is ontstaan.

> ⓘ Opmerking
>
> Hoewel bij herhaling in beide richtingen wijzigingen naar zowel de oorspronkelijke locatie als naar de doellocatie worden herhaald, worden alleen de versies op de doellocatie gemarkeerd met een conflictpictogram.

> ⓘ Opmerking
>
> Gebruikers die toegang hebben tot de CMC en de herhalingstaken, kunnen het XML-logboek raadplegen; dit wordt in de map voor logboekbestanden geplaatst. Met een objectpictogram van een doellocatie wordt een conflict aangeduid. Tijdens de verwerking wordt er een conflictlogboek gemaakt.

De beheerder kan in het gebied Federatie van de CMC een lijst ophalen met alle herhaalde objecten waarin een conflict is ontstaan. Objecten waarin een conflict is ontstaan, worden gegroepeerd door de externe verbinding waarmee de verbinding met de oorspronkelijke locatie tot stand is gebracht. Als u deze lijsten wilt openen, gaat u naar *CMC* > *Federatie* > *Herhalingsfouten* > *Externe verbinding*.

> ⓘ Opmerking
>
> Wanneer een herhalingstaak die gebruikmaakt van een externe verbinding is voltooid, wordt de lijst bijgewerkt. Deze lijst bevat alle conflicterende objecten voor alle herhalingstaken die gebruikmaken van de desbetreffende externe verbinding. Alle herhaalde objecten op een doellocatie worden gemarkeerd met het herhalingspictogram. Als er een conflict is, worden objecten gemarkeerd met het conflictpictogram.

Voorbeeld

Michel wijzigt rapport A op de oorspronkelijke locatie. Daan wijzigt de herhaalde versie van het rapport op de doellocatie. Wanneer de volgende herhalingstaak wordt uitgevoerd, ontstaat er een conflict in het rapport, omdat dit op beide locaties is gewijzigd en het conflict niet automatisch wordt opgelost.

Het rapport op de doellocatie blijft ongewijzigd en de wijzigingen in het rapport op de oorspronkelijke locatie worden niet herhaald. Alle volgende replicatietaken worden op dezelfde manier verwerkt, totdat het conflict is opgelost. Wijzigingen in het rapport op de oorspronkelijke locatie worden niet herhaald totdat het conflict handmatig is opgelost door de (gedelegeerde) beheerder.

> ⓘ Opmerking
>
> In dit geval wordt het object niet herhaald. Ook wijzigingen die geen conflict veroorzaken, worden niet herhaald.

> **Opmerking**
>
> Gebruikers die toegang hebben tot de CMC en de herhalingstaken, kunnen het XML-logboek raadplegen; dit wordt in de map voor logboekbestanden geplaatst. Met een objectpictogram van een doellocatie wordt een conflict aangeduid. Tijdens de verwerking wordt er een conflictlogboek gemaakt.

De beheerder kan in het gebied Federatie van de CMC een lijst ophalen met alle herhaalde objecten waarin een conflict is ontstaan. Objecten waarin een conflict is ontstaan, worden gegroepeerd door de externe verbinding waarmee de verbinding met de oorspronkelijke locatie tot stand is gebracht. Als u deze lijsten wilt openen, gaat u naar *CMC* > *Federatie* > *Herhalingsfouten* > *Externe verbinding*.

> **Opmerking**
>
> Wanneer een herhalingstaak die gebruikmaakt van een externe verbinding is voltooid, wordt de lijst bijgewerkt. Deze lijst bevat alle conflicterende objecten voor alle herhalingstaken die gebruikmaken van de desbetreffende externe verbinding. Alle herhaalde objecten op een doellocatie worden gemarkeerd met het herhalingspictogram. Als er een conflict is, worden objecten gemarkeerd met het conflictpictogram.

Er zijn drie opties voor het handmatig oplossen van een conflict:

1. Maak een herhalingstaak waarmee alleen de conflicterende objecten worden herhaald. Deze taak moet gebruikmaken van dezelfde externe verbinding en herhalingslijst.
   Als u de wijzigingen op de oorspronkelijke locatie wilt behouden, maakt u een herhalingstaak. Stel Herhalingsmodus vervolgens in op “Vernieuwen vanaf oorsprong” en Automatische conflictoplossing op “Oorspronkelijke site heeft voorrang”.
   Als u de wijzigingen op de doellocatie wilt behouden, maakt u een herhalingstaak en stelt u Herhalingstype in op “Herhaling in beide richtingen”, Herhalingsmodus op “Vernieuwen vanaf doel” en Automatische conflictoplossing op “Doelsite heeft voorrang”.

   > **Opmerking**
   >
   > Stel in de herhalingsmodus “Vernieuwen vanaf oorsprong” of “Vernieuwen vanaf doel” in om alleen de conflicterende objecten in de herhalingslijst te selecteren. Op deze manier worden andere objecten niet herhaald. Plan vervolgens wanneer de herhalingstaak moet worden uitgevoerd; de geselecteerde objecten worden herhaald en het conflict wordt opgelost zoals aangegeven.

2. Maak een herhalingstaak waarmee alleen de conflicterende objecten worden herhaald. Deze taak moet gebruikmaken van dezelfde externe verbinding. In tegenstelling tot hetgeen het geval is bij optie 1, kunt u echter een nieuwe herhalingslijst maken op de oorspronkelijke locatie. Gebruik alleen de conflicterende objecten en maak een nieuwe herhalingstaak voor deze specifieke herhalingslijst.
   Om de wijzigingen op de oorspronkelijke locatie te behouden, stelt u de automatische conflictoplossing in op: “Oorspronkelijke locatie heeft voorrang”.
   Om de wijzigingen op de doellocatie te behouden, stelt u de automatische conflictoplossing in op: “Doellocatie heeft voorrang” en het herhalingstype op: “Herhaling in twee richtingen”.
3. Verwijder het object van de locatie waarop deze zich niet moet bevinden.

> **Opmerking**
>
> Wees voorzichtig bij het verwijderen van objecten, omdat andere objecten die hiervan afhankelijk zijn, hierdoor mogelijk worden verwijderd, uitgeschakeld of niet meer zijn beveiligd. Optie 1 en 2 worden aanbevolen.

Als u de wijzigingen op de doellocatie wilt behouden, kunt u het object op de oorspronkelijke locatie verwijderen. De volgende keer dat de herhalingstaak wordt uitgevoerd, wordt het object van de doellocatie naar de oorspronkelijke locatie herhaald.

> ⓘ Opmerking
>
> Wees voorzichtig bij het verwijderen van een object op een oorspronkelijke locatie; andere doellocaties die dat object herhalen, voeren hun herhalingstaak mogelijk uit voordat de kopie weer is teruggeplaatst. Hierdoor wordt het object op de andere doellocaties verwijderd en is het pas weer beschikbaar wanneer de kopie is teruggeplaatst.

Als u de wijzigingen op de oorspronkelijke locatie wilt behouden, kunt u het object op de doellocatie verwijderen.

27.12 Webservices gebruiken in Federatie

De functie Federatie gebruikt webservices voor het verzenden van objecten en de bijbehorende wijzigingen van de oorspronkelijke locatie naar doellocatie(s) en omgekeerd. Federatie-specifieke webservices worden automatisch in de installatie van BI-platform geïnstalleerd en geïmplementeerd. Mogelijk wilt u echter eigenschappen of aangepaste implementaties in webservices aanpassen om de functionaliteit te verbeteren, zoals in deze sectie wordt beschreven.

> → Tip
>
> Voor het verbeteren van bestandsbeheer en -functionaliteit, schakelt u de bestandencache in Federatie in.

27.12.1 Sessievariabelen

Als u veel inhoudsbestanden wilt overdragen in één herhalingstaak, kunt u overwegen om de sessietime-out voor de Federatie-webservices te verhogen.

Deze eigenschap bevindt zich in het bestand `dsws.properties`:

```
<installatiemap toepassingsserver>\dswsbobje\Web-INF\classes
```

Bijvoorbeeld:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\classes
```

Activeer een sessievariabele door het volgende op te geven:

```
session.timeout = x
```

Waarbij “x” de gewenste tijd aanduidt; “x” wordt gemeten in seconden. Als deze niet is opgegeven, is de standaardwaarde 1200 seconden of 20 minuten.

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om het WAR-

bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

27.12.2 Bestandencache

De bestandencache stelt webservices in staat zeer grote bijlagen te verwerken zonder het geheugen als buffer te gebruiken. Als de bestandencache niet is ingeschakeld bij de overdracht van grote volumes, loopt het geheugen van Java Virtual Machine mogelijk helemaal vol en mislukt de herhalingsbewerking.

> ⓘ Opmerking
>
> Het gebruik van de bestandencache komt de prestaties ten goede, omdat de webservices voor de verwerking gebruikmaken van bestanden in plaats van het geheugen. U kunt ook een combinatie van beide mogelijkheden gebruiken door grote hoeveelheden naar een bestand te sturen en kleinere naar het geheugen.

Als u de bestandencache wilt inschakelen, past u het bestand `Axis2.xml` aan op de volgende locatie:

```
<installatiemap toepassingsserver>\dswsbobje\Web-Inf\conf
```

Bijvoorbeeld:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
```

Typ het volgende:

```
<parameter name="cacheAttachments" locked="false">true</parameter>

<parameter name="attachmentDIR" locked="false">temp directory</parameter>

<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> ⓘ Opmerking
>
> De eenheid voor de drempelwaarde is bytes.

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

27.12.3 Aangepaste implementatie

Federatie-webservices kunnen automatisch worden geïmplementeerd en hiervoor moeten de services “federator”, “biplatform” en “session” worden geactiveerd. Als u Federatie of een andere webservice wilt uitschakelen, past u het desbetreffende webservicesbestand `service.xml` aan.

De webservices van BI-platform bevinden zich in:

```
<installatiemap toepassingsserver>\dswsbobje\WEB-INF\services
```

Voorbeeld:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services
```

Webservices uitschakelen:

- Voeg de eigenschap “activate” toe aan de code voor de servicenaam in het bestand `service.xml` en stel deze in op False.
- Start de Java-toepassingsserver opnieuw op.

Voorbeeld: Federatie uitschakelen

Het bestand `services.xml` bevindt zich in:

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Wijzig de servicenaam van:

```
<service name="Federator">
```

in:

```
<service name="Federator" activate="false">
```

De nieuwe eigenschappen worden pas toegepast nadat de gewijzigde webtoepassing opnieuw is geïmplementeerd op de computer die de webtoepassingsserver uitvoert. Gebruik WDeploy om het WAR-bestand opnieuw op de webtoepassingsserver te implementeren. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* als u informatie wilt over het gebruik van WDeploy.

27.13 Externe planning en lokaal uitgevoerde exemplaren

In deze sectie wordt aandacht besteed aan externe planning, lokaal uitgevoerde exemplaren en gedeelde exemplaren. Met deze functies kunnen rapporten worden uitgevoerd op de locatie waar de gegevens zijn opgeslagen en worden de voltooide exemplaren vervolgens naar de juiste locatie verzonden.

27.13.1 Externe planning

In Federatie kunt u een rapport plannen op de doellocatie en vervolgens verwerken op de oorspronkelijke locatie. Het verwerkte exemplaar wordt geretourneerd naar de doellocatie.

Als u externe planning wilt inschakelen, plant u een rapport op de gebruikelijke manier en schakelt u de optie “Uitvoeren op oorspronkelijke locatie” in. Als u deze optie wilt inschakelen, klikt u op *Planning* > *Servergroep voor planning* > *Uitvoeren op oorspronkelijke locatie*. Nadat de geplande exemplaren zijn gemaakt, krijgen ze de status Uitstaand.

Bij externe planning worden de verzonden gegevens op de doellocatie genegeerd en behoudt het rapportexemplaar de status In behandeling.

Wanneer voor de volgende herhalingstaak de optie voor externe planning is ingeschakeld, wordt het rapportexemplaar voor verwerking naar de oorspronkelijke locatie gekopieerd. Het exemplaar blijft uitstaand totdat het door de Scheduler is verwerkt. Intussen worden alle eerder voltooide exemplaren en objectwijzigingen geretourneerd door de herhalingstaak die het exemplaar heeft verzonden.

Wanneer het exemplaar op de oorspronkelijke locatie is verwerkt, krijgt het de status Voltooid. Wanneer de volgende herhalingstaak voor het rapport in de externe planning wordt uitgevoerd, wordt het voltooide exemplaar gebruikt om de kopie op de doellocatie bij te werken. Nadat het exemplaar is bijgewerkt, krijgt het op de doellocatie de status Voltooid.

> ⓘ Opmerking
>
> Een herhalingstaak moet tweemaal worden uitgevoerd voordat een exemplaar de status Voltooid krijgt.

Voorbeeld

1. Tom schakelt externe planning in voor rapport A.
2. Rapport A wordt op de doellocatie gemaakt en heeft de status In behandeling.
3. Herhalingstaak A wordt uitgevoerd. Eerst worden wijzigingen op de oorspronkelijke locatie herhaald naar de doellocatie (inclusief wijzigingen in eerder voltooide exemplaren). Vervolgens wordt het uitstaande exemplaar gekopieerd naar de oorspronkelijke locatie, evenals de wijzigingen die van de doellocatie naar de oorspronkelijke locatie moeten worden gerepliceerd.
4. Het exemplaar met de status In behandeling wordt op de oorspronkelijke locatie door de Scheduler naar de juiste Job Server verzonden voor verwerking. Het exemplaar wordt verwerkt en met de status Voltooid op de oorspronkelijke locatie geplaatst.
5. Herhalingstaak A wordt weer uitgevoerd. Wanneer de inhoud van de oorspronkelijke locatie naar de doellocatie wordt herhaald, wordt het voltooide rapportexemplaar A verzonden en worden de wijzigingen aangebracht in de versie op de doellocatie.
6. Wanneer deze taak is voltooid, is de versie op de doellocatie voltooid.

Externe planning werkt alleen voor herhalingstaken in beide richtingen. De optie “Externe planningen herhalen” moet zijn ingeschakeld. Deze optie bevindt zich op de pagina *Eigenschappen van herhalingstaak* in het gebied “Herhalingsfilters”. Het kan voorkomen dat u extern geplande taken vaker wilt herhalen dan de andere objecten in uw herhalingslijst. Maak hiertoe twee herhalingstaken. Voor de taak waarmee u de extern geplande objecten wilt herhalen, schakelt u “Externe planningen herhalen” in. Schakel voor de andere taak de optie “Documentsjablonen herhalen” of “Alle objecten herhalen (geen filter)” in.

> ⓘ Opmerking
>
> Als u externe planning inschakelt, worden voltooide en mislukte exemplaren op zowel de oorspronkelijke locatie als op de doellocatie weergegeven.
>
> Als een gebruiker op de doellocatie de optie voor externe planning voor een rapport inschakelt terwijl deze gebruiker niet bestaat op de oorspronkelijke locatie, mislukt het exemplaar op de oorspronkelijke locatie. De eigenaar van het mislukte exemplaar is de gebruikersaccount van het object Externe verbinding waarmee de verbinding naar de oorspronkelijke locatie is gemaakt.

> Hoewel een herhalingstaak alleen voor externe planning kan worden ingesteld, blijft het de hogerliggende objecten van het rapportexemplaar herhalen. Als er wijzigingen worden aangebracht tussen herhalingen, houdt dit in dat het werkelijke rapport, de rapportmap, enzovoort worden herhaald. Als u niet wilt dat deze wijzigingen op de doellocatie worden herhaald naar de oorspronkelijke locatie, kunt u met behulp van beveiligingsrechten bepalen welke wijzigingen worden herhaald.

Verwante informatie

Beveiligingsrechten beheren [pagina 965]

27.13.2 Lokaal uitgevoerde exemplaren

Lokaal uitgevoerde exemplaren zijn exemplaren van een rapport die zijn gegenereerd op basis van rapporten op de doellocatie. In Federatie kunt u de voltooide exemplaren op de doellocatie herhalen naar de oorspronkelijke locatie.

Als met een herhalingstaak voltooide en mislukte exemplaren van de doellocatie moeten worden herhaald naar de oorspronkelijke locatie, klikt u op *Eigenschappen van herhalingstaak* > *Herhalingsfilters* > *Lokaal uitgevoerde, voltooide exemplaren herhalen*.

In bepaalde gevallen wilt u met een herhalingstaak alleen lokaal uitgevoerde exemplaren herhalen. Schakel hiertoe “Lokaal uitgevoerde, voltooide exemplaren herhalen” in.

> ⓘ Opmerking
>
> Wanneer u lokaal uitgevoerde exemplaren inschakelt voor een herhalingstaak, worden zowel voltooide als mislukte exemplaren herhaald naar de oorspronkelijke locatie. Dit betekent dat er zowel op de oorspronkelijke locatie als op de doellocatie kopieën zullen zijn.
>
> Uitstaande exemplaren worden nooit gerepliceerd.
>
> Als de eigenaar van een lokaal uitgevoerd exemplaar niet op de oorspronkelijke locatie bestaat, wordt de gebruikersaccount die voor het maken van de verbinding met het object Externe verbinding wordt gebruikt de eigenaar.

27.13.3 Exemplaren delen

Als u de opties voor externe planning en lokaal uitgevoerde exemplaren voor een herhalingstaak inschakelt, worden exemplaren mogelijk gedeeld wanneer u één oorspronkelijke locatie met vele doellocaties hebt waarop hetzelfde rapport wordt herhaald.

Voorbeeld

Rapport A bevindt zich op de oorspronkelijke locatie en wordt door zowel doellocatie A als B herhaald. Het delen van exemplaren vindt plaats op beide doellocaties:

- Bij ingeschakelde herhalingstaken met "Externe planningen herhalen" en/of "Lokaal uitgevoerde, voltooide exemplaren herhalen" wordt rapport A herhaald met dezelfde bovengenoemde herhalingstaak.
- Rapport A is op de doellocatie gepland voor "uitvoering op de oorspronkelijke locatie" en/of voor lokale uitvoering.

In het geval waarin rapport A op zowel doellocatie A als B wordt herhaald en de bijbehorende herhalingstaken externe planning en/of lokaal uitgevoerde exemplaren herhalen, worden alle exemplaren die op doellocatie A en/of namens doellocatie A op de oorspronkelijke locatie zijn verwerkt, met doellocatie B gedeeld.

Zo ook worden exemplaren die op doellocatie B en/of de oorspronkelijke locatie zijn verwerkt, gedeeld met doellocatie A. Uiteindelijk zullen op de oorspronkelijke locatie en de doellocaties A en B identieke exemplaren voorkomen.

Het delen van exemplaren is in veel gevallen ideaal. Bijvoorbeeld wanneer gebruikers van andere locaties gegevens moeten kunnen opvragen bij andere vestigingen. Als u in dergelijke gevallen wilt voorkomen dat exemplaren door lokale gebruikers worden weergegeven, moet u de juiste beveiligingsrechten instellen. Pas de rechten bijvoorbeeld toe op een rapportobject, zodat gebruikers alleen de exemplaren te zien krijgen waarvan ze zelf de eigenaar zijn.

> **Opmerking**
>
> Op alle objecten zijn de beveiligingsregels van BI-platform van toepassing. Als u ervoor wilt zorgen dat gebruikers en groepen alleen bepaalde exemplaren kunnen weergeven, wordt u aangeraden rechten in te stellen, zodat de gebruikers alleen exemplaren kunnen weergeven waarvan ze zelf eigenaar zijn. Pas de rechten bijvoorbeeld toe op een rapportobject, zodat gebruikers alleen de exemplaren te zien krijgen waarvan ze zelf de eigenaar zijn.

Verwante informatie

Beveiligingsrechten beheren [pagina 965]

27.14 Herhaalde inhoud importeren en overbrengen

In bepaalde gevallen wilt u mogelijk herhaalde inhoud van het ene BI-platform importeren in of overbrengen naar het andere. In deze sectie wordt dit in het kader van federatie beschreven.

> **Opmerking**
>
> Objectmigraties kunnen het beste worden uitgevoerd door leden van de Beheerdersgroep, met name de gebruikersaccount Beheerder. Als u een object wilt migreren, moeten veel verwante objecten misschien ook worden gemigreerd. Het is misschien niet mogelijk om de vereiste beveiligingsrechten voor alle objecten te verkrijgen voor een gedelegeerde beheerdersaccount.

27.14.1 Herhaalde inhoud importeren

Als u met LifeCycle Manager inhoud van de ene implementatie van een BI-platform naar een andere importeert, worden via LifeCycle Manager geen herhalingsspecifieke gegevens geïmporteerd die zijn gekoppeld aan herhaalde objecten die worden geïmporteerd. Dit betekent dat het object zich na het importeren gedraagt alsof het niet is herhaald. Dit is kenmerkend voor herhaalde objecten op een doellocatie en wordt in het volgende scenario beschreven.

Voorbeeld

BI-platform A is een doelsite in een federatieproces. Rapport A, een herhaald rapport op systeem A, wordt met LifeCycle Manager van systeem A geïmporteerd naar BI-platform B.

Resultaat: wanneer rapport A naar BI-platform B wordt gekopieerd, bevat het geen herhaalde gegevens. Rapport A wordt niet meer gemarkeerd met een herhalingspictogram. Als het object een conflict had op BI-platform A, is dit niet het geval op systeem B. Het object wordt beschouwd als een object dat zich oorspronkelijk op systeem B bevond.

> ⓘ Opmerking
>
> De CUID kan al dan niet gelijk zijn, afhankelijk van de importopties die u in LifeCycle Manager opgeeft.

27.14.2 Herhaalde inhoud importeren en herhaling voortzetten

Wanneer u herhaalde inhoud hebt geïmporteerd, wilt u de geïmporteerde objecten mogelijk opnemen in een Federatie-proces. Er zijn twee scenario's: gebruik het systeem met de geïmporteerde objecten als oorspronkelijke locatie of gebruik het systeem als doellocatie. Wanneer u dit systeem als oorspronkelijke locatie wilt gebruiken, gaat u op de gebruikelijke manier verder met Federatie.

Wanneer u het systeem als doellocatie wilt gebruiken en de geïmporteerde objecten van de oorspronkelijke locatie wilt herhalen, gaat u als volgt te werk:

- Zorg ervoor dat de CUID van de objecten behouden blijft wanneer u LifeCycle Manager gebruikt.
- Let erop dat conflictoplossing voor de eerste herhalingstaak is ingesteld op “Oorspronkelijke locatie wint” of “Doellocatie wint”.

> → Tip
>
> In plaats van het object met LifeCycle Manager van een doellocatie te importeren in een andere doellocatie, is het efficiënter en aan te bevelen het object alleen te herhalen met Federatie.

Voorbeeld

Rapport A is gemaakt op BI-platform A. Op systeem X is Federatie gebruikt om rapport A van systeem A naar systeem X te herhalen. Vervolgens is rapport A met LifeCycle Manager van systeem X geïmporteerd in systeem Y.

Plan: systeem Y wil Federatie instellen op systeem A en rapport A behouden als onderdeel van de herhaling. Systeem Y is de doellocatie en Systeem A de oorspronkelijke locatie.

Actie: wanneer rapport A van systeem X wordt geïmporteerd in systeem Y, moet de CUID van rapport A behouden blijven. Wanneer de eerste herhalingstaak wordt uitgevoerd, wordt bovendien geprobeerd rapport A te herhalen. Aangezien het object al voorkomt op systeem Y, leidt herhaling tot een conflict. Geef aan welke versie moet worden gebruikt door conflictoplossing in te stellen op "Oorspronkelijke locatie wint" of "Doellocatie wint".

> ⓘ Opmerking
>
> In dit voorbeeld is het raadzaam het object niet met LifeCycle Manager van een doellocatie te importeren in een andere doellocatie, maar het object te herhalen met Federatie. Rapport A wordt herhaald van systeem A naar systeem Y en u hoeft LifeCycle Manager niet te gebruiken voor het importeren van systeem X in systeem Y.

27.14.3 Inhoud overbrengen vanuit een testomgeving

In alle organisaties wordt eerst een testfase doorlopen voordat een product in een productieomgeving wordt geplaatst. Het is gebruikelijk om Federatie tussen BI-platformsystemen in een ontwikkel- of testomgeving te testen voordat Federatie wordt ingesteld op de productiecomputers. Wanneer u de oorspronkelijke locatie en doellocaties en de inhoud in een testomgeving hebt gemaakt, kunt u deze instellingen aan de hand van de volgende stappen overbrengen naar de productiecomputers:

1. Gebruik LifeCycle Manager om de inhoud van de oorspronkelijke locatie in de testomgeving over te brengen naar de productiecomputer die als oorspronkelijke locatie fungeert.

   > ⓘ Opmerking
   >
   > Wanneer u LifeCycle Manager gebruikt, kunt u het herhalingslijstobject niet selecteren.

2. Maak de herhalingslijst op de oorspronkelijke locatie in de productieomgeving en neem de gewenste inhoud op.
3. Kies een van de volgende twee opties:
   - A) Maak een externe verbinding en de gewenste herhalingstaken op de productiecomputers die als doellocaties zullen fungeren.
   - B) Importeer met LifeCycle Manager de externe verbinding en de herhalingstaken van de doellocatie in de ontwikkel- of QA-omgeving in de productiecomputers die als doellocaties fungeren. Bewerk de geïmporteerde externe verbindingen vervolgens, zodat ze verwijzen naar de productiecomputer die als oorspronkelijke locatie fungeert.

27.14.4 Opnieuw verwijzen naar een doellocatie

Als een object vanuit een oorspronkelijke site is herhaald, moet het momenteel altijd vanuit deze site worden herhaald en kan het niet vanaf een ander BI-platform worden herhaald als het externe verbindingsobject wordt bewerkt om naar een nieuw systeem te wijzen. Wanneer u een object probeert te herhalen dat vanuit een ander BI-platformsysteem is herhaald, kan het externe verbindingsobject niet worden herhaald. Als u een object wilt herhalen vanaf een andere oorspronkelijke locatie, moet u het eerst van de doellocatie verwijderen.

> ⓘ Opmerking
>
> Wanneer u een herhaald object kopieert, wordt de CUID van de kopie gewijzigd en bevat de kopie geen herhalingsgegevens.

27.15 Gebruiksadviezen

U kunt Federator gebruiken om de prestaties van een herhalingstaak te optimaliseren.

Als één herhalingstaak een groot aantal objecten bevat, kunt u extra stappen uitvoeren om te zorgen dat de taak goed wordt uitgevoerd. Per herhalingstaak kunt u gewoonlijk maximaal 32.000 objecten herhalen. Voor bepaalde implementaties kan het echter nodig zijn om configuraties in te stellen met meer of minder herhalingen.

1) Configureer een exclusieve webserviceprovider.

Als u gebruikmaakt van Federatie, wordt herhaalde inhoud via webservices verzonden. Bij een standaardinstallatie van het BI-platform wordt dezelfde webserviceprovider gebruikt voor alle webservices. Grotere herhalingstaken kunnen de webserviceprovider langer bezet houden en mogelijk een vertraagde respons op andere webserviceaanvragen of toepassingen veroorzaken.

Als u een groot aantal objecten tegelijkertijd wilt herhalen of verscheidene herhalingstaken achter elkaar wilt uitvoeren, kunt u overwegen om de webservices voor Federatie op een exclusieve Java-toepassingsserver te implementeren of een exclusieve webserviceprovider te gebruiken.

Gebruik hiervoor het installatieprogramma van BI-platform om webservices te installeren. Er moet al een Java-toepassingsserver actief zijn. Als u dit niet doet, installeert u de optie Onderdelen weblaag volledig zodat hiermee de webservices en Tomcat worden geïnstalleerd.

> ⓘ Opmerking
>
> U moet informatie opgeven voor een bestaande CMS (bijvoorbeeld hostnaam, poort en wachtwoord van de beheerder).

> ⓘ Opmerking
>
> Geef de URI van de nieuwe webserviceprovider op in het veld voor de URI van de externe verbinding.

2) Vergroot het geheugen van de Java-toepassingsserver.

Vergroot het beschikbare geheugen van de Java-toepassingsserver als u per herhalingstaak veel objecten wilt herhalen of als de toepassingsserver wordt gedeeld met andere toepassingen.

Als u het BI-platform en Tomcat hebt geïmplementeerd, is de standaardgrootte van het beschikbare geheugen 1 GB. Het beschikbare geheugen voor Tomcat vergroten:

Windows:

1. Klik op *Start* > *Programma's* > *Tomcat* > *Tomcat-configuratie*.
2. Selecteer *Java*.
3. Zoek in het tekstvak *Java-opties* naar de vermelding `-Xmx1024M`
4. Verhoog de waarde van de parameter `-Xmx1024M`.

Voorbeeld

Als u het geheugen wilt vergroten tot 2 GB, geeft u op: `-Xmx2048M`

Unix:

1. Ga naar `<BOE_installatiemap>/setup/` en open `env.sh` in een teksteditor. Verhoog de waarde van de parameter `-Xmx1024m`.
2. Zoek de volgende regels op:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

> **Opmerking**
>
> In BI 4.2 Support Package 5 kunt u de parameter MaxMetaspaceSize gebruiken om geheugengrootte van metaspace te definiëren, en niet de parameter MaxPermSize.
>
> - Als u een upgrade uitvoert van eerdere versies dan BI 4.2 Support Package 5 naar BI 4.2 Support Package 5, moet u de parameter voor alle bestaande servers handmatig bewerken.
> - Als u een nieuwe installatie van BI 4.2 Support Package 5 uitvoert, wordt de parameter standaard vervangen.

3. Verhoog de waarde van de parameter `-Xmx1024m`.

Voorbeeld

Als u het geheugen wilt vergroten tot 2 GB, geeft u op: `-Xmx2048m`

> **Tip**
>
> Als u het geheugen van een andere Java-toepassingsserver wilt vergroten, raadpleegt u de documentatie bij de gewenste server.

3) Verlaag de grootte van de BIAR-bestanden die worden gemaakt.

De functie Federatie gebruikt webservices voor het herhalen van inhoud van de oorspronkelijke locatie naar de doellocatie en omgekeerd. Omwille van een efficiënte verzending worden objecten gegroepeerd en in BIAR-bestanden gecomprimeerd.

Als u een groot aantal objecten wilt herhalen, stelt u de Java-toepassingsserver zo in dat er kleinere BIAR-bestanden worden gemaakt. Federatie zorgt ervoor dat de objecten over een aantal kleinere BIAR-bestanden worden verdeeld, zodat u altijd net zoveel objecten kunt herhalen als u zelf wilt.

U kunt de grootte van de BIAR-bestanden verkleinen door de volgende Java-parameters aan de Java-toepassingsserver toe te voegen:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

Met `bobj.biar.suggestSplit` wordt ernaar gestreefd de nieuwe waarde voor de BIAR-bestanden te benaderen. De nieuwe waarde is 90 MB.

Met `bobj.biar.forceSplit` wordt de nieuwe waarde voor de BIAR-bestanden geforceerd als maximum gehanteerd. De nieuwe waarde is 100 MB.

> **Opmerking**
>
> U hoeft de standaardgrootte voor BIAR-bestanden pas aan te passen als het geheugen van de toepassingsserver ontoereikend is en de maximale heapgrootte niet meer kan worden verhoogd.

Tomcat in Windows:

1. Voor het openen van het hulpprogramma *Tomcat-configuratie* klikt u op *Start* > *Programma's* > *Tomcat* > *Tomcat-configuratie*.
2. Selecteer *Java*.
3. Voeg in het tekstvak *Java-opties* de volgende regels aan het einde toe:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

Tomcat in Unix/Linux:

1. Open het bestand Env.sh in een teksteditor. Dit bestand bevindt zich in `<BOE_installatiemap>/setup/`.
2. Zoek de volgende regels op:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Voeg de gewenste parameters voor de grootte van de BIAR-bestanden toe.

Voorbeeld: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

Raadpleeg voor andere Java-toepassingsservers de documentatie bij de desbetreffende server.

4) Verhoog de sockettime-out.

De herhalingstaak wordt door de Adaptive Job Server uitgevoerd. Tijdens het uitvoeren van de herhalingstaak maakt de Adaptive Job Server verbinding met de oorspronkelijke locatie. Wanneer er grote hoeveelheden gegevens van de oorspronkelijke locatie worden ontvangen, is het belangrijk dat er geen time-out optreedt in de socket die door de Adaptive Job Server wordt gebruikt voor het ontvangen van gegevens.

De standaardwaarde is 90 minuten. U kunt de sockettime-out desgewenst verhogen.

De sockettime-out verhogen op de Adaptive Job Server:

1. Open de CMC (Central Management Console).
2. Ga naar de sectie *Server* en selecteer *Adaptive Job Server*.
3. Klik op *Eigenschappen*.
4. Voeg "opdrachtregelparameters" toe aan het einde van het volgende:
   - **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
   - **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

Verwante informatie

Probleemoplossing bij foutberichten [pagina 1005]
Webservices gebruiken in Federatie [pagina 993]
Beperkingen van de huidige release [pagina 1004]

27.15.1 Beperkingen van de huidige release

Federatie is een flexibel hulpprogramma. Tijdens de productie kunnen de prestaties echter worden beïnvloed door bepaalde beperkingen. In deze sectie wordt beschreven welke wijzigingen u kunt aanbrengen om optimaal resultaat te bereiken met bewerkingen die u uitvoert in Federatie.

- Maximum aantal objecten
  Met elke herhalingstaak worden objecten tussen de BI-platformimplementaties herhaald. Het is raadzaam om het maximum aantal objecten dat u per herhalingstaak opgeeft te beperken tot 100.000. Hoewel herhalingstaken met meer dan 100.000 objecten mogelijk worden uitgevoerd, ondersteunt Federatie maximaal 100.000 objecten.
- Rechten
  In Federatie worden rechten alleen herhaald van de oorspronkelijke locatie naar de doellocatie.
  U wordt aangeraden om gebruikersrechten die voor beide implementaties gelden, in te stellen op de oorspronkelijke locatie en met de optie Herhaling in beide richtingen te herhalen naar de doellocaties. Gebruikersrechten voor een specifieke locatie worden zoals gebruikelijk beheerd in een BI-platformimplementatie op de locatie waar de gebruiker zich bevindt.

- Business Views en gekoppelde objecten
  Op BI-platform kunnen Business Views-weergaven, Business Elements, gegevensverzamelingen, gegevensverbindingen en zoeklijsten worden opgeslagen. Met deze objecten wordt de functionaliteit van Crystal Reports-rapporten uitgebreid.
  Als deze objecten eerst op de doellocatie worden gemaakt en vervolgens naar de oorspronkelijke locatie worden herhaald met de optie Herhaling in beide richtingen, werken deze mogelijk niet juist en worden de bijbehorende gegevens mogelijk niet weergegeven in Crystal Reports-rapporten.
  Het is daarom raadzaam om Business Views-weergaven, Business Elements-items, gegevensverzamelingen, gegevensverbindingen en zoeklijsten op de oorspronkelijke locatie te maken en ze vervolgens naar de doellocatie te herhalen. Werk de objecten bij op de doellocatie of op de oorspronkelijke locatie (mits u over de vereiste rechten beschikt); de wijzigingen worden dan correct herhaald van de ene locatie naar de andere.
- Universe-overloads
  Op BI-platform kunnen universe-overloads worden opgeslagen. Als universe-overloads op de doellocatie worden gemaakt en vervolgens naar de oorspronkelijke locatie worden herhaald met de optie Herhaling in beide richtingen, functioneren ze mogelijk niet naar behoren.
  U kunt dit voorkomen door de universe-overloads eerst op de oorspronkelijke locatie te maken en ze vervolgens naar de doellocatie te herhalen. Vervolgens stelt u de gewenste beveiliging voor de universe-overloads in op de oorspronkelijke locatie en herhaalt u deze vervolgens naar de doellocatie.
- Objecten opschonen
  Bij het opschonen van objecten worden objecten verwijderd die op de andere locatie zijn verwijderd. Het opschonen van objecten wordt momenteel uitsluitend ondersteund van de oorspronkelijke locatie naar de doellocatie.
- Federatie-logboekbestanden
  Federatie-logboekbestanden worden opgeslagen in XML-bestanden op basis van XML 1.1-standaarden. Als u de logboekbestanden wilt weergeven in een browser, moet de browser XML 1.1 ondersteunen.

Verwante informatie

Opschoning van objecten beheren [pagina 985]

27.15.2 Probleemoplossing bij foutberichten

In deze sectie vindt u foutberichten die bij het gebruik van Federatie in uitzonderlijke gevallen worden weergegeven. Deze berichten worden vastgelegd in het logboekbestand voor herhalingstaken of in het functionaliteitsgedeelte van een rapport.

1) Ongeldige GUID

Voorbeeld van fout: `FOUT 2008-01-10T00:31:08.234Z De GUID ASXOOFyvy0FJnRcD0dZNTZg (gevonden in eigenschap SI_PARENT_CUID in objectnummer 1285) is geen geldige GUID`.

Deze fout geeft aan dat u een object herhaalt waarvan het bovenliggende object niet in de herhaling is opgenomen en nog niet voorkomt op de doellocatie. Dit doet zich bijvoorbeeld voor wanneer een object wordt herhaald, maar de map waarin het zich bevindt niet. Het bovenliggende object wordt mogelijk niet herhaald, omdat de account waarmee de objecten worden herhaald niet beschikt over de vereiste rechten voor het bovenliggende object.

2) Er worden in Crystal Reports-rapporten geen gegevens weergegeven op de oorspronkelijke locatie

Deze fout treedt mogelijk op wanneer het Crystal Reports-rapport gebruikmaakt van een Business Views-weergave, Business Elements-item, gegevensverzameling, gegevensverbinding of zoeklijst die op de doellocatie is gemaakt en vervolgens is herhaald naar de oorspronkelijke locatie.

3) Universe-overloads zijn niet juist toegepast.

Deze fout doet zich voor wanneer het Crystal Reports-rapport gebruikmaakt van een universe met daarin een universe-overbelasting die op de doellocatie is gemaakt en vervolgens naar de oorspronkelijke locatie is herhaald.

4) Java heeft onvoldoende geheugen.

Voorbeeld van fout: `java.lang.OutOfMemoryError`.

Deze fout doet zich voor wanneer het geheugen van de Java-toepassingsserver vol raakt tijdens het uitvoeren van een herhalingstaak. Mogelijk is de herhalingstaak te groot of is de geheugencapaciteit van de Java-toepassingsserver te klein.

Maak meer geheugen beschikbaar op de Java-toepassingsserver door Federatie-webservices naar een speciale computer te verplaatsen of geef minder objecten per herhalingstaak op.

5) Sockettime-out

Voorbeeld van fout: `Fout bij communicatie met oorspronkelijke locatie. Time-out tijdens lezen.`

De gegevens die van de oorspronkelijke locatie naar de Adaptive Job Server zijn verzonden, overschrijden de toegewezen time-out. Verhoog de time-out van de socket op de Adaptive Job Server of geef minder objecten op voor de herhalingstaak.

6) Querylimiet

Voorbeeld van fout: `SDK-fout opgetreden op doellocatie. Geen geldige query. (FWB 00025) …...Queryreeks is groter dan lengtelimiet query.`

Deze fout doet zich voor wanneer u te veel objecten tegelijkertijd herhaalt en er door Federatie een query wordt verzonden die te groot is voor de CMS. Objecten die van de oorspronkelijke locatie aan de doellocatie worden toegewezen. Wijzigingen die aan de oorspronkelijke locatie moeten worden toegewezen, worden echter niet verwerkt. Conflicten worden opgelost zoals opgegeven, maar er worden geen conflictaanduidingen voor handmatige oplossing op het object ingesteld. Objecten die aan de doellocatie zijn toegewezen, functioneren naar behoren.

U kunt dit probleem verhelpen door minder objecten per herhalingstaak op te geven.

7) Time-out voor herhalingstaak

Voorbeeld van fout: `Object kan niet worden gepland binnen het opgegeven tijdinterval`.

Dit bericht wordt mogelijk weergegeven wanneer er een time-out voor uw herhalingstaak is opgetreden tijdens het wachten op de voltooiing van een andere herhalingstaak. Deze situatie doet zich voor wanneer meerdere herhalingstaken gelijktijdig verbinding maken met dezelfde oorspronkelijke locatie. De mislukte herhalingstaak wordt op het volgende geplande tijdstip weer gestart.

U kunt dit probleem verhelpen door de mislukte herhalingstaak te plannen op een tijdstip dat niet samenvalt met de planning van andere herhalingstaken die dezelfde oorspronkelijke locatie hebben.

8) Herhalingslimiet

Voorbeeld van fout: `SDK-fout opgetreden op doellocatie. Fout bij databasetoegang. …. Fout in interne queryprocessor: De queryprocessor heeft geen stackruimte meer beschikbaar tijdens queryoptimalisatie. Fout bij uitvoeren query in ExecWithDeadlockHandling.`

Dit bericht wordt weergegeven wanneer het aantal ondersteunde objecten wordt overschreden dat gelijktijdig kan worden herhaald. U kunt dit probleem verhelpen door minder objecten voor de herhalingstaak op te geven. Voer de herhalingstaak vervolgens opnieuw uit.

9) Object is verwijderd

Voorbeeld van fout: `er is een fout opgetreden bij het controleren van de beveiligingsrechten` of `er is een fout opgetreden bij het inpakken van het object`.

Dit bericht wordt mogelijk weergegeven als een object is verwijderd uit het herhalingspakket. Dit kan voorkomen als via Federatie wordt gezocht naar een object dat moet worden herhaald, maar voordat de rechten worden gecontroleerd en het object wordt ingepakt.

10) Adaptive Processing Server

Voorbeeld van fout: `er is een fout opgetreden in de Job Processing Server`.

Deze fout kan optreden als er te veel klassen worden geladen via Federatie en er onvoldoende geheugen beschikbaar is voor de verwerking van de herhalingstaak.

U kunt dit probleem verhelpen door de volgende twee stappen uit te voeren:

1. Voeg in de opdrachtregelargumenten van de Adaptive Processing Server de volgende regel toe: `-javaArgs "XX:MaxMetaspaceSize=256m"`.

   > **Opmerking**
   >
   > In BI 4.2 Support Package 5 kunt u de parameter MaxMetaspaceSize gebruiken om geheugengrootte van metaspace te definiëren, en niet de parameter MaxPermSize.
   >
   > - Als u een upgrade uitvoert van eerdere versies dan BI 4.2 Support Package 5 tot BI 4.2 Support Package 5, moet u de parameter voor alle bestaande servers handmatig bewerken.
   > - Als u een nieuwe installatie van BI 4.2 Support Package 5 uitvoert, wordt de parameter standaard vervangen.

2. Voeg de volgende parameters toe aan de Java-toepassingsserver waarmee u verbinding maakt voor Federatie om de grootte van de BIAR-bestanden die u gebruikt, te beperken:
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

11) Adaptive Processing Servers aanpassen

Het nieuwe Java-argument `-XX:MetaspaceSize` is toegevoegd aan de APS-opdrachtregel in combinatie met de bestaande `-XX:MaxMetaspaceSize` om de initialisatie-ervaring te verbeteren en de ongewenste en complete schijfopruiming binnen het Java-proces gerelateerd aan Adaptive Processing Server(s) te vermijden.

Wanneer wordt getest op een VM met minimale RAM-resourcing, een standaard-APS en Alle services, lijken deze waarden voor MetaSpace en MaxMetaSpace de APS iets sneller te starten en te initialiseren dan de basisinstellingen. Er worden nul complete schijfopruimingen gemeld.

Voor meer informatie over *JAVA-opties van Adaptive Processing Servers aanpassen om volledige schijfopruiming te voorkomen met MetaSpace*, raadpleegt u SAP Note 3001317.

12) Object Manager-ruimte

Voorbeeld van fout: `Kan geen pushpakket maken. Er is een invoer-/uitvoeruitzondering opgetreden: "Onvoldoende ruimte op apparaat."`

Dit gebeurt als de tijdelijke map die door Federatie wordt gebruikt onvoldoende schijfruimte bevat. U kunt dit probleem verhelpen door extra ruimte vrij te maken in de tijdelijke map of een andere locatie voor de tijdelijke map te gebruiken.

Als u een andere locatie voor de tijdelijke map wilt opgeven op de oorspronkelijke locatie, voegt u de volgende regel toe aan de configuratiebestanden van de Java-toepassingsserver: `-Dbobj.tmp.dir=<TempDir>`.

Als u een andere locatie voor de tijdelijke map wilt opgeven op de doellocatie, voegt u de volgende regel toe aan de opdrachtregelargumenten van de Adaptive Processing Server: `-javaArgs "-Dbobj.tmp.dir=<TempDir>"`.

In de vorige voorbeelden is `<TijdelijkeMap>` de locatie van de tijdelijke map die u wilt gebruiken.

13) Universefout

Voorbeeld van fout: `Een interne fout opgetreden bij het aanroepen van API processDPCommands.`

Dit gebeurt als een universe die is herhaald, een ongeldige koppeling voor de universe-naar-universeverbinding heeft of als deze koppeling ontbreekt. U kunt dit probleem verhelpen door de herhalingstaak uit te voeren, waarbij u de optie *Vernieuwen vanaf oorsprong* hebt geselecteerd, en te controleren of de universeverbinding wordt herhaald.

U kunt de universe ook openen in Universe Designer, de verbinding van de universe bewerken en de universe opnieuw toewijzen.

Verwante informatie

Gebruiksadviezen [pagina 1001]
Beperkingen van de huidige release [pagina 1004]

28 Aanvullende configuraties voor ERP-omgevingen

28.1 Configuraties voor SAP NetWeaver-integratie

28.1.1 Integreren met SAP Business Warehouse (BW)

28.1.1.1 Overzicht

In deze sectie wordt getoond hoe u BW configureert om het publiceren van rapporten vanuit de toepassing SAP NetWeaver Business Warehouse naar het BI-platform in te schakelen en te beheren.

Voordat u met deze sectie begint, moet u de configuratie van de SAP-verficatie-invoegtoepassing hebben voltooid in de CMC.

Verwante informatie

SAP-verificatie configureren [pagina 330]

28.1.1.1.1 Mappen en beveiliging instellen in het BI-platform

Wanneer u een machtigingssysteem definieert in het BI-platform, maakt het systeem een logische mappenstructuur die overeenkomt met uw SAP-systeem. Wanneer u functies importeert en inhoud naar het BI-platform publiceert, worden er corresponderende mappen gemaakt. Als beheerder hoeft u deze mappen niet te maken. Deze mappen worden gemaakt in reactie op het definiëren van een machtigingssysteem, wanneer u de SAP-verificatie-invoegtoepassing configureert, de functies importeert in de CMC en inhoud publiceert naar het BI-platform.

> **Opmerking**
>
> De beheerder van BI-platform is verantwoordelijk voor het toekennen van de juiste rechten aan deze mappen:
>
> - *SAP-map op hoogste niveau*
> Zorg dat de groep ledereen beperkte toegang heeft tot de SAP-map op het hoogste niveau.
> - *Systeem-id-mappen*
> Ken de principal Publisher de volgende rechten toe in de CMC:
>
> > **Opmerking**
> >
> > De principal Publisher is niet beschikbaar totdat inhoud wordt gepubliceerd.

- Objecten toevoegen aan map
- Objecten weergeven
- Objecten bewerken
- Rechten van gebruikers voor objecten wijzigen
- Objecten verwijderen

→ Tip

U kunt het beheren van rechten gemakkelijker maken door een aangepast toegangniveau voor Publisher te maken en dit toegangsniveau toe te kennen aan de principal Publisher voor relevante systeem-id-mappen.

Verwante informatie

Werken met toegangsniveaus [pagina 137]
Werking van rechten in BI-platform [pagina 123]

28.1.1.1.2 Standaardpatronen voor mappenbeveiliging

Als u vanuit SAP inhoud publiceert naar het BI-platform, wordt op het platform automatisch de resterende hiërarchie van functies, mappen en rapporten gemaakt. Het systeem ordent uw rapporten in mappen die op basis van de systeem-id en het clientnummer en de naam van de functie een naam krijgen:

- Het systeem maakt mappen op het hoogste niveau, dat wil zeggen de mappen SAP, 2.0 en de systeemmappen (`<SID>`), wanneer u een machtigingssysteem definieert.
- Het systeem maakt indien nodig functiemappen (als groepen geïmporteerd in het BI-platform) wanneer een functie vanuit BW wordt gepubliceerd.
- Het systeem maakt een inhoudsmap voor elke rol waarnaar inhoud is gepubliceerd.
- Voor elk rapportobject wordt beveiliging ingesteld, zodat gebruikers alleen de rapporten kunnen weergeven die tot hun functies behoren.

De beheerder is verantwoordelijk voor het toekennen van de juiste rechten aan leden van verschillende functies. In de Workbench voor contentbeheer kunt u rapportpublicatiefuncties beheren vanuit SAP BW. U kunt rollen van het SAP BW-systeem identificeren met bepaalde BI-platformsystemen, rapporten publiceren en rapporten synchroniseren tussen SAP BW en een BI-platformimplementatie.

Inhoudsmappen

Het BI-platform importeert een groep voor elke functie die is toegevoegd aan het machtigingssysteem zoals het is gedefinieerd in de CMC.

Teneinde ervoor te zorgen dat de geschikte standaardrechten worden toegekend aan alle leden van een rol voor het bewaren van inhoud, kent u in de Werkbank voor inhoudbeheer de juiste rechten toe voor elk

machtigingssysteem zoals het is gedefinieerd in het BI-platform. Als u de Werkbank voor inhoudbeheer wilt starten, voert u de transactie /CRYSTAL/RPTADMIN uit:

1. Breid in de Werkbank voor inhoudbeheer achtereenvolgens *Enterprise-systeem* en *Beschikbare systemen* uit.
2. Dubbelklik op het gewenste systeem.
3. Open het tabblad *Layout*.
4. Stel *Standaardbeveiligingsbeleid voor rapporten* in op *Weergeven*.
5. Stel *Standaardbeveiligingsbeleid voor rollenmap* in op *Weergeven op aanvraag*.
6. Klik op *OK*.

Deze instellingen worden in het BI-platform weergegeven voor alle inhoudsfuncties. Met andere woorden, functies waarnaar inhoud is gepubliceerd. Leden van deze functies kunnen nu geplande exemplaren van rapporten bekijken die zijn gepubliceerd naar andere functies en kunnen rapporten vernieuwen die zijn gepubliceerd naar functies waarvan zij lid zijn.

> **Opmerking**
>
> het wordt ten zeerste aanbevolen de activiteiten van functies gescheiden te houden. Zo is het bijvoorbeeld weliswaar mogelijk vanuit een beheerdersfunctie te publiceren, maar het is beter alleen vanuit functies van publishers te publiceren. Bovendien zijn functies voor het publiceren alleen bedoeld om te bepalen welke gebruikers inhoud kunnen publiceren. Publicatiefuncties moeten dus geen inhoud bevatten en publishers moeten publiceren naar functies voor het bewaren van inhoud die toegankelijk zijn voor normale functieleden.

28.1.1.1.3 Op BW-gebeurtenissen gebaseerde planning

U kunt nu objecten gebaseerd op BW-gebeurtenissen in het BI-platform plannen. U moet een vertrouwd kanaal van communicatie tussen een SAP NetWeaver Business Warehouse (BW)-systeem en het BI-platform vastleggen om planning gebaseerd op BW-gebeurtenissen te activeren.

28.1.1.1.3.1 BW-gebeurtenissen maken en configureren

Volg de onderstaande stappen om een BW-gebeurtenis te maken.

1. Meld uzelf aan bij CMC.
2. Ga naar *Gebeurtenissen* > *BW-gebeurtenissen*.
3. Selecteer om een nieuwe gebeurtenis te maken.
4. Geef een *Gebeurtenisnaam* en *Beschrijving* op.
5. Selecteer *Maken*.
   U hebt een nieuwe BW-gebeurtenis gemaakt.

28.1.1.1.3.2 BW-gebeurtenissen toevoegen tijdens het inplannen van een rapport

Volg de onderstaande stappen om een BW-gebeurtenis toe te voegen terwijl rapporten worden ingepland.

1. Ga in **CMC** naar het beheergebied *Mappen* en selecteer een rapport.
2. Selecteer in het contextmenu van het rapport de optie *Plannen*.
3. Ga in het deelvenster *Navigatie* naar *Gebeurtenissen* > *BW-gebeurtenissen*.
4. Selecteer een gebeurtenis uit *Beschikbare gebeurtenissen*.
5. Voeg het toe aan Gebeurtenissen om te wachten op het gebruik van >>.
6. Ga in het deelvenster *Navigatie* naar *Terugkeerpatroon*.
7. Geef de parameters *Object uitvoeren*, *Toegestaan aantal pogingen* en *Interval tussen pogingen in seconden* op.
8. Selecteer *Plannen*.

   Zodra de gebeurtenis is gestart, wijzigt de planningsstatus van het rapport naar **Actief** van **In behandeling**.

   > **Opmerking**
   >
   > De planningsstatus blijf in de status **In behandeling** state als (een) gebeurtenis(sen) die onder *Gebeurtenissen waarop wordt gewacht* is/zijn gedefinieerd, niet wordt gestart.

28.1.1.1.3.3 BI-platform en ABAP-systeem integreren

Dit onderwerp legt uit hoe u op een BW-gebeurtenis gebaseerde planning kunt activeren.

Volg de onderstaande stappen:

1. Configureer HTTPS/SSL voor elke willekeurige toepassingsserver in BI-platform en voeg de sleutel van het gedeelde geheim toe op `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`. Zie het onderwerp HTTPS/SSL configureren [pagina 519] voor WACS en SSL in Tomcat configureren [pagina 403] voor Tomcat.

   > **Opmerking**
   >
   > Raadpleeg de SAP Product Availablity Matrix (PAM) voor meer informatie over de ondersteunde toepassingsservers.

2. Exporteer het servercertificaat van het BI-platform vanuit een browser naar een lokaal systeem. U kunt de certificaten vanuit de Chrome-browser downloaden door de onderstaande stappen te volgen.
1. Ga naar http://<hostname>:<port_number>/biprws. Zie het onderwerp De basis-URL voor RESTful-webservices configureren [pagina 531] voor meer informatie over het specifieke poortnummer voor elke toepassing.
2. Open de ontwikkelaarstools van de Chrome-browser door op F12 te drukken.
3. Navigeer naar het tabblad *Beveiliging* en selecteer *Certificaat weergeven*.
   De wizard `Certificaat` wordt weergegeven.

4. Ga in de wizard `Certificaat` naar het tabblad *Details* en selecteer *Kopiëren naar bestand*.
   De *Wizard Certificaat exporteren* wordt weergegeven.
5. Selecteer *Volgende*.
6. Selecteer in de pagina *Bestandsindeling voor export* de indeling *Base-64 encoded X.509 (.CER)* en selecteer *Volgende*.
7. Geef een naam op voor het certificaatbestand en sla het bestand lokaal op.

3. Download het certificaat van het SAP NetWeaver BW-systeem.

1. Start SAP NetWeaver BW.
2. Ga naar de transactie *STRUSTSSO2*.
3. Navigeer naar *Systeem-PSE* > *Onderwerp* > *Eigen certificaat*.
4. Selecteer *Downloaden*.
5. Geef een bestandspad op en selecteer de bestandsindeling *Base64*.
6. Selecteer .

Het certificaat van het SAP NetWeaver BW-systeem wordt naar de opgegeven locatie gedownload.

4. Importeer het certificaat van het BI-platform naar het SAP NetWeaver BW-systeem.

1. Ga naar de transactie *STRUSTSSO2*.
2. Schakel over naar de *Bewerkingsmodus*.
3. Selecteer de map *SSL-client SSL-client (Standaard)*.
4. Selecteer *Importeren*.
5. Upload het certificaat van het SAP NetWeaver BW-systeem en selecteer *Toevoegen aan certificatenlijst*.
   Het certificaat wordt weergegeven in de *certificatenlijst*.
6. Sla de transactie op.

5. Importeer het certificaat van het SAP NetWeaver BW-systeem naar het BI-platform. Raadpleeg de twaalfde stap in het onderwerp HTTPS/SSL configureren [pagina 519] voor meer informatie over het importeren van certificaten.

6. Een gebruiker in het BI-platform maken.

> **Opmerking**
>
> U moet ervoor zorgen dat de gebruikersnaam in het BI-platform dezelfde is als in het SAP NetWeaver BW-systeem. Als systeemnaam van SAP NetWeaver BW bijvoorbeeld MijnSysteem is, dan moet u een gebruiker in het BI-platform met de naam MijnSysteem maken.

7. Creëer een HTTP-doel in het SAP NetWeaver BW-systeem.

1. Ga naar de transactie *SM59*.
2. Selecteer *HTTP-verbindingen met externe server*.
3. Kies .
4. Schakel in het venster *RFC-doel* om naar het tabblad Technische instellingen en voer de *Host*, *Poort* en *Padprefix* als respectievelijk `<hostname>`, `<port_number>` en `/biprws` in.
5. Schakel over naar het tabblad *Aanmelden & beveiliging* en selecteer *Actief* voor *SSL*.
6. Selecteer *DEFAULT SSL-client (standaard)* als *SSL-certificaat*.
7. Selecteer *Opslaan*.
8. Selecteer Verbinding testen Connection Test om de verbinding met het HTTP-doel te testen. Het resultaat van de verbindingstest wordt weergegeven en de statustekst wordt als OK weergegeven.

> **Opmerking**
>
> De HTTP-verbinding tussen SAP NetWeaver BW en het BI-platform is niet mogelijk als niet aan de onderstaande voorwaarden is voldaan.
>
> - Het BW-systeem moet zijn bijgewerkt en de versies TLS 1.1 en TLS 1.2 ondersteunen.
> - Het BW-systeem moet dezelfde Cipher Suites ondersteunen als de Cipher Suites die op het BI-platform worden ondersteund.

9. Maak een procesketen in het SAP NetWeaver BW-systeem.
1. Ga naar de transactie *RSPC*.
2. Open het contextmenu van *Procesketens* en selecteer *Weergavecomponent maken*.
3. Geef in het venster *Groepering maken* de *Toepassingscomponent* en de *Lange beschrijving* op.
   Een SAP Netweaver BW-component wordt gemaakt.
4. Selecteer in het contextmenu van de toepassingscomponent de optie *Procesketen maken*.
5. Geef de naam en beschrijving op en selecteer .
   Nadat u de naam van de nieuwe procesketen hebt opgegeven, wordt het dialoogvenster `Startproces invoegen` geopend. Hiermee kunt u een startproces voor de procesketen invoegen.
6. Geef de *Procesvariant*en en *Lange beschrijving* op en selecteer .
   Het venster Startproces verzorgen wordt weergegeven.
7. Selecteer *Condities bewerken* en selecteer *Direct* om de procesketen direct uit te voeren.
8. Selecteer *Opslaan* in het venster `Starttijdstip`.
9. Selecteer *Opslaan* in het venster `Startproces verzorgen`.
10. In het venster `Startproces invoegen` selecteert u .
    Procesketen wordt gemaakt.
10. Configureer het procestype in de procesketen.
1. Selecteer de proces die na de vorige stap uit de kolom *Procesketens* is gemaakt.
2. Vouw de map *Proces en nabewerking laden* uit en selecteer *Gebeurtenis activeren in SAP BOBJ BI-platform voor BW-gegevenswijzigingen*.
   Het dialoogvenster `Gebeurtenis activeren in SAP BOBJ BI -platform voor BW-gegevenswijzigingen invoegen` wordt geopend.
3. In *Gebeurtenis activeren in SAP BOBJ BI -platform voor BW-gegevenswijzigingen invoegen* selecteert u .
4. Voer de *Procesvarianten* en *Lange beschrijving* in.
5. Selecteer .
   Het venster `Procesverzorging` wordt weergegeven.
6. Selecteer voor *Doel* om een doel te kiezen.
7. Selecteer voor *Gebeurtenis* om een gebeurtenis te kiezen.
8. Sla de wijzigingen op.
9. Selecteer in het dialoogvenster `Gebeurtenis activeren in SAP BOBJ BI -platform voor BW-gegevenswijzigingen invoegen`.
   Het procestype wordt gemaakt.
11. Activeer de procesketen en voer deze uit.

De actie start de BW-gebeurtenis die in het procestype wordt vermeld.

28.1.1.2 BW Publisher configureren

Met BW Publisher kunt u Crystal Reports-rapporten (.rpt-bestanden) afzonderlijk of in batches vanuit BW publiceren naar het BI-platform.

In Windows kunt u BW Publisher op een van de volgende twee manieren configureren:

- Start BW Publisher met een service op een computer waarop het BI-platform wordt gehost. De BW-publicatieservice start exemplaren van BW Publisher wanneer dat nodig is.
- Start BW Publisher met een lokale SAP-gateway als u BW Publisher-exemplaren wilt maken.

Wanneer u de voor- en nadelen van elke configuratie hebt overwogen, moet u een configuratiemethode selecteren op basis van de vereisten van de site. Zodra u BW Publisher hebt geconfigureerd in het BI-platform, moet u publicatie in Werkbank voor inhoudbeheer configureren.

28.1.1.3 BW Publisher als een service configureren

In dit gedeelte wordt uitgelegd hoe u met de volgende procedure de publicatie van rapporten vanuit BW naar het BI-platform met BW Publisher als een service kunt inschakelen.

28.1.1.3.1 De BW Publisher-installatie distribueren

In deze sectie wordt de distributie toegelicht van de BW Publisher-service en wordt uitgelegd hoe u BW Publisher kunt scheiden van andere BI-platformonderdelen.

U kunt de publicatietaken van BW verspreiden door BW Publisher-services te installeren op twee afzonderlijke computers in hetzelfde BI-platformsysteem.

Wanneer u BW Publisher op de computer met het BI-platform installeert, configureert u elke computer zo dat ze dezelfde programma-id en SAP Gateway-host en Gateway-service gebruiken. Wanneer u een RFC-doel hebt gemaakt die deze programma-id gebruikt, worden de publicatietaken door BW verdeeld over de computers waarop het BI-platform wordt gehost. En als één BW Publisher defect raakt, blijft BW gebruikmaken van de andere BW Publisher.

U kunt een extra niveau van systeemredundantie toevoegen aan elke configuratie met meer BW-toepassingsservers. Configureer elke BW-toepassingsserver zo dat deze als een SAP-gateway functioneert. Installeer voor elk exemplaar een aparte BW Publisher-service op een computer waarop het BI-platform wordt gehost. Configureer elke BW Publisher-service zo dat deze de gatewayhost en gatewayservice gebruikt van een afzonderlijke BW-toepassingsserver. In deze configuratie kan de publicatie vanuit BW doorgaan, ook als een BW Publisher of een toepassingsserver defect raakt.

Als u BW Publisher wilt scheiden van andere BI-platformonderdelen, installeert u BW met een zelfstandige SAP-gateway.

In dit geval moet u een lokale SAP-gateway installeren op dezelfde computer als BW Publisher. Daarnaast heeft BW Publisher toegang nodig tot de SDK van BI-platform en de Crystal Reports-afdrukengine. Als u de BW Publisher en de lokale SAP-gateway op een speciale computer installeert, moet u ook de SIA-server installeren.

28.1.1.3.2 BW Publisher starten: UNIX

Voer het BW Publisher-script uit om een of meerdere exemplaren van de publisher te maken om publicatieverzoeken af te handelen. Het wordt aanbevolen één exemplaar voor de publisher te starten.

Zodra BW Publisher wordt gestart, wordt er een verbinding tot stand gebracht met de SAP-gatewayservice die u hebt opgegeven toen u het installatieprogramma van BI-platform uitvoerde.

28.1.1.3.3 BW Publisher starten: Windows

Gebruik in Windows de Central Configuration Manager™ (CCM) om de BW Publisher-service te starten. Als u de BW Publisher-service start, wordt een exemplaar voor de publisher gemaakt voor publicatieverzoeken vanuit uw BW-systeem. Als het volume van publicatieverzoeken toeneemt, zorgt BW Publisher automatisch voor aanvullende publishers om aan de vraag te voldoen.

28.1.1.3.4 Doelen configureren voor de BW Publisher-service

Als u BW Publisher wilt inschakelen, moet u een RFC-doel configureren op uw BW-server voor communicatie met de BW Publisher-service. Als u een BW-cluster hebt, configureert u het RFC-doel op elke server en gebruikt u het centrale BW-exemplaar in elk geval als uw gatewayhost.

Als u meerdere BI-platformsystemen vanuit BW wilt publiceren, maakt u een apart RFC-doel voor de BW Publisher-service in elke BI-platformimplementatie. U moet unieke programma-id's voor elk doel gebruiken, maar dezelfde gatewayhost en gatewayservice.

28.1.1.3.5 BW Publisher configureren met een lokale SAP-gateway

> **Opmerking**
>
> Gebruik deze configuratie niet als het BI-platform onder UNIX is geïnstalleerd. Het gebruik van deze methode in UNIX kan resulteren in een onvoorspelbare werking van het systeem.

Voer de volgende procedure uit als u de publicatie van rapporten vanuit BW naar het BI-platform met een lokale SAP-gateway wilt inschakelen:

- Lokale SAP-gateways installeren [pagina 1018].
- Doelen configureren voor BW Publisher [pagina 1018].

28.1.1.3.6 Lokale SAP-gateways installeren

Er moet een lokale SAP-gateway zijn geïnstalleerd op de computer waarop u de BW Publisher hebt geïnstalleerd. Het wordt aanbevolen dat een SAP BASIS-beheerder de installatie van een van deze SAP-gateways uitvoert.

Raadpleeg voor bijgewerkte instructies voor het installeren van een lokale SAP-gateway de SAP-installatie-instructies die op de presentatie-cd van SAP te vinden zijn.

Zie voor een gedetailleerde lijst met geteste omgevingen de PAM (Product Availability Matrix) op http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540. De PAM bestand bevat specifieke versie- en Service Pack-vereisten voor toepassingsservers, besturingssystemen, SAP-onderdelen enzovoort.

Nadat u de SAP-gateway hebt geïnstalleerd, gebruikt u `regedit` om de registervermeldingen `TMP` en `TEMP` onder de subsleutel `HKEY_CURRENT_USER\Environment` te controleren. Beide registervermeldingen moeten dezelfde reekswaarde bevatten, die een geldig absoluut mappad moet zijn. Als een van de vermeldingswaarden de variabele `%USERPROFILE%` bevat, vervangt u deze door een absoluut mappad. Meestal worden beide registervermeldingen ingesteld op `C:\WINDOWS\TEMP`

28.1.1.4 Doelen configureren voor BW Publisher

Als u BW Publisher wilt inschakelen, moet u een RFC-doel configureren om BW de locatie te verschaffen van de computer waarop u de lokale SAP-gateway en BW Publisher hebt geïnstalleerd.

28.1.1.5 Publiceren configureren in Werkbank voor inhoudbeheer

In de Workbench voor contentbeheer kunt u rapportpublicatiefuncties beheren vanuit SAP BW. U kunt rollen van het SAP BW-systeem identificeren met bepaalde BI-platformsystemen, rapporten publiceren en rapporten synchroniseren tussen SAP BW en een BI-platformimplementatie. Zodra u een SAP-verificatie hebt ingesteld en BW Publisher hebt geconfigureerd, voert u de in deze sectie uitgelegde functies uit om publiceren in te schakelen. Met deze instructies kunt u het volgende doen:

- Juiste machtigingen instellen voor verschillende gebruikers van Werkbank voor inhoudbeheer.
- Verbindingen met BI-platform instellen waarin inhoud wordt gepubliceerd.
- Definiëren welke rollen naar elk BI-platform kunnen publiceren.
- Publiceer inhoud van BW naar het BI-platform.

28.1.1.6 Gebruikers die toegang kunnen krijgen tot de Werkbank voor inhoudbeheer

Er zijn drie typen gebruikers die toegang kunnen krijgen tot Werkbank voor inhoudbeheer:

- Inhoudgebruikers, die behoren tot de functies voor het bewaren van inhoud functies, en die functies kunnen weergeven. Ze mogen alleen rapporten weergeven.
- Inhoudpublishers van BI-platform, die rapporten vanuit BW kunnen weergeven, publiceren, wijzigen en (optioneel) verwijderen.
- Beheerders van BI-platform die alle taken in Werkbank voor inhoudbeheer kunnen uitvoeren. Deze taken omvatten het definiëren van BI-platformsystemen, het publiceren van rapporten en het uitvoeren van rapportonderhoud.

28.1.1.7 Functies in BW maken voor aangewezen inhoudpublishers

Als u BW configureert voor integratie met het BI-platform, bepaalt u of u met de huidige rolstructuur bepaalde BW-gebruikers snel kunt aanwijzen als inhoudpublishers of systeembeheerders voor de BI-platformsystemen.

Geef alle nieuwe functies die u maakt, een beschrijvende naam. Voorbeelden van beschrijvende functienamen zijn `BOE_INHOUDPUBLISHERS` en `SBOP_SYSTEEMBEHEERDERS`.

> → Tip
>
> U kunt aan een beheergebruiker volledige systeembeheerrechten of een subset van deze rechten toewijzen.

Als u de rechten wilt wijzigen die aan deze nieuwe functies (of aan een van uw bestaande functies) zijn verleend in het BI-platform, moet u eerst SAP-verificatie instellen en de functies importeren. Vervolgens kunt u de rechten van elke geïmporteerde functie wijzigen met behulp van de CCM (Central Management Console).

Raadpleeg de SAP-documentatie voor informatie over het maken van functies. Zie de volgende secties voor meer informatie over het gebruik van functies in het beheren van inhoud:

- SAP-rollen importeren [pagina 339].
- Mappen en beveiliging instellen in het BI-platform [pagina 1010].
- Standaardpatronen voor mappenbeveiliging [pagina 1011].

28.1.1.8 Toegang configureren tot Werkbank voor inhoudbeheer

Voor elk gebruikerstype dat toegang heeft tot de Werkbank voor inhoudbeheer, moet u de juiste reeks machtigingen toepassen binnen BW. De machtigingen worden in de volgende tabellen vermeld.

Machtigingen voor beheergebruikers

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
S_TCODE	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI

Machtigingsobject	Veld	Waarden
	ACTVT	Uitvoeren (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Wijzigen, Weergeven (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	Uitvoeren (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Nieuw maken, Wijzigen, Weergeven, Verwijderen (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Nieuw maken, Verwijderen (01, 06)
ZCNTADMRPT	ACTVT	Weergeven, Verwijderen, Activeren, Onderhouden, Controleren (03, 06, 07, 23, 39)

Machtigingen voor inhoudpublishers

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Uitvoeren (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	Uitvoeren (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Weergeven (03)
ZCNTADMJOB	ACTVT	(Nieuw, Verwijderen) 01, 06

Machtigingsobject	Veld	Waarden
ZCNTADMRPT	ACTVT	Weergeven, Activeren, Onderhouden, Controleren (03, 07, 23, 39) Verwijderen (optioneel) (06) Bewerken (optioneel) (02)

Het toekennen van het recht aan inhoudpublishers om rapporten te verwijderen in Werkbank voor inhoudbeheer voor BW is optioneel. Houd er echter rekening mee dat wanneer u een rapport verwijdert in BW, het rapport in het BI-platform ook wordt verwijderd. Als publishers niet voldoende rechten hebben om rapporten te verwijderen in het platform, verschijnt er een fout.

Machtigingen voor inhoudgebruikers

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	Uitvoeren (16)
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Uitvoeren (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Weergeven (03)

28.1.1.9 Een BI-platformsysteem definiëren

U moet een systeemdefinitie maken in Werkbank voor inhoudbeheer voor elk BI-platformsysteem waarnaar u rapporten wilt publiceren.

28.1.1.9.1 Een BI-platformsysteem toevoegen

1. Voer de transactie `/crystal/rptadmin` uit om toegang te krijgen tot Werkbank voor inhoudbeheer.
2. In het deelvenster *Bewerkingen* selecteert u *Enterprise-systeem*.
3. Dubbelklik op *Nieuw systeem toevoegen*.

4. Ga op het tabblad *Systeem* als volgt te werk:
   - Typ een beschrijvende naam in het veld *Alias*. Gebruik geen spaties of speciale tekens aangezien deze speciale behandeling behoeven wanneer de aliasnaam tijdens de configuratie van Enterprise Portals wordt gebruikt.
   - Typ de naam van de computer waarop de CMS wordt uitgevoerd. Als u de CMS hebt geconfigureerd om te luisteren naar een andere poort dan de standaardpoort, typt u **`CMSNAAM:POORT`**.
   - Selecteer *Standaardsysteem* als u rapporten naar dit systeem wilt publiceren vanuit een functie die niet expliciet is toegewezen aan een BI-platformsysteem. Er kan slechts één BI-platformsysteem als standaard worden gebruikt.
     In de lijst met beschikbare systemen wordt het standaardsysteem met een groen vinkje aangegeven.
5. Klik op *Opslaan*.
6. Voeg op het tabblad *RFC-doelen* elk RFC-doel toe dat aan dit systeem is gekoppeld.

   Klik op de knop *Rij invoegen* als u een doel wilt toevoegen. Dubbelklik in de lijst die verschijnt op de naam van het RFC-doel.

   > **Opmerking**
   >
   > Een BI-platformsysteem kan meerdere doelen hebben om systeemredundantie toe te voegen. Zie "De BW Publisher-installatie distribueren".

7. Schakel het selectievakje in naast de doelnaam die u hebt toegevoegd, en klik op *BOE-definitie verifiëren*.

   Met deze test wordt gecontroleerd of BW contact kan maken met de opgegeven BW Publisher en bij dit systeem kan aanmelden met de Crystal-machtigingsgebruikersaccount.
8. Ga op het tabblad *HTTP* als volgt te werk:
   - In het veld *Protocol* typt u **`http`** of **`https`**, als de webserver die is verbonden met het BI-platform, is geconfigureerd voor HTTPS.
   - Typ in het veld *Webserverhost en -poort* de volledig gekwalificeerde domeinnaam of het IP-adres van de webserver die als host fungeert voor BI-startpunt. Neem het poortnummer op voor een installatie waarvoor een Java-toepassingsserver wordt gebruikt. Typ bijvoorbeeld **`boserver01.businessobjects.com:8080`**.
   - Typ in het veld *Pad* de tekst **`SAP`**.
     Dit pad is in wezen het virtuele pad dat uw webserver gebruikt bij de verwijzing naar de submap `sap` met de webinhoud van uw BI-platform. Geef alleen een andere waarde op als u uw webomgeving en de locatie van de webinhoudbestanden van het platform hebt aangepast.
     Plaats geen schuine streep aan het begin of einde van deze vermelding.
   - Typ in het vak *Viewertoepassing* de naam van uw viewer.
     Typ **`openDocument.jsp`** als u de standaard BI-platformviewer wilt gebruiken die de Java-versie van BI-startpunt gebruikt.
     Als het BI-platform op Windows is geïnstalleerd met de standaardconfiguratie van `ASP.NET`, typt u **`report/report_view.aspx`** om de standaardbrowser te gebruiken.
9. Selecteer op het tabblad *Talen* de talen van rapporten die naar dit systeem worden gepubliceerd.
10. Voeg op het tabblad *Rollen* de rollen voor het bewaren van inhoud toe die u aan dit BI-platformsysteem wilt koppelen.

    Zie "SAP-rollen importeren".
11. Klik op de knop *Rij invoegen*.

    Er wordt een lijst weergegeven met functies die aan dit systeem kunnen worden toegevoegd.

> **Opmerking**
>
> Elke functie kan slechts naar één BI-platformsysteem worden gepubliceerd. Als de rollen die u aan dit BI-platformsysteem wilt toevoegen, niet in de lijst worden weergegeven, klikt u op *Annuleren* om naar het tabblad *Rollen* terug te keren en klikt u vervolgens op *Rollen opn. toewijzen*.

12. Selecteer de rollen die u naar dit systeem wilt publiceren en klik op *OK*.
13. Selecteer op het tabblad *Indeling* de standaardbeveiligingsinstellingen voor rapport- en rolmappen die naar dit BI-platformsysteem zijn gepubliceerd.

> **Opmerking**
>
> In het BI-platform wordt automatisch een map gemaakt voor elke functie die naar dat systeem is gepubliceerd. Deze map bevat snelkoppelingen naar de rapporten die met die rol zijn gepubliceerd.

> **Opmerking**
>
> Zodra u een BI-platformsysteem hebt geconfigureerd, heeft wijziging van de standaardbeveiligingsniveaus hier geen effect op de beveiligingsniveaus van gepubliceerde functiemappen of rapporten. Als u de standaardbeveiligingsniveaus wilt wijzigen voor alle functies en inhoud die naar het platform zijn gepubliceerd, verwijdert u de functiemappen en snelkoppelingen in het systeem (Hierdoor worden de werkelijke rapporten niet verwijderd.) Wijzig hier de beveiligingsinstellingen en publiceer de rollen en rapporten opnieuw.

14. Klik op *OK* onderaan om uw instellingen op te slaan en maak het BI-platformsysteem in Werkbank voor inhoudbeheer.

U kunt nu vanuit BW rapporten publiceren naar het BI-platform.

Verwante informatie

De BW Publisher-installatie distribueren [pagina 1016]
SAP-rollen importeren [pagina 339]

28.1.1.10 Rapporten publiceren met Werkbank voor inhoudbeheer

Nadat een rapport voor BW is opgeslagen, kunt u het publiceren met Werkbank voor inhoudbeheer. U kunt met Werkbank voor inhoudbeheer afzonderlijke rapporten publiceren of alle rapporten die voor een bepaalde functie zijn opgeslagen. Alleen een gebruiker die de machtigingen van een Crystal-inhoudpublisher heeft (zie Machtigingen maken en toepassen [pagina 1039]), kan rapporten met de Werkbank voor inhoudbeheer publiceren en onderhouden.

28.1.1.11 Functies of rapporten publiceren

1. Voer de transactie `/crystal/rptadmin` uit om toegang te krijgen tot Werkbank voor inhoudbeheer.
2. In het deelvenster *Bewerkingen* selecteert u *Rapporten publiceren*.
3. Dubbelklik op *Rapporten en functies selecteren die moeten worden gepubliceerd* om inhoud te vinden die is opgeslagen in uw BW-systeem.
   Er verschijnt een dialoogvenster waarin u de beschikbare functies en rapporten kunt filteren.
4. Selecteer in de lijst Systeem het systeem of de systemen met inhoud die u wilt weergeven.

   > **Opmerking**
   >
   > De lijst bevat alle beschikbare systemen die zijn gedefinieerd op het BW-systeem.

5. Filter uw resultaten vervolgens om het aantal rapporten en functies te beperken dat wordt weergegeven. Gebruik de volgende opties:
   - *Objectversie*
     Als A: active wordt geselecteerd, worden alle rapporten weergegeven die kunnen worden gepubliceerd. Als de lege optie wordt geselecteerd, worden alle rapporten weergegeven. (De overige opties zijn voor SAP gereserveerde termen.)
   - *Objectstatus*
     Selecteer ACT actief, uitvoerbaar om alleen gepubliceerde rapporten weer te geven. Selecteer INA inactief, niet uitvoerbaar om alleen niet-gepubliceerde rapporten weer te geven. Laat het veld leeg om alle rapporten weer te geven. (De overige opties zijn voor SAP gereserveerde termen.)
   - *Functiefilter*
     Als u tekst in dit vak typt, worden alleen de functies weergegeven die overeenkomen met de tekst die u hier typt. Gebruik * als jokerteken. Typ bijvoorbeeld 'd*' om alle functies weer te geven die beginnen met de letter d.
   - *Rapportbeschrijving*
     Als u tekst in dit vak typt, worden alleen de rapporten weergegeven waarvan de beschrijvingen overeenkomen met de tekst die u hier typt. Gebruik * als jokerteken voor overeenkomsten met een willekeurig aantal tekens. Gebruik + als jokerteken voor overeenkomsten met 0 of 1teken. Als u bijvoorbeeld alle rapporten wilt weergeven waarvan de beschrijving het woord omzet bevat, typt u *omzet*.
6. Klik op *OK*.
   De lijst met rapporten die voldoen aan uw criteria wordt in het venster aan de rechterzijde weergegeven. De rapporten worden in een hiërarchie gerangschikt: BI-platformsysteem > Functies op dat systeem > Rapporten die zijn opgeslagen voor de functie.
   Elk item in de hiërarchie bevat een rode, gele of groene stip. Items die zich hoger in de hiërarchie bevinden, geven de status weer van de items die ze bevatten, waarbij de minst gunstige voorwaarde boven in de hiërarchie wordt gefilterd. Als één rapport in een functie bijvoorbeeld geel is (actief), maar alle andere rapporten groen zijn (gepubliceerd), wordt de functie geel weergegeven (actief).
   - Groen: het item is volledig gepubliceerd. Als het item een BI-platformsysteem of een functie is, zijn alle rapporten in dat item gepubliceerd.
   - Geel: het item is actief maar niet gepubliceerd. Als het item een rapport is, is het item beschikbaar voor publicatie. Als het item een functie of BI-platformsysteem is, is alle inhoud actief en is minstens één item in de functie of in het systeem niet gepubliceerd.

- Rood: het item is SAP-inhoud en is niet beschikbaar voor publicatie met de Werkbank voor inhoudbeheer. Inhoud is pas beschikbaar voor publicatie als deze is geactiveerd met de BW-werkbank voor inhoudbeheer.

7. Selecteer de rapporten die u wilt publiceren.
   Als u alle rapporten in een functie wilt publiceren, selecteert u de functie. Selecteer het systeem als u alle functies op een BI-platformsysteem wilt publiceren.

   > ⓘ Opmerking
   >
   > Als u een functie (of een systeem) selecteert, worden alle rapporten in die functie (of dat systeem) geselecteerd. Als u deze selectie wilt wissen, wist u het selectievakje voor de functie (of het systeem) en klikt u op Vernieuwen.

8. Klik op *Publiceren*.

   > ⓘ Opmerking
   >
   > Rapporten die op de achtergrond zijn gepubliceerd, worden verwerkt als systeembronnen beschikbaar worden. Klik op *Op achtergrond* in plaats van op *Publiceren* als u deze optie wilt gebruiken.

9. Klik op *Vernieuwen* als u de weergave van de status van BI-platformsystemen, functies en rapporten in Werkbank voor inhoudbeheer wilt bijwerken.

   > → Tip
   >
   > Klik met de rechtermuisknop op het rapport en selecteer *Weergeven* als u een rapport wilt weergeven. Klik met de rechtermuisknop op het rapport en selecteer *Gebruikte query's* om te zien welke query's door het rapport worden gebruikt.

   > ⓘ Opmerking
   >
   > Nadat u een rapport hebt gepubliceerd naar het BI-platform, klikt u op *Overschrijven* als u het gepubliceerde rapport wilt overschrijven.

Verwante informatie

Achtergrondpublicaties plannen [pagina 1025]

28.1.1.12 Achtergrondpublicaties plannen

Als u rapporten op de achtergrond publiceert, ofwel direct ofwel als een geplande taak, bespaart u systeembronnen. Het wordt aanbevolen dat u rapporten op de achtergrond publiceert om het reactievermogen van het systeem te verbeteren.

Als u rapporten periodiek publiceert als geplande taken, worden de rapportgegevens tussen BW en uw BI-platformimplementatie gesynchroniseerd. Het wordt aanbevolen alle rapporten (of functies die deze rapporten bevatten) te plannen. U kunt functies en rapporten ook handmatig synchroniseren met de statusoptie

Bijwerken van de bewerking Rapportonderhoud. Zie Rapportstatus bijwerken [pagina 1026] voor meer informatie.

28.1.1.13 Systeemgegevens bijwerken voor gepubliceerde rapporten

BW Publisher gebruikt de hier ingevoerde SAP-systeemgegevens om de gegevensbron van gepubliceerde rapporten bij te werken. U kunt kiezen voor de lokale BW-toepassingsserver of het centrale BW-exemplaar als u de voorkeur geeft aan een configuratie met taakverdeling.

28.1.1.14 Rapporten onderhouden

Het onderhoud van rapporten bestaat uit het synchroniseren van gegevens over rapporten tussen het BI-platform en BW (Status bijwerken), het verwijderen van ongewenste rapporten (Rapporten verwijderen), en het bijwerken van rapporten die zijn gemigreerd uit oudere versies van het platform (Postmigratie).

28.1.1.14.1 Rapportstatus bijwerken

Als u een wijziging in een gepubliceerd rapport aanbrengt in een BI-platformsysteem (zoals het wijzigen van de functie waarnaar een rapport wordt gepubliceerd), wordt deze wijziging pas in BW weergegeven als u het BI-platform en BW synchroniseert. U kunt een publicatietaak zo plannen dat het BI-platform en BW periodiek worden gesynchroniseerd (zie Achtergrondpublicaties plannen [pagina 1025]). U kunt de status van het rapport ook bijwerken met het hulpprogramma Rapportonderhoud.

28.1.1.14.2 Rapporten verwijderen

Als u een gepubliceerd rapport uit BW verwijdert met Werkbank voor inhoudbeheer, wordt het rapport ook verwijderd uit het BI-platform. Alleen gebruikers aan wie de machtigingen zijn toegekend om rapporten te verwijderen in zowel het BW- als het BI-platformsysteem, kunnen rapporten verwijderen.

> ⓘ Opmerking
>
> Als een gebruiker rechten heeft om een rapport in BW te verwijderen, maar niet in het BI-platformsysteem waar dat rapport is gepubliceerd, kan een fout optreden.

28.1.1.15 Http-verzoekhandler van SAP configureren

Als u de weergave van rapporten in BW wilt inschakelen, moet u BW configureren voor gebruik van de http-verzoekhandler die wordt meegeleverd als onderdeel van het Werkbank voor inhoudbeheer. Wanneer een

BW-gebruiker vervolgens een Crystal Reports-rapport opent in de SAPGUI, kan BW het weergaveverzoek via het web op de juiste wijze doorsturen.

Gebruik de transactie SICF om toegang te krijgen tot de lijst met virtuele hosts en services die in uw BW-systeem actief zijn. Maak een nieuw knooppunt met de naam `ce_url` onder BW in de hiërarchie `default_host` en voeg `/CRYSTAL/CL_BW_HTTP_HANDLER` aan de handlerlijst toe. Mogelijk moet u deze service handmatig activeren nadat deze is gemaakt.

28.1.1.16 Configuratie voor verwerking van SAP-gegevens

28.1.1.16.1 Geplande rapporten verwerken in de batchmodus van SAP

Als u met Windows werkt, kunt u geplande rapporten op het BI-platform uitvoeren met de batchmodus van SAP. Met de InfoSet- en Open SQL-stuurprogramma's kunnen rapporten worden uitgevoerd in de batchmodus of de achtergrondmodus van SAP wanneer specifieke omgevingsvariabelen zijn ingesteld op 1. De relevante omgevingsvariabelen zijn:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (voor het InfoSet-stuurprogramma)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (voor het Open SQL-stuurprogramma)

Het wordt echter aanbevolen deze functie alleen te gebruiken als u een gedistribueerde installatie van het BI-platform hebt. Als deze omgevingsvariabelen zijn ingesteld op 1, worden met de stuurprogramma's rapporten uitgevoerd in de batchmodus van SAP, ongeacht het rapportageonderdeel dat het rapport werkelijk uitvoert. Als u deze omgevingsvariabelen als systeemomgevingsvariabelen aanmaakt op een computer die een combinatie van BI-platformservers gebruikt, voeren de stuurprogramma's alle rapporten in batchmodus uit (inclusief rapportverzoeken op aanvraag van de Crystal Reports-verwerkingsserver en de Report Application Server).

Teneinde ervoor te zorgen dat stuurprogramma's alleen uw geplande rapporten in de batchmodus uitvoeren (rapporten die worden uitgevoerd door Adaptive Job Server) moet u geen systeemomgevingsvariabelen instellen op computers die combinaties van BI-platformservers uitvoeren. Voer in plaats daarvan de volgende stappen uit om de omgevingsvariabelen aan te passen voor elke Adaptive Job Server.

> **Opmerking**
>
> SAP-gebruikers die rapporten in het BI-platform plannen, hebben mogelijk aanvullende machtigingen in SAP nodig.

Verwante informatie

Rapporten plannen in de batchmodus met een Open SQL-query [pagina 1054]

28.1.1.16.2 Geplande rapporten verwerken in de batchmodus van SAP

1. Maak een batchscript (`.bat`-bestand) in een teksteditor, zoals Kladblok, met de volgende inhoud:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   Met dit script worden de omgevingsvariabelen ingesteld op 1 en worden alle parameters uitgevoerd die aan het script zijn doorgegeven vanaf de opdrachtregel.
2. Sla het bestand als `jobserver_batchmode.bat` op in een map op elke Adaptive Job Server-computer.
3. Meld u aan bij de CMC (Central Management Console).
4. Kies *Servers*.
5. Vouw het knooppunt *Servicecategorieën* uit en kies *Analysis-services*.
6. Selecteer *Adaptive Processing Server* en kies *Eigenschappen* in het snelmenu.
   De pagina *Eigenschappen* wordt geopend.
7. Zoek op de pagina *Eigenschappen* het veld *Opdrachtregelparameters*.

   Dit is de opstartopdracht voor de Adaptive Job Server. Bijvoorbeeld:

   ```
   "\\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. Laat de standaardopdracht voorafgaan door het volledige pad naar het bestand `jobserver_batchmode.bat` dat u hebt opgeslagen op de Adaptive Job Server-computer.

   In dit voorbeeld wordt het batchbestand op een computer met de naam SERVER01 opgeslagen als:

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```

   De nieuwe opstartopdracht voor de Adaptive Job Server is:

   ```
   "\\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
   ```

   Met deze nieuwe opstartopdracht wordt eerst het batchbestand gestart. Het batchbestand stelt vervolgens de vereiste omgevingsvariabelen in voordat de oorspronkelijke opstartopdracht voor Adaptive Job Server wordt uitgevoerd. Hierdoor zijn de voor Adaptive Job Server beschikbare omgevingsvariabelen anders dan de omgevingsvariabelen die beschikbaar zijn voor servers die gebruikt worden voor rapportage op aanvraag (de Crystal Reports Processing Server en de Report Application Server).
9. Klik op *Opslaan en sluiten*.
10. Klik met de rechtermuisknop op de Adaptive Job Server en selecteer *Start* in het snelmenu.

> **Opmerking**
>
> Als de Adaptive Job Server niet kan worden gestart, controleert u de nieuwe opstartopdracht.

28.1.1.17 Configuraties voor SAP-transport

28.1.1.17.1 Overzicht

Het BI-platform bevat de volgende transporten:

- Transport Open SQL-connectiviteit
- Transport InfoSet-connectiviteit
- Transport Beveiligingsdefinitie op rijniveau
- Transport Clusters definiëren
- Transport Werkbank voor inhoudbeheer
- Transport Aangepaste parameters voor BW-query's
- MDX-transport
- ODS-transport

Er zijn twee verschillende transportsets: Unicode-compatibele transporten en ANSI-transporten. Als u met een BASIS-systeem versie 6.20 of later werkt, gebruikt u het Unicode- compatibele transport. Als u met een BASIS systeem werkt dat ouder is dan 6.20 gebruikt u de ANSI-transporten. De geïnstalleerde transporten bevinden zich in de volgende map op de distributiemedia van uw product: `\Collaterals\Add-Ons\SAP\Transports\`.

> **Opmerking**
>
> Wanneer u op installatieconflicten controleert, moet u nagaan of de objectnamen nog niet in uw SAP-systeem voorkomen. Objecten gebruiken standaard een **`/crystal/`**-naamruimte, zodat u deze naamruimte niet zelf hoeft te maken. Als u de **`/crystal/`**-naamruimte handmatig maakt, wordt u gevraagd om licentiereparatiesleutels waartoe u geen toegang hebt.

28.1.1.17.2 Transporten configureren

Als u Gegevenstoegang of de BW Publisher-onderdelen van het BI-platform wilt instellen, moet u de juiste transportbestanden in uw SAP-systeem importeren. Deze onderdelen gebruiken de inhoud van deze transportbestanden bij de communicatie met het SAP-systeem.

De installatie- en configuratieprocedures die voor het SAP-systeem zijn vereist, moeten door een BASIS-deskundige worden uitgevoerd die bekend is met het Change and Transport-systeem en die beheerdersrechten voor het SAP-systeem heeft. Welke procedure exact moet worden gebruikt voor het importeren van transportbestanden, is afhankelijk van de BASIS-versie die u gebruikt. Raadpleeg de SAP-documentatie voor specifieke proceduredetails.

Als u het onderdeel Gegevenstoegang voor de eerste keer implementeert, kunnen alle gebruikers standaard toegang krijgen tot al uw SAP-tabellen. Met de Beveiligingsdefinitie-editor beveiligt u de SAP-gegevens waartoe gebruikers toegang hebben.

Nadat u transporten hebt geïmporteerd, moet u de juiste niveaus van gebruikerstoegang configureren. Maak de vereiste machtigingen en pas deze via profielen of functies op SAP-gebruikers toe die Crystal Reports-rapporten ontwerpen, uitvoeren of plannen.

Verwante informatie

Machtigingen maken en toepassen [pagina 1039]

28.1.1.17.2.1 Typen transporten

Er zijn twee verschillende transportsets: Unicode-compatibele transporten en ANSI-transporten. Als u met een BASIS-systeem versie 6.20 of later werkt, gebruikt u het Unicode- compatibele transport. Als u met een BASIS systeem werkt dat ouder is dan 6.20 gebruikt u de ANSI-transporten. De geïnstalleerde transporten bevinden zich in de volgende map op de distributie van uw product: `\Collaterals\Add-Ons\SAP\Transports\`. Het bestand `transports.txt` geeft een overzicht van de met de Unicode compatibele en ANSI-transportbestanden.

Transporttypen worden hieronder weergegeven:

- Open SQL Connectivity-transport
  Met het transport Open SQL-connectiviteit kan het Open SQL-stuurprogramma verbinding maken met en rapporten maken op basis van het SAP-systeem.
- Transport Beveiligingsdefinitie op rijniveau
  Dit transport bevat de beveiligingsdefinitie-editor, een hulpprogramma dat dienst doet als grafische interface voor de /crystal/auth-tabellen in het Open SQL Connectivity-transport.
- Transport Clusters definiëren
  Dit transport verschaft het hulpprogramma Clusters definiëren. Met dit hulpprogramma kunt u een metagegevensbibliotheek opbouwen voor ABAP-gegevensclusterdefinities. Deze definities verschaffen het Open SQL-stuurprogramma de gegevens die het nodig heeft om uit deze gegevensclusters te rapporteren.

  > **Opmerking**
  >
  > ABAP-gegevensclusters zijn niet hetzelfde als clustertabellen. Clustertabellen zijn al gedefinieerd in de DDIC.

- InfoSet Connectivity-transport
  Dankzij het InfoSet Connectivity-transport heeft het InfoSet-stuurprogramma toegang tot InfoSets en SAP-query's.
- Transport Werkbank voor inhoudbeheer
  Dit transport verschaft BW-systemen de functionaliteit van inhoudbeheer. Dit transport is alleen beschikbaar als een UNICODE-compatibel transport.
- Transport Aangepaste parameters voor BW-query's
  Dit transport biedt ondersteuning voor aangepaste parameterwaarden en standaardparameterwaarden in rapporten op basis van BW-query's.
- Transport BW MDX-connectiviteit
  Via dit transport heeft het MDX-querystuurprogramma toegang tot BW-kubussen en -query's. Dit transport is compatibel met BW 3.0B patch 27 of hoger en met BW 3.1C patch 21 of hoger.
- Transport ODS-connectiviteit
  Via dit transport heeft het ODS-querystuurprogramma toegang tot ODS-gegevens. Dit transport is compatibel met BW 3.0B patch 27 of hoger en met BW 3.1C patch 21 of hoger.

28.1.1.17.2.2 Controleren op conflicten

De inhoud van de transportbestanden wordt automatisch onder de SAP BusinessObjects-naamruimte geregistreerd wanneer u de bestanden importeert. De SAP BusinessObjects-naamruimte is hiervoor gereserveerd in recente versies van R/3 en MYSAP ERP. Het kan echter voorkomen dat bepaalde objecten, zoals verificatieobjecten, verificatieklassen en verouderde objecten niet de juiste prefix hebben. Het is raadzaam deze objecttypen te controleren op conflicten voordat u de transportbestanden importeert.

Als de functiegroep, een van de functiemodules of een van de andere objecten al in het SAP-systeem bestaat, moet u de naamruimte herleiden voordat SAP BusinessObjects-transportbestanden worden geïmporteerd. Raadpleeg de documentatie van technologieplatform SAP NetWeaver voor de procedures die uw versie van SAP betreffen.

28.1.1.17.2.3 Transportbestanden importeren

Lees het bestand `transports_NL.txt` in de volgende map op de distributiemedia van uw product: `\Collaterals\Add-Ons\SAP\Transports\`. In dit tekstbestand wordt een overzicht gegeven van de exacte namen van de bestanden waaruit elk transport bestaat. (De mappen `cofiles` en `data` onder de map `transports` horen bij de mappen .../`trans/cofiles` en .../`trans/data` op uw SAP-server.)

U moet het transport Open SQL-connectiviteit importeren voordat het transport Beveiligingsdefinitie op rijniveau of het transport Clusters definiëren wordt geïmporteerd. U kunt de andere transporten in elke willekeurige volgorde importeren.

> **Opmerking**
>
> Controleer nadat bestanden van cd naar server zijn gekopieerd of naar alle bestanden kan worden geschreven voordat u de transporten importeert. Het importeren mislukt als de importbestanden het kenmerk Alleen-lezen hebben.

> **Opmerking**
>
> Omdat de transportbestanden binair zijn, moet u de bestanden bij UNIX-installaties via FTP in binaire modus toevoegen (om beschadiging van bestanden te voorkomen). Bovendien moet u schrijfmachtigingen voor de UNIX-server hebben.

28.1.1.17.2.4 Transport

28.1.1.17.2.4.1 Transport Open SQL-connectiviteit

Met het transport Open SQL-connectiviteit kunnen de stuurprogramma's verbinding maken met en rapporten maken op basis van het SAP-systeem.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/OPENSQL	Functiegroep	Open SQL-functies
/CRYSTAL/OSQL_AUTH_FORMS	Programma	Helper-programma
/CRYSTAL/OSQL_EXECUTE	Programma	Helper-programma
/CRYSTAL/OSQL_TYPEPOOLPROG	Programma	Helper-programma
/CRYSTAL/OSQL_TYPEPOOLS	Programma	Helper-programma
/CRYSTAL/OSQL_UTILS	Programma	Helper-programma
ZSSI	Verificatieobjectklasse	Rapportagemachtigingsobjecten
ZSEGREPORT	Machtigingsobject	Rapportagemachtigingsobject
/CRYSTAL/OSQL_CLU_ACTKEY_EN-TRY	Tabel	Metagegevens cluster
/CRYSTAL/OSQL_FCN_PARAM	Tabel	Metagegevens functie
/CRYSTAL/OSQL_FCN_PARAM_FIELD	Tabel	Metagegevens functie
/CRYSTAL/OSQL_FIELD_ENTRY	Tabel	Metagegevens tabel
/CRYSTAL/OSQL_OBJECT_ENTRY	Tabel	Metagegevens tabel
/CRYSTAL/OSQL_RLS_CHK_ENTRY	Tabel	Metagegevens RLS
/CRYSTAL/OSQL_RLS_FCN_ENTRY	Tabel	Metagegevens RLS
/CRYSTAL/OSQL_RLS_VAL_ENTRY	Tabel	Metagegevens RLS
ZCLUSTDATA	Tabel	Metagegevens cluster
ZCLUSTID	Tabel	Metagegevens cluster
ZCLUSTKEY	Tabel	Metagegevens cluster
ZCLUSTKEY2	Tabel	Metagegevens cluster
/CRYSTAL/AUTHCHK	Tabel	Metagegevens RLS
/CRYSTAL/AUTHFCN	Tabel	Metagegevens RLS
/CRYSTAL/AUTHKEY	Tabel	Metagegevens RLS
/CRYSTAL/AUTHOBJ	Tabel	Metagegevens RLS

Object	Type	Beschrijving
/CRYSTAL/AUTHREF	Tabel	Metagegevens RLS
ZSSAUTHCHK	Tabel	Metagegevens oude RLS
ZSSAUTHOBJ	Tabel	Metagegevens oude RLS
ZSSAUTHKEY	Tabel	Metagegevens oude RLS
ZSSAUTHREF	Tabel	Metagegevens oude RLS
ZSSAUTH FCN	Tabel	Metagegevens oude RLS

28.1.1.17.2.4.2 Transport InfoSet-connectiviteit

Dankzij het transport InfoSet-connectiviteit heeft het InfoSet-stuurprogramma toegang tot InfoSets. Dit transport is compatibel met R/3 4.6c en hoger. Importeer dit transport niet als u werkt met SAP R/3 4.6a of ouder.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/FLAT	Functiegroep	InfoSet wrapper-functies
/CRYSTAL/QUERY_BATCH	Programma	Uitvoering in batchmodus
/CRYSTAL/QUERY_BATCH_STREAM	Programma	Uitvoering in streaming batchmodus

28.1.1.17.2.4.3 Transport Beveiligingsdefinitie op rijniveau

Dit transport bevat de beveiligingsdefinitie-editor, een hulpprogramma dat dienst doet als een grafische interface voor de /CRYSTAL/AUTH-tabellen in het Open SQL Connectivity-transport.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/TABMNT	Functiegroep	Functiegroep voor de weergave van tabelonderhoud voor functiebeperkingen
/CRYSTAL/RLSDEF	Programma	Hoofdprogramma

Object	Type	Beschrijving
/CRYSTAL/RLS_INCLUDE1	Programma	Include-programma met moduledefinities
/CRYSTAL/RLS_INCLUDE2	Programma	Include-programma met de subroutinedefinities
TDDAT [/CRYSTAL/AUTHFCN]	Tabelinhoud	Definitie van tabelonderhoud
TVDIR [/CRYSTAL/AUTHFCN]	Tabelinhoud	Definitie van tabelonderhoud
/CRYSTAL/AUTHFCNS	Definitie van transport- en onderhoudsobject	Definitie van tabelonderhoud
/CRYSTAL/RLS	Transactie	Hoofdprogrammatransactie
/CRYSTAL/RLSFCN	Transactie	Helper-transactie die intern door hoofdprogramma wordt aangeroepen.

28.1.1.17.2.4.4 Transport Clusters definiëren

Dit transport verschaft het hulpprogramma Clusters definiëren. Met dit hulpprogramma kunt u een metagegevensbibliotheek opbouwen voor ABAP-gegevensclusterdefinities. Deze definities verschaffen het Open SQL-stuurprogramma de gegevens die het nodig heeft om uit deze gegevensclusters te rapporteren.

> ⓘ Opmerking
>
> ABAP-gegevensclusters zijn niet hetzelfde als clustertabellen. Clustertabellen zijn al gedefinieerd in de DDIC.

Object	Type	Beschrijving
ZCIMPRBG	Programma	Hoofdprogramma
ZCRBGTOP	Programma	Include-programma
ZCDD	Transactie	Hoofdprogrammatransactie

28.1.1.17.2.4.5 Transport Werkbank voor inhoudbeheer

Dit transport verschaft BW-systemen de functionaliteit van inhoudbeheer. Het is alleen beschikbaar als een met Unicode compatibel transport.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/CL_BW_HTTP_HANDLER	Klasse	Multi-CE HTTP-verzoekhandler
/CRYSTAL/OBJECT_STATUS_DOM	domein	Rapportactiviteit
/CRYSTAL/OBJ_POLICY_DOM	domein	CE-objectbeveiliging
/CRYSTAL/OBJECT_STATUS	Gegevenselement	Rapportactiviteit
/CRYSTAL/OBJ_POLICY	Gegevenselement	CE-objectbeveiliging
/CRYSTAL/CE_SYNCH	Functiegroep	Publisher stubs
/CRYSTAL/CA_MSG	Berichtklasse	Statusberichten
/CRYSTAL/CE_SYNCH_FORMS	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_AD-MIN_CLASS_D	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_AD-MIN_CLASS_I	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_CTREE	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_FORMS	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_MODU-LES	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_PAIS	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_PBOS	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_AD-MIN_TAB_FRM	Programma	Programmaonderdeel
/CRYSTAL/CONTENT_ADMIN_TOP	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WORKER	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WORKER_DISP	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WORKER_DISP_I	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WOR-KER_FORMS	Programma	Programmaonderdeel

Object	Type	Beschrijving
/CRYSTAL/PUBLISH_WORKER_PROC	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WOR-KER_PROC_I	Programma	Programmaonderdeel
/CRYSTAL/PUBLISH_WOR-KER_SCREEN	Programma	Programmaonderdeel
/CRYSTAL/CA_DEST	Tabel	Toepassingsstatus
/CRYSTAL/CA_JOB	Tabel	Toepassingsstatus
/CRYSTAL/CA_JOB2	Tabel	Toepassingsstatus
/CRYSTAL/CA_LANG	Tabel	Toepassingsstatus
/CRYSTAL/CA_PARM	Tabel	Toepassingsstatus
/CRYSTAL/CA_ROLE	Tabel	Toepassingsstatus
/CRYSTAL/CA_SYST	Tabel	Toepassingsstatus
/CRYSTAL/MENU_TREE_ITEMS	Structuur	Toepassingsstatus
/CRYSTAL/REPORT_ID	Tabel	Toepassingsstatus
/CRYSTAL/RPTADMIN	Transactie	Hoofdprogrammatransactie
/CRYSTAL/EDIT_REPORT	Programma	Wrapper voor rapportbewerking
/CRYSTAL/EDIT_REPORT	Functiegroep	Functies voor rapportbewerking
ZSSI	Verificatieobjectklasse	Crystal-verificaties
ZCNTADMCES	Machtigingsobject	CE-bewerkingen
ZCNTADMRPT	Machtigingsobject	Rapportbewerkingen
ZCNTADMJOB	Machtigingsobject	Achtergrondtaakbewerkingen

28.1.1.17.2.4.6 Transport ODS-connectiviteit

Via dit transport heeft het ODS-querystuurprogramma toegang tot ODS-gegevens. Dit transport is compatibel met BW 3.0B patch 27 of hoger en met BW 3.1C patch 21 of hoger.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/ODS_REPORT	Functiegroep	ODS-functies

28.1.1.17.2.4.7 Transport Aangepaste parameters voor BW-query's

Dit transport biedt ondersteuning voor aangepaste parameterwaarden en standaardparameterwaarden in rapporten op basis van BW-query's.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/PERS_VAR	Structuur	Variabeledefinitie
/CRYSTAL/PERS_VALUE	Structuur	Waardedefinitie
/CRYSTAL/PERS	Functiegroep	Aanpassingsfuncties

28.1.1.17.2.4.8 Transport BW MDX-connectiviteit

Via dit transport heeft het MDX-querystuurprogramma toegang tot BW-kubussen en -query's. Dit transport is compatibel met BW 3.0B patch 27 of hoger en met BW 3.1C patch 21 of hoger.

Object	Type	Beschrijving
/CRYSTAL/BC	Pakket	Ontwikkelingsklasse
/CRYSTAL/MDX	Functiegroep	MDX-functies
/CRYSTAL/MDX_STREAM_LAYOUT	Tabeldefinitie	Structuur gegevensset
/CRYSTAL/CX_BAPI_ERROR	Klasse	Uitzondering
/CRYSTAL/CX_METADATA_ERROR	Klasse	Uitzondering
/CRYSTAL/CX_MISSING_STREA-MINFO	Klasse	Uitzondering
/CRYSTAL/CX_NO_MORE_CELLS	Klasse	Uitzondering

Object	Type	Beschrijving
/CRYSTAL/CX_NO_MORE_MEMBERS	Klasse	Uitzondering
/CRYSTAL/CX_NO_MORE_PROPER-TIES	Klasse	Uitzondering
/CRYSTAL/CX_SAVE_SESSION_STATE	Klasse	Uitzondering
/CRYSTAL/MDX_APPEND_DATA	Klasse	Processor gegevensset
/CRYSTAL/MDX_READER_BASE	Klasse	Processor gegevensset
/CRYSTAL/MDX_READ_DIMENSIONS	Klasse	Processor gegevensset
/CRYSTAL/MDX_READ_MEASURES	Klasse	Processor gegevensset
/CRYSTAL/MDX_READ_PROPERTIES	Klasse	Processor gegevensset
/CRYSTAL/MDX_AXIS_LEVELS	Tabeltype	Structuur metagegevens
/CRYSTAL/MDX_PROPERTY_KEYS	Tabeltype	Structuur metagegevens
/CRYSTAL/MDX_PROPERTY_VALUES	Tabeltype	Structuur metagegevens
/CRYSTAL/MDX_STREAM_LAY-OUT_TAB	Tabeltype	Structuur metagegevens

28.1.1.18 Overzicht van machtigingen

Deze sectie bevat een lijst met SAP-machtigingen die op basis van ervaring en tests vereist blijken te zijn bij het uitvoeren van algemene taken met BI-platform in een geïntegreerde SAP-omgeving. Afhankelijk van uw afzonderlijke implementatie kunnen machtigingsobjecten of -velden vereist zijn.

Van elk machtigingsobject moet u een machtiging maken en de juiste veldwaarden definiëren. Vervolgens past u de juiste machtigingen toe op de profielen (of functies) van uw SAP-gebruikers. In de volgende secties worden de vereiste machtigingen beschreven en vindt u de benodigde veldwaarden. Raadpleeg de SAP-documentatie voor proceduregegevens die specifiek voor uw versie van SAP gelden.

> **Opmerking**
>
> De informatie in deze sectie dient uitsluitend als een richtlijn.

> **Opmerking**
>
> Het machtigingsobject ZSEGREPORT behoort tot de objectklasse ZSSI die wordt geïnstalleerd als u de transportbestanden van SAP Integration importeert die nodig zijn voor ondersteuning van Open SQL-query's.

28.1.1.18.1 Machtigingen maken en toepassen

Met behulp van Desktop Intelligence Integration voor SAP moet u de machtigingen maken en toepassen die iedere gebruiker nodig heeft om toegang te krijgen tot gegevens. De exacte procedures voor het maken, configureren en toepassen van machtigingen zijn afhankelijk van de SAP-versie die u hebt geïnstalleerd. Deze sectie bevat een lijst met SAP-machtigingen die op basis van ervaring en tests vereist blijken te zijn bij het uitvoeren van algemene taken met het BI-platform geïntegreerd in een SAP Netweaver ABAP-omgeving. Afhankelijk van uw afzonderlijke implementatie kunnen machtigingsobjecten of -velden vereist zijn.

Verwante informatie

Publiceren configureren in Werkbank voor inhoudbeheer [pagina 1018]

28.1.1.19 Acties in BW

In deze sectie wordt u door een lijst met verschillende acties in BW geleid.

28.1.1.19.1 Acties in Crystal Reports

28.1.1.19.1.1 Nieuwe rapporten maken van een query in een BW-functie

Machtigingsobject	Veld	Waarden
S_USER_AGR	ACT_GROUP	**<USER_ROLE>**
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****

Machtigingsobject	Veld	Waarden
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<USER_ROLE>**: hiermee wordt de naam aangegeven van een functie waartoe de gebruiker behoort. U kunt meerdere waarden in dit veld invoeren.

<QUERY_OWNER>: hiermee wordt de naam aangegeven van de eigenaar van de query. Als u een naam opgeeft, kunt u alleen rapporten maken op basis van de query's met die eigenaar. Voer * in om rapporten te maken op basis van query's met een eigenaar.

Voer voor **<INFO_AREA>, **<INFO_CUBE>** of **<COMP_ID >** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.2 Bestaande rapporten openen vanuit een BW-functie

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****

Machtigingsobject	Veld	Waarden
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.3 Rapporten bekijken of vernieuwen

Machtigingsobject	Veld	Waarden
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>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.4 Databases controleren (tabeldefinities in een rapport vernieuwen)

Machtigingsobject	Veld	Waarden
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>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.5 Locatie instellen van de gegevensbron

Machtigingsobject	Veld	Waarden
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>***

Machtigingsobject	Veld	Waarden
	ACTVT	16

* **<QUERY_OWNER>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.6 Rapporten opslaan in een BW-functie

Machtigingsobject	Veld	Waarden
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>**: hiermee wordt de naam aangegeven van een functie waartoe de gebruiker behoort. U kunt meerdere waarden in dit veld invoeren.

28.1.1.19.1.7 Rapporten voorbereiden voor vertaling tijdens het opslaan naar BW

Machtigingsobject	Veld	Waarden
S_USER_AGR	ACT_GROUP	**<USER_ROLE>**
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>**: hiermee wordt de naam aangegeven van een functie waartoe de gebruiker behoort. U kunt meerdere waarden in dit veld invoeren.

28.1.1.19.1.8 Rapporten opslaan en tegelijkertijd publiceren naar het BI-platform

Machtigingsobject	Veld	Waarden
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>**: hiermee wordt de naam aangegeven van een functie waartoe de gebruiker behoort. U kunt meerdere waarden in dit veld invoeren.

** **<QUERY_OWNER>**: hiermee wordt de naam weergegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

*** Voer voor **< INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.1.9 Starten van de BEx Query Designer™

Machtigingsobject	Veld	Waarden
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP

Machtigingsobject	Veld	Waarden
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>**: hiermee wordt de naam weergegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **< INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.2 Acties in BI-startpunt

28.1.1.19.2.1 Aanmelden bij het BI-platform met SAP-referenties

Machtigingsobject	Veld	Waarden
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

28.1.1.19.2.2 SAP BW-rapporten weergeven op aanvraag

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****

Machtigingsobject	Veld	Waarden
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.2.3 Rapporten vernieuwen vanuit de viewer

Machtigingsobject	Veld	Waarden
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP

Machtigingsobject	Veld	Waarden
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>**: hiermee wordt de naam weergegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **< INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.2.4 Rapporten plannen

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

Machtigingsobject	Veld	Waarden
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>**: hiermee wordt de naam aangegeven van de eigenaar van de query op basis waarvan u het rapport maakt. Als u de naam invoert van de eigenaar van de query, kunt u alleen rapporten maken op basis van query's met deze eigenaar. Voer * in om een queryeigenaar aan te geven.

** Voer voor **<INFO_AREA>**, **<INFO_CUBE>** of **<COMP_ID>** * in om een waarde aan te geven. Als u een specifieke waarde opgeeft, kunt u alleen rapporten maken op basis van query's die deze informatiegebieden, kubussen en component-ID's bevatten.

28.1.1.19.2.5 Dynamische selectielijsten lezen in rapportparameters

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

28.1.1.19.3 Acties in SAP NetWeaver (ABAP)

28.1.1.19.3.1 In Crystal Reports met het stuurprogramma Open SQL

In deze sectie wordt u in Crystal Reports met het stuurprogramma Open SQL door een lijst met verschillende acties in SAP Netweaver (ABAP) geleid.

28.1.1.19.3.2 Aanmelden bij een SAP-server

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.3 Nieuwe rapporten maken

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

28.1.1.19.3.4 Bestaande rapporten openen of bekijken

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

28.1.1.19.3.5 Databases controleren (tabeldefinities in een rapport vernieuwen)

Machtigingsobject	Veld	Waarden
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.6 Locatie instellen van de gegevensbron

Machtigingsobject	Veld	Waarden
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.4 Acties in Crystal Reports met InfoSet-stuurprogramma en rapportage op basis van InfoSet

28.1.1.19.4.1 Aanmelden bij een SAP-server

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.4.2 Een nieuw rapport uit een InfoSet op SAP Netweaver (ABAP) maken

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

> ⓘ Opmerking
>
> voeg tevens voldoende machtigingen toe om gegevensrijen weer te geven. Bijvoorbeeld P_ORIG of P_APAP.

Verwante informatie

Locatie instellen van de gegevensbron [pagina 1051]

28.1.1.19.4.3 Databases controleren (tabeldefinities in een rapport vernieuwen)

Machtigingsobject	Veld	Waarden
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM

28.1.1.19.4.4 Locatie instellen van de gegevensbron

Machtigingsobject	Veld	Waarden
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

28.1.1.19.5 Acties in Crystal Reports met het InfoSet-stuurprogramma en rapportage op basis van een ABAP-query

28.1.1.19.5.1 Aanmelden bij een SAP-server

Machtigingsobject	Veld	Waarden
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.5.2 Nieuwe rapporten maken vanuit een ABAP-query in SAP Netweaver

Machtigingsobject	Veld	Waarden
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	Naam van tabelgroep

28.1.1.19.5.3 Verifiëren van de database

Machtigingsobject	Veld	Waarden
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

28.1.1.19.5.4 Locatie instellen van de gegevensbron

Machtigingsobject	Veld	Waarden
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Naam van tabelgroep

28.1.1.19.6 Acties in het BI-platform

28.1.1.19.6.1 Rapporten plannen in de dialoogmodus (met een Open SQL-query)

Machtigingsobject	Veld	Waarden
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> **Opmerking**
>
> de waarde voor CLASS is BLANK.

28.1.1.19.6.2 Rapporten plannen in de batchmodus met een Open SQL-query

Machtigingsobject	Veld	Waarden
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

> ⓘ Opmerking
>
> de waarde voor CLASS is BLANK.

28.1.1.19.6.3 Crystal-machtigingssysteem

Machtigingsobject	Veld	Waarde
Machtiging voor bestandstoegang (S_DATASET)	Activiteit (ACTVT)	Lezen, Schrijven (33, 34)
	Fysieke bestandsnaam (FILENAME)	* (geeft Alle aan)
	ABAP-programmanaam (PROGRAM)	*
Machtigingscontrole op RFC-toegang (S_RFC)	Activiteit (ACTVT)	16
	Naam van RFC die moet worden beveiligd (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Type RFC-object dat moet worden beveiligd (RFC_TYPE)	Functiegroep (FUGR)

Machtigingsobject	Veld	Waarde
Onderhoud basisgegevens gebruiker: Gebruikersgroepen (S_USER_GRP)	Activiteit (ACTVT)	Maken of genereren, en weergeven (03)
	Gebruikersgroep in onderhoud basisgegevens gebruiker (CLASS)	* **Opmerking** Mogelijk geeft u voor een betere beveiliging liever expliciet een overzicht weer van de gebruikersgroepen waarvan de leden toegang nodig hebben tot het BI-platform.

28.1.1.19.6.4 BW BeX-query's uitvoeren en ontwerpen

Wanneer een rapport van een universe wordt gemaakt op basis van een BW BeX-query, en als er een datumdimensie is opgenomen, moet de systeembeheerder `S_RS_IOBJ`-toestemming geven aan de gebruiker die de universe ontwerpt, en de gebruiker die het rapport uitvoert.

Machtigingsobject	Veld	Waarden
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

28.2 Configureren voor JD Edwards-integratie

28.2.1 Eenmalige aanmelding configureren voor SAP Crystal Reports

Het BI-platform wordt standaard zo geconfigureerd dat SAP Crystal Reports-gebruikers toegang hebben tot JD Edwards EnterpriseOne-gegevens met eenmalige aanmelding.

28.2.1.1 Eenmalige aanmelding voor JD Edwards en SAP Crystal Reports deactiveren

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Selecteer *crdb_pseone*.
5. Klik op *Verwijderen*.
6. Klik op *Opslaan en sluiten*.
7. Selecteer op de pagina *Servers* in de CMC de optie *Crystal Reports Services* en klik op *Server opnieuw starten*.

28.2.1.2 Eenmalige aanmelding activeren voor JD Edwards en SAP Crystal Reports

Als u eenmalige aanmelding hebt gedeactiveerd voor JD Edwards en SAP Crystal Reports en u deze optie weer wilt activeren.

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Onder *SSO-context gebruiken voor aanmelding bij database met de volgende stuurprogramma's* typt u *crdb_pseone*.
5. Klik op *Toevoegen*.
6. Klik op *Opslaan en sluiten*.
7. Selecteer op de pagina *Servers* in de CMC de optie *Crystal Reports Services* en klik op *Server opnieuw starten*.

28.2.2 Secure Sockets Layer configureren voor JD Edwards-integraties

U kunt het SSL-protocol (Secure Sockets Layer) gebruiken voor alle netwerkcommunicatie tussen clients en servers in uw implementatie van het BI-platform en JD Edwards EnterpriseOne.

Voor het gebruik van de JD Edwards EnterpriseOne-gegevens met het BI-platform moet u enkele wijzigingen aanbrengen aan uw SSL-configuratie. Sla net zoals bij de SSL-configuratie voor andere BI-platformservers en -clients de volgende sleutel- en certificaatbestanden op een veilige plaats op (in dezelfde map) die toegankelijk is voor de computers in uw BI-platformimplementatie.

- Het vertrouwde certificaatbestand (cacert.der).
- Het gegenereerde servercertificaatbestand (servercert.der).

- Het serversleutelbestand (server.key).
- Het wachtwoordbestand (passphrase.txt).

28.2.2.1 JD Edwards EnterpriseOne-gegevensconnectiviteit met SSL inschakelen

> **Opmerking**
>
> Alle waarden in de volgende procedure zijn hoofdlettergevoelig.

1. Kopieer uw SSL-certificaten naar `C:\SSLCert`.
2. Start de CCM (Central Configuration Manager).
3. De SIA (Server Intelligence Agent) stoppen.
4. Dubbelklik op de SIA om het dialoogvenster *Eigenschappen* te openen.
5. Klik op het tabblad *Protocol*.
6. Selecteer *SSL inschakelen*.
7. Selecteer voor de *SSL-certificatenmap* de directory die de SSL-certificaten bevat: `C:\SSLCert`.
8. Kies voor het *SSL-certificaatbestand server* de optie `servercert.der`.
9. Kies voor de *Bestanden met vertrouwde SSL-certificaten* de optie `cacert.der`.
10. Kies voor de *SSL-privé-sleutelbestand* de optie `server.key`.
11. Kies voor het *Wachtwoordbestand SSL-privé-sleutel* de optie `passphrase.txt`.
12. Klik op *Toepassen*.
13. Start de Server Intelligence Agent.

U moet uw rapportageservices van BI-platform opnieuw starten (zoals de Adaptive Job Server) om deze wijzigingen te implementeren.

28.2.2.2 Eigenschappenbestand van SSL-configuratie

Het eigenschappenbestand `sslconf.properties` bevat alle informatie over vereiste certificaten en sleutels die door het BI-platform gebruikt worden. Bijvoorbeeld:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Het bestand `sslconf.properties` moet in een map worden geplaatst waarin het BI-platform is geïnstalleerd (dit is standaard `C:\Program Files\Business Objects\BusinessObjects 13.0`).

28.3 Configureren voor PeopleSoft Enterprise-integratie

28.3.1 Eenmalige aanmelding configureren voor SAP Crystal Reports en PeopleSoft Enterprise

Het BI-platform wordt standaard zo geconfigureerd dat SAP Crystal Reports-gebruikers toegang hebben tot PeopleSoft Enterprise-gegevens met eenmalige aanmelding.

28.3.1.1 Eenmalige aanmelding deactiveren voor PeopleSoft Enterprise en SAP Crystal Reports

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Selecteer *crdb_psenterprise*.
5. Klik op *Verwijderen*.
6. Klik op *Opslaan en sluiten*.
7. Selecteer op de pagina *Servers* in de CMC de optie *Crystal Reports Services* en klik op *Server opnieuw starten*.

28.3.1.2 Eenmalige aanmelding activeren voor PeopleSoft Enterprise en SAP Crystal Reports

Als u eenmalige aanmelding hebt gedeactiveerd voor PeopleSoft Enterprise en SAP Crystal Reports en u deze optie weer wilt activeren.

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Onder *SSO-context gebruiken voor aanmelding bij database met de volgende stuurprogramma's* typt u *crdb_psenterprise*.
5. Klik op *Toevoegen*.
6. Klik op *Opslaan en sluiten*.
7. Selecteer op de pagina *Servers* in de CMC de optie *Crystal Reports Services* en klik op *Server opnieuw starten*.

28.3.2 Secure Sockets Layer-communicatie configureren

U kunt het SSL-protocol (Secure Sockets Layer) gebruiken voor alle netwerkcommunicatie tussen clients en servers in uw implementatie van BI-platform.

Sla net zoals bij de SSL-configuratie voor andere BI-platformservers en -clients de volgende sleutel- en certificaatbestanden op een veilige plaats op (in dezelfde map) die toegankelijk is voor de computers in uw BI-platformimplementatie.

- Het vertrouwde certificaatbestand (cacert.der).
- Het gegenereerde servercertificaatbestand (servercert.der).
- Het serversleutelbestand (server.key).
- Het wachtwoordbestand (passphrase.txt).

28.3.2.1 Eigenschappenbestand van SSL-configuratie

Het eigenschappenbestand `sslconf.properties` bevat alle informatie over vereiste certificaten en sleutels die door BI-platformonderdelen gebruikt worden. Bijvoorbeeld:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Het bestand `sslconf.properties` moet worden opgeslagen in de map waar het BI-platform is geïnstalleerd. Dit is standaard `C:\Program Files\Business Objects\BusinessObjects Integration 12.0 Kit for PeopleSoft\`.

28.3.2.2 PeopleSoft-queryserver met SSL inschakelen

> **Opmerking**
>
> Alle waarden in de volgende procedure zijn hoofdlettergevoelig.

1. Kopieer uw SSL-certificaten naar `C:\SSLCert`.
2. Start de CCM (Central Configuration Manager).
3. De SIA (Server Intelligence Agent) stoppen.
4. Dubbelklik op de SIA om het dialoogvenster *Eigenschappen* te openen.
5. Klik op het tabblad *Protocol*.
6. Selecteer *SSL inschakelen*.
7. Selecteer voor de *SSL-certificatenmap* de directory die de SSL-certificaten bevat: `C:\SSLCert`.
8. Kies voor het *SSL-certificaatbestand server* de optie `servercert.der`.

9. Kies voor de *Bestanden met vertrouwde SSL-certificaten* de optie `cacert.der`.
10. Kies voor de *SSL-privé-sleutelbestand* de optie `server.key`.
11. Kies voor het *Wachtwoordbestand SSL-privé-sleutel* de optie `passphrase.txt`.
12. Klik op *Toepassen*.
13. Start de Server Intelligence Agent.

U moet uw rapportageservices van BI-platform opnieuw starten (zoals de Adaptive Job Server) om deze wijzigingen te implementeren.

28.3.2.3 Beveiligingsbrug met SSL inschakelen

> **Opmerking**
>
> Alle waarden in de volgende procedure zijn hoofdlettergevoelig.

1. Kopieer uw SSL-certificaten naar `C:\SSLCert`.
2. Start de CCM (Central Configuration Manager).
3. De SIA (Server Intelligence Agent) stoppen.
4. Dubbelklik op de SIA om het dialoogvenster *Eigenschappen* te openen.
5. Klik op het tabblad *Protocol*.
6. Selecteer *SSL inschakelen*.
7. Selecteer voor de *SSL-certificatenmap* de directory die de SSL-certificaten bevat: `C:\SSLCert`.
8. Kies voor het *SSL-certificaatbestand server* de optie `servercert.der`.
9. Kies voor de *Bestanden met vertrouwde SSL-certificaten* de optie `cacert.der`.
10. Kies voor de *SSL-privé-sleutelbestand* de optie `server.key`.
11. Kies voor het *Wachtwoordbestand SSL-privé-sleutel* de optie `passphrase.txt`.
12. Klik op *Toepassen*.
13. Start de Server Intelligence Agent.

28.3.3 Prestatie-afstemming voor PeopleSoft-systemen

Om te zorgen voor optimale prestaties wanneer u rapporteert over PeopleSoft-query's, is het belangrijk om te weten hoe query's worden uitgevoerd door Crystal Reports en het BI-platform.

Telkens wanneer u een rapport dat is gebaseerd op een PeopleSoft-query vernieuwt of uitvoert, wordt verbinding gemaakt met een PeopleSoft-server:

- In PeopleSoft Enterprise-omgevingen (PeopleTools 8.46 of hoger) wordt een verbinding gemaakt met de *PeopleSoft Analytic Server*.
- In PeopleSoft Enterprise-omgevingen met PeopleTools 8.21-8.45 wordt verbinding gemaakt met de *PeopleSoft-toepassingsserver*.

28.3.3.1 Aanbevelingen

In een optimale implementatie worden een of meer PeopleSoft Analytic of Application Servers ingesteld om alleen rapportaanvragen af te handelen. In elk van deze servers bepalen de instellingen voor Min en Max Instances (minimum- en maximumaantal exemplaren) het aantal rapportaanvragen dat tegelijkertijd kan worden verwerkt. Deze instellingen bieden de volgende voordelen:

- Er is geen conflict tussen rapportaanvragen en andere transactieaanvragen in de PeopleSoft-server.
- Het is mogelijk om onderhoud uit te voeren op de server die rapportaanvragen afhandelt zonder dat u de server die transactieaanvragen afhandelt hoeft uit te schakelen.

In een omgeving waarin zowel rapport- als transactieaanvragen worden afgehandeld door dezelfde PeopleSoft Analytic of Application Server, moet u het BI-platform zodanig configureren dat niet meer dan één rapport tegelijkertijd wordt uitgevoerd. Anders kunnen gebruikers geen transactieaanvragen doen als alle PSANALYTICSRV of PSAPPSRV-processen worden gebruikt om rapporten uit te voeren.

> **Opmerking**
>
> Zie 'Servers beheren en configureren' in de *Beheerdershandleiding voor het SAP BusinessObjects Business Intelligence-platform* voor informatie over de manier waarop u het aantal geplande rapporttaken en taken voor rapportweergave op aanvraag kunt beperken.

> **Opmerking**
>
> Het is niet mogelijk het systeem zodanig te configureren dat het aantal Crystal Reports-gebruikers dat tegelijkertijd toegang mag hebben tot de server, wordt beperkt.

Als er zich toch prestatieproblemen voordoen, gebruikt u het configuratieprogramma Psadmin om te bepalen of aanvragen in de wachtrij worden geplaatst. Controleer bovendien de systeembronnen op het PeopleSoft Analytic of Application Server-apparaat. Als er virtueel geheugen wordt gebruikt vanwege een gebrek aan fysiek geheugen, kan de verwerking ook trager verlopen.

28.3.3.2 PeopleSoft-servers

In een PeopleSoft Analytic Server is het proces waarmee de rapporten worden vernieuwd of uitgevoerd het PSANALYTICSRV-proces. In een PeopleSoft Application Server is het proces waarmee de rapporten worden vernieuwd of uitgevoerd het PSAPPSRV-proces. Het aantal beschikbare PSANALYTICSRV of PSAPPSRV-processen bepaalt het aantal rapporten dat tegelijkertijd kan worden uitgevoerd.

Een doorsnee PeopleSoft Analytic of Application Server-configuratiebestand bevat de volgende informatie:

```
Min Instances=3
Max Instances=5
```

In dit voorbeeld zijn op elk moment minimaal drie PSANALYTICSRV of PSAPPSRV-processen beschikbaar, met de mogelijkheid om dit te verhogen tot maximaal vijf processen. De instellingen betekenen niet noodzakelijkerwijs dat altijd vijf rapporten tegelijk kunnen worden uitgevoerd; de processen kunnen ook worden gebruikt voor het afhandelen van andere taken in het systeem. Als er geen PSANALYTICSRV of PSAPPSRV-processen beschikbaar zijn om een aanvraag af te handelen, wordt deze in de wachtrij geplaatst totdat een proces beschikbaar komt.

> **Opmerking**
>
> Het configuratiebestand voor PeopleSoft *Application* Servers bevat gewoonlijk ook de parameter `Service Timeout`, waarmee wordt aangegeven hoelang aanvragen in de wachtrij moeten wachten tot een proces beschikbaar is. Als er geen proces beschikbaar komt binnen de tijd die voor de parameter is opgegeven, verstrijkt de tijd voor de aanvraag.

28.4 Configureren voor Siebel-integratie

28.4.1 Siebel configureren voor integratie met SAP BI-platform

De integratie van het BI-platform biedt een koppeling met Crystal Reports zodat u inhoud van de BusinessObjects Business Intelligence-suite in een Siebel-toepassing kan insluiten. Nadat het nieuwe menu-item geïnstalleerd en geconfigureerd is, kunnen gebruikers hiermee BI-startpunt starten vanuit de Siebel-toepassing.

De vereiste bestanden worden standaard in de volgende map geïnstalleerd: `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

28.4.1.1 BI-platform/Siebel-integratieproject importeren

1. Start Siebel Tools.
2. Klik op *Tools (Hulpprogramma's)* > *Import from Archive (Importeren uit archief)*.
3. Wanneer u om een archiefbestand wordt gevraagd, gaat u naar de map met Siebel-bestanden van uw geïnstalleerde integratieproduct.

   Standaard is dit: `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.
4. Ga naar de juiste submap (Siebel 7.7 of Siebel 8.0) en selecteer het bestand `BusinessObjectsEnterprise.sif`.
   De wizard Importeren wordt geopend.
5. Klik op *Merge the object definition from the archive file with the definition in the repository* (Objectdefinitie uit archiefbestand met definitie in gegevensopslagruimte samenvoegen).
6. Doorloop de vensters van de wizard om het importeren van het integratieproject te voltooien.
   Het integratieproject wordt aan uw gegevensopslagruimte toegevoegd.
7. Vergrendel het *BusinessObjects Integration*-project.

28.4.2 Het menu-item Crystal Reports aanmaken

1. Vergrendel het project *Menu* (Menu) in Siebel Tools.
2. Selecteer het object *Menu item* (Menu-item) in de Object Explorer (Objectenverkenner).

   > **Opmerking**
   >
   > Als het object Menu niet in de Object Explorer (Objectenverkenner) verschijnt, klikt u op *View (Beeld)* > *Options (Opties)* in Siebel Tools. Klik vervolgens op de tab *Object Explorer (Objectenverkenner)* en selecteer het object *Menu*.

3. Selecteer in de lijst *Menus*(Menu's) het menu *Generic Web* (Algemeen web).
4. Klik op de lijstkop *Menu Items* (Menu-items).
5. Klik op *Bewerken* > *Nieuwe record*.
6. Definieer het nieuwe menu-item. De aanbevolen waarden zijn:
   - Naam: Beeld - Crystal Reports
   - Opdracht: Crystal Reports
   - Opmerkingen: SAP BusinessObjects Integrated Report Menu
   - Inactief: False
7. Gebruik een positienummer om een locatie voor het menu-item in uw menu Beeld te selecteren.

   Sorteer de menu-items op Positie om het kiezen van een positienummer te vergemakkelijken.
8. U kunt nu landinstellingsrecords toevoegen om het bijschrift desgewenst te lokaliseren.

Compileer uw Siebel-toepassing nu opnieuw. Zie De Siebel-toepassing opnieuw compileren [pagina 1063].

28.4.2.1 De Siebel-toepassing opnieuw compileren

Wanneer u het BI-platform hebt geïnstalleerd en de bijbehorende opdrachten beschikbaar hebt gemaakt voor gebruikers via een Siebel-menuoptie, moet u uw Siebel-toepassing opnieuw compileren volgens de gebruikelijke procedures. Raadpleeg de Siebel Bookshelf voor meer informatie.

Wanneer u uw Siebel-toepassing opnieuw hebt gecompileerd, moet u de JavaScript-bestanden van de toepassing opnieuw genereren. In Siebel 7.7 en later kunnen de JavaScript-bestanden automatisch opnieuw gegenereerd worden als onderdeel van het compilatieproces.

Omdat de vereiste stappen voor compilatie van de Siebel Repository (Siebel-gegevensopslagruimte) op uw Siebel Tools-werkstation worden uitgevoerd, moet u de resulterende JavaScripts van het Siebel Tools-werkstation op uw Siebel Server implementeren. Meestal, en afhankelijk van de locatie waarop Siebel is geïnstalleerd, staan de gegenereerde JavaScript-bestanden op de volgende locatie:

```
C:\sea77\tools\PUBLIC\ENU\<srf1096416329_444>
```

De voorbeeldmapnaam `<srf1096416329_444>` wordt door Siebel Tools gegenereerd, en komt uniek overeen met het resulterende gegevensopslagbestand.

De JavaScript-bestanden moeten op de Siebel Server worden geïmplementeerd. Afhankelijk van waar Siebel is geïnstalleerd, gaat het meestal om de volgende locatie:

```
C:\sea77\SWEApp\PUBLIC\ENU\<srf1096416329_444>
```

Behoud de mapnaam die door Siebel Tools wordt gegenereerd.

U moet ook uw Siebel-configuratiebestand op de Siebel Server-computer bijwerken om de service toe te staan. Zoek het toepasselijke configuratiebestand op uw Siebel Server-computer. Als u bijvoorbeeld een Engelse versie van het Siebel Call Center uitvoert, gebruikt u `uagent.cfg`. Dit bestand kunt u standaard vinden op `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` for Siebel 7.7.

Voeg dan de volgende regel toe aan het einde van de SWE-sectie van het configuratiebestand:

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

De `ClientBusinessService`-nummers vormen een opeenvolgende reeks. Als er zich geen andere ClientBusinessServices in de SWE-sectie bevinden, stelt u **`<NUMBER>`** op 0 in. Stel **`<NUMBER>`** anders in op de volgende hoogste waarde.

Voor Siebel 8.x of hoger:

1. Meld u aan bij Siebel Tools en ga naar de toepassing *Siebel Universal Agent* in de Object Explorer (Objectenverkenner).
2. Vouw de toepassingsobjecten uit zodat het object *Application User Prop* zichtbaar wordt.
3. Maak een nieuwe record voor elke bedrijfsservice die gedeclareerd moet worden, en stel daarbij de waarde en naameigenschappen als volgt in:
   - Naam = ClientBusinessServiceX
   - Waarde = BusinessObjects Integration

U maakt nu het menu-item Crystal Reports aan waarmee de geïmporteerde Siebel-opdracht opgeroepen kan worden.

28.4.3 Contextgebonden regels

Contextgebonden regels is een functie die de gebruiker rapporten biedt die waarschijnlijk relevant zijn voor hun huidige taak. Gebruikers die vanuit een Siebel-clienttoepassing rechtstreeks toegang hebben tot Crystal Reports, krijgen in dit geval automatisch rapporten te zien die zijn ontwikkeld om Siebel-gegevens op te nemen.

28.4.3.1 Contextgebonden regels configureren

Voordat u voor contextgevoeligheid configureert, moet u het volgende uitvoeren:

- het Siebel Integration-product installeren
- Siebel geconfigureerd voor integratie met BI-platform

1. Open de CMC (Central Management Console).
2. Klik op *Verificatie*.

3. Dubbelklik op *Siebel*.
   De Siebel-interface voor toewijzingen wordt weergegeven.
4. Klik op *Domeinen*.
   Het domein voor de interface voor toewijzingen wordt weergegeven.
5. Noteer de domeinnaam die overeenkomt met de Siebel-server die u wilt gebruiken.
6. Sluit de Siebel-interface voor toewijzingen.
7. Open het BI-startpunt.
8. Maak een nieuwe map onder `OpenbareMappen\Siebel` met dezelfde naam als het Siebel-domein in de CMC.
9. Plaats alle rapporten die ontworpen zijn om Siebel-informatie op te nemen in deze map.

28.4.3.2 De URL voor contextgebonden regels opgeven

1. Nadat u de JavaScript-bestanden van de toepassing opnieuw hebt gegenereerd, gaat u naar de map met Siebel-bestanden van uw `BI-platform`installatie. Standaard is dit: C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\.
2. Kopieer het bestand `BusinessObjectsEnterpriseServer.html`. Zoek vervolgens de openbare map waarin het genbscript-programma de nieuwe JavaScript-bestanden heeft gegenereerd, en zet een kopie van `BusinessObjectsEnterpriseServer.html` in de toepasselijke taalsubmap.

   Als u de JavaScript-bestanden van een toepassing bijvoorbeeld gegenereerd hebt in de map `C:\sea752\SWEApp\PUBLIC\ENU` op de Siebel-server, kopieert u het bestand `BusinessObjectsEnterpriseServer.html` naar de map `c:\sea752\SWEApp\PUBLIC\ENU`.
3. Open het bestand `BusinessObjectsEnterpriseServer.html` vanuit de openbare map in een teksteditor zoals Notepad, en zoek deze regel:

   ```
   Var userDomain = "SIEB78"
   ```

   ```
   var destAddr = "http://<SAP BusinessObjects-server>:8080/BOE/BI/logon/
   siebelStart.do"
   ```

> **Opmerking**
>
> Als u de variabele `<userDomain>` of `<destAddr>` wijzigt, moet u de webpagina's in cache van uw browser wissen om ervoor te zorgen dat de browser naar het juiste doeladres wijst.

> **Opmerking**
>
> userDomain is hoofdlettergevoelig.

28.4.3.3 Contextgebonden regels controleren

1. Klik in Siebel Tools op *Debug* > *Start* (Fouten opsporen/Start).
2. Navigeer naar een willekeurig scherm en klik op het menu *View (Beeld)*.
   Uw nieuwe menu-item Crystal Reports moet in het menu worden weergegeven.

3. Klik op het menu-item *Crystal Reports*.
   Het BI-platform opent het venster BI-startpunt waarvoor de gebruikersnaam en het wachtwoord vereist is om verbinding te maken. Dit hoeft u alleen te doen bij de eerste keer dat u zich aanmeldt voor een sessietime-out. De domeinnaam die in html geconfigureerd is en de Siebel-verificatie moeten al ingevuld zijn.

> **Opmerking**
>
> Deze stap dient enkel ter verificatie van uw installatie tot aan dit punt. U kunt zich niet bij het BI-platform aanmelden met Siebel-verificatie tot u Siebel-verantwoordelijkheden aan het BI-platform hebt toegewezen.

28.4.3.4 Mappen aan BI-platform toevoegen

Bij de BI-platformintegratie voor Siebel moeten een aantal mappen worden aan het BI-startpunt worden toegevoegd om contextgebonden regels volledig te kunnen inschakelen.

De contextgebonden map moet de volgende structuur hebben om te kunnen functioneren: `Openbare mappen\Siebel\<Domeinnaam>`. Alleen rapporten die in de submap `<Domeinnaam>` zijn opgeslagen en in het Siebel-systeem geconfigureerd zijn voor koppeling aan het specifieke SAP Business Objects-bedrijfsonderdeel, worden als onderdeel van de functie voor contextgebonden regels weergegeven. De `<Domeinnaam>` die hier gebruikt wordt, moet hetzelfde zijn als de domeinnaam die voor Siebel in de verificatieconfiguratie geconfigureerd is, en als de waarde die in het Siebel-bestand `BusinessObjectsEnterpriseServer.html` geconfigureerd is.

> **Opmerking**
>
> U moet Siebel Tools hebben om de stappen in deze sectie te voltooien.

28.4.4 Eenmalige aanmelding configureren voor SAP Crystal Reports en Siebel

BI-platform wordt standaard zo geconfigureerd dat SAP Crystal Reports-gebruikers toegang hebben tot Siebel-gegevens met eenmalige aanmelding.

28.4.4.1 Eenmalige aanmelding deactiveren voor Siebel en SAP Crystal Reports

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Selecteer *crdb_siebel*.

5. Klik op *Verwijderen*.
6. Klik op *Opslaan en sluiten*.
7. Start SAP Crystal Reports opnieuw op.

28.4.4.2 Eenmalige aanmelding activeren voor Siebel en SAP Crystal Reports

Als u eenmalige aanmelding hebt gedeactiveerd voor Siebel en SAP Crystal Reports en u deze optie weer wilt activeren.

1. Klik op *Toepassingen* in de CMC (Central Management Console).
2. Dubbelklik op *Crystal Reports-configuratie*.
3. Klik op *Opties voor eenmalige aanmelding*.
4. Typ onder *SSO-context gebruiken voor eenmalige aanmelding... crdb_siebel*.
5. Klik op *Toevoegen*.
6. Klik op *Opslaan en sluiten*.
7. Start SAP Crystal Reports-servers opnieuw op.

28.4.5 Configureren voor Secure Sockets Layer-communicatie

U kunt het SSL-protocol (Secure Sockets Layer) gebruiken voor alle netwerkcommunicatie tussen clients en servers in uw implementatie van Siebel en BI-platform.

Sla net zoals bij de SSL-configuratie voor andere BI-platformservers en -clients de volgende sleutel- en certificaatbestanden op een veilige plaats op (in dezelfde map) die toegankelijk is voor de computers in uw Siebel-implementatie.

- Het vertrouwde certificaatbestand (cacert.der).
- Het gegenereerde servercertificaatbestand (servercert.der).
- Het serversleutelbestand (server.key).
- Het wachtwoordbestand (passphrase.txt).

Eigenschappenbestand van SSL-configuratie

Het eigenschappenbestand `sslconf.properties` bevat alle gegevens voor vereiste certificaten en sleutels die door onderdelen van de Integration voor Siebel worden gebruikt. Bijvoorbeeld:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
```

```
passphrase=passphrase.txt
```

Het bestand `sslconf.properties` moet in een map worden geplaatst waarin BI-platform is geïnstalleerd (dit is standaard `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`).

28.4.5.1 Siebel-gegevensconnectiviteit met SSL inschakelen

> **Opmerking**
>
> Alle waarden in de volgende procedure zijn hoofdlettergevoelig.

1. Kopieer uw SSL-certificaten naar `C:\SSLCert`.
2. Start de CCM (Central Configuration Manager).
3. De SIA (Server Intelligence Agent) stoppen.
4. Dubbelklik op de SIA om het dialoogvenster *Eigenschappen* te openen.
5. Klik op het tabblad *Protocol*.
6. Selecteer *SSL inschakelen*.
7. Selecteer voor de *SSL-certificatenmap* de directory die de SSL-certificaten bevat: `C:\SSLCert`.
8. Kies voor het *SSL-certificaatbestand server* de optie `servercert.der`.
9. Kies voor de *Bestanden met vertrouwde SSL-certificaten* de optie `cacert.der`.
10. Kies voor de *SSL-privé-sleutelbestand* de optie `server.key`.
11. Kies voor het *Wachtwoordbestand SSL-privé-sleutel* de optie `passphrase.txt`.
12. Klik op *Toepassen*.
13. Start de Server Intelligence Agent.

U moet uw rapportageservices van BI-platform opnieuw starten (zoals de Adaptive Job Server) om deze wijzigingen te implementeren.

29 Logboeken beheren en configureren

29.1 Tracering voor onderdelen registreren

Logboeken

Het BI-platform genereert berichten op systeemniveau en schrijft deze naar logboekbestanden. Systeembeheerders kunnen deze logboekbestanden gebruiken om prestaties te controleren of fouten op te sporen.

Traceringen

Het BI-platform genereert ook traceringen (registraties van gebeurtenissen die optreden tijdens de werking van een gecontroleerd onderdeel) en verzamelt ze in logboekbestanden die de extensie `GLF` hebben. Getraceerde gebeurtenissen lopen uiteen van statusberichten tot ernstige uitzonderingsfouten. SAP-ondersteuningsmedewerkers en -ontwikkelaars kunnen traceringen gebruiken om te rapporteren over de prestaties van BI-platformonderdelen (servers en webtoepassingen) en de activiteit van de gecontroleerde onderdelen.

Wanneer u het traceringslogboekniveau voor een onderdeel instelt, bepaalt u het type en de uitvoerigheid van de informatie die naar het logboekbestand wordt verzonden. Het traceringslogboekniveau is een filter dat traceringen onder een opgegeven drempel onderdrukt. Door het traceringslogboek van een onderdeel te controleren kunt u bepalen of het huidige exemplaar van een onderdeel of de configuratie moet worden gewijzigd om onder een verhoogde belasting te functioneren.

> **Opmerking**
>
> U kunt de logboekbestanden van het BI-platform met een willekeurige teksteditor weergeven.

29.2 Niveaus voor traceringslogboeken

De volgende traceringslogboekniveaus zijn beschikbaar voor BI-platformonderdelen:

Niveau	Beschrijving
Onbepaald	Het niveau voor het traceringslogboek wordt opgegeven via een andere methode, meestal een `INI`-bestand.
Geen	Er wordt geen tracering uitgevoerd.

Niveau	Beschrijving
Laag	Met het filter van het traceringslogboek kunnen foutberichten worden geregistreerd, terwijl waarschuwingen en statusberichten worden genegeerd. Belangrijke statusberichten worden geregistreerd voor het opstarten en afsluiten van onderdelen en begin- en eindverzoeken. Dit niveau wordt niet aanbevolen voor foutopsporing.
Gemiddeld	Het filter voor het traceringslogboek is zo ingesteld dat fout-, waarschuwings- en de meeste statusberichten worden opgenomen. De minder belangrijke of zeer uitgebreide statusberichten worden weggefilterd. Dit niveau is niet uitgebreid genoeg voor foutopsporing.
Hoog	Er worden geen berichten gefilterd. Dit niveau wordt aanbevolen voor foutopsporing. **⚠ Let op** Dit niveau van het traceringslogboek heeft een aanzienlijk effect op systeembronnen, verhoogt CPU-gebruik en neemt opslagruimte in.

29.3 Tracering voor servers configureren

Een logboekbericht is een permanente record van gebeurtenissen en statussen van een softwaresysteem. Traceringen voor een gecontroleerde `BI-platform`implementatie worden naar een specifiek GLF-logboekbestand geschreven in de logboekmap opgeslagen.

- In Windows is de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- In Unix is de standaardlocatie `<INSTALLATIEMAP>/sap_bobj/logging`

De naam van het `GLF`-bestand bevat een korte id, de naam van de server en een nummerreferentie, bijvoorbeeld `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Er wordt een nieuw traceringslogboekbestand gemaakt voor de gecontroleerde server wanneer de grootte van het logboekbestand de drempel van tien megabyte nadert. Bovendien worden vijf logboekbestanden tegelijk onderhouden. Wanneer er nieuwe logboekbestanden worden gemaakt, worden oude logboekbestanden verwijderd.

U kunt de ernst en het belang van de traceringen die in het logboekbestand verzameld zijn, configureren door het traceringslogboekniveau in te stellen voor een bepaalde server of voor een verzameling servers.

> **ⓘ Opmerking**
>
> Als u de traceringslogboekniveaus voor specifieke servers of groepen servers wilt wijzigen, gebruikt u de Traceerlogboekservice in de CMC (Central Management Console). Als u andere parameters wilt wijzigen, wijzigt u het traceringslogboekniveau en andere instellingen handmatig in het bestand `BO_trace.ini`.

29.3.1 Het logboekniveau instellen in de CMC

U kunt het traceringslogboekniveau voor een server aanpassen zonder dat dit invloed heeft op de andere traceringsinstellingen.

1. Roep in het gebied *Servers* van de CMC een server op.
   - Selecteer een server in een specifieke categorie.
   - Klik op *Serverlijst* in het navigatievenster om de complete lijst met servers op te roepen, en selecteer een server.
2. Klik met de rechtermuisknop op de geselecteerde server en selecteer *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
3. Selecteer in het gebied *Traceerlogboekservice* een instelling in de lijst *Logboekniveau*.
4. Klik op *Opslaan en sluiten*.

Het nieuwe traceringslogboekniveau wordt onmiddellijk geïmplementeerd.

Als u een andere uitvoermap voor logboekbestanden wilt opgeven, neemt u de parameter `-loggingPath <doelmap>` in het gebied *Opdrachtregelparameters* op. Start de server opnieuw op om deze instelling te implementeren.

Verwante informatie

Niveaus voor traceringslogboeken [pagina 694]

29.3.2 Het logboekniveau voor meerdere servers instellen in de CMC

1. Roep in het gebied *Servers* van de CMC meerdere servers op.
   - Selecteer servers in een specifieke categorie.
   - Klik op *Serverlijst* in het navigatievenster om de complete lijst met servers op te roepen. Houd `Ctrl` ingedrukt en klik op meerdere servers om ze te selecteren.
2. Klik met de rechtermuisknop op de geselecteerde servers en selecteer *Algemene services bewerken*.
   Het dialoogvenster *Algemene services bewerken* wordt weergegeven.
3. Selecteer in het gebied *Traceerlogboekservice* een instelling in de lijst *Logboekniveau*.
4. Klik op *OK*.

Het nieuwe traceringslogboekniveau wordt onmiddellijk geïmplementeerd.

Als u een andere uitvoermap voor logboekbestanden wilt opgeven, neemt u de parameter `-loggingPath <doelmap>` in het gebied *Opdrachtregelparameters* op. Start de server opnieuw op om deze instelling te implementeren.

Verwante informatie

Niveaus voor traceringslogboeken [pagina 694]

29.3.3 Servertracering configureren via het bestand BO_trace.ini

In het bestand `BO_trace.ini` worden standaard alleen fouten en bevestigingen geregistreerd.

1. Open het bestand `BO_trace.ini`.
   - In Windows is de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - In Unix is de standaardlocatie `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/conf/`.
2. Behandel de regels in de sectie "Trace Syntax and Setting" als programmacode.
3. Wijzig de servertraceringsparameters. De volgende parameters worden gebruikt voor het configureren van servertracering:

Parameter	Mogelijke waarden	Beschrijving
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Hiermee wordt het ernstniveau van logboekberichten bepaald. Het standaardernstniveau van logboekberichten is **`log_error`**. Het ernstniveau van logboekberichten volgt een hiërarchie, waarbij **`log_information`** het hoogste niveau is en **`log_none`** het laagste. Wanneer u een ernstniveau voor logboekberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u het ernstniveau van het logboek instelt op **`log_warning`**, worden berichten zoals **`log_warning`**, **`log_error`** en **`log_fatal`** naar het logboekbestand geschreven. **Opmerking** **`log_information`** en **`log_warning`** kunnen worden ingekort tot **`log_info`** en **`log_warn`**.

Parameter	Mogelijke waarden	Beschrijving
`sap_trace_level`	`trace_debug` `trace_path` `trace_information` `trace_error` `trace_none`	Hiermee wordt het ernstniveau van traceringsberichten bepaald. Het standaardernstniveau van traceringsberichten is `trace_error`. Het ernstniveau van traceringsberichten volgt een hiërarchie, waarbij `trace_debug` het hoogste niveau is en `trace_none` het laagste. Wanneer u een ernstniveau voor traceringsberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u het ernstniveau van traceringsberichten bijvoorbeeld op `trace_path` instelt, worden berichten zoals `trace_path`, `trace_information` en `trace_error` naar het logboekbestand geschreven. **Opmerking** `trace_information` kan worden ingekort tot `trace_info`.

4. Sla het bestand `BO_trace.ini` op en sluit het.

Het bestand `BO_trace.ini` wordt geregeld gelezen. Wijzigingen in het `BO_trace.ini`-bestand worden vijf minuten na het opslaan geïmplementeerd. Als u de CMS opnieuw start, worden wijzigingen in het bestand `BO_trace.ini` onmiddellijk geïmplementeerd.

Voorbeeld

Het bestand `BO_trace.ini`

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

29.3.3.1 Tracering configureren voor een specifieke server

In het bestand `BO_trace.ini` worden traceringsparameters voor BI-platformservers opgegeven. De instellingen zijn van invloed op alle beheerde servers. Beheerders kunnen het bestand `BO_trace.ini` gebruiken om bepaalde traceringsparameters in te stellen voor een specifieke server.

> ⚠ Let op
>
> Nieuwe instellingen voor traceringslogboekniveau die in de CMC voor een specifieke server zijn opgegeven, overschrijven instellingen in `BO_trace.ini`.

1. Open het bestand `BO_trace.ini`.
   - In Windows is de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - In Unix is de standaardlocatie `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/conf/`.
2. Gebruik een `if`-instructie om traceringsinstellingen voor een specifieke server op te geven. Bijvoorbeeld:

   ```
   if (process == "aps_MySIA.ProcessingServer") {
     sap_log_level=log_warning;
     sap_trace_level=trace_path;
   }
   ```

   > → Tip
   >
   > Het proces moet worden opgegeven om de traceringsinstelling op een specifieke server toe te passen.
3. Sla het bestand `BO_trace.ini` op en sluit het.

De gewijzigde instellingen worden binnen vijf minuten geïmplementeerd.

29.4 Tracering configureren voor webtoepassingen

Traceringen voor een gecontroleerde BI-platformimplementatie worden naar een specifiek `GLF`-bestand geschreven en opgeslagen in een map op de computer waarop de webtoepassingsmap wordt gehost.

- In Windows is de standaardlocatie `C:\Windows\System32\config\systemprofile\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` Bijvoorbeeld `C:\Windows\System32\config\systemprofile\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- In Unix is de standaardlocatie `$userHome/SBOPWebapp_<TOEPASSING>_<IP-ADRES>_<POORT>/` Bijvoorbeeld `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

Het traceringslogboekniveau voor webtoepassingen in de CMC is standaard ingesteld op *Niet opgegeven*. Instellingen voor het traceringslogboek zijn beschikbaar voor de volgende toepassingen in de CMC:

- Central Management Console
- BI-startpunt
- Open Document

- Webservice

> **Opmerking**
>
> Als u de traceringslogboekniveaus voor specifieke servers of groepen servers wilt wijzigen, gebruikt u de Traceerlogboekservice in de CMC (Central Management Console). Als u andere parameters wilt wijzigen, wijzigt u het traceringslogboekniveau en andere instellingen handmatig in het bestand `BO_trace.ini`. Dit bestand wordt met de bestanden `BOE.war` en `dswsbobje.war` op uw webtoepassingsserver geïmplementeerd.

Voordat u het bestand `BO_trace.ini` configureert, moet u het Wdeploy-hulpprogramma gebruiken om de implementatie van bestaande webtoepassingen op uw webtoepassingsserver ongedaan te maken. Nadat u het bestand `BO_trace.ini` opnieuw hebt geconfigureerd, moet het bestand samen met de webtoepassingen opnieuw worden geïmplementeerd op uw webtoepassingsserver. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy voor voorbereiding, en implementatie van webtoepassingen en het ongedaan maken van deze implementaties.

29.4.1 Het niveau voor het traceringslogboek voor webtoepassingen instellen in de CMC

Als u andere webtoepassingen wilt traceren, moet u het bijbehorende `BO_trace.ini`-bestand handmatig configureren.

1. Klik in het gebied *Toepassingen* van de CMC met de rechtermuisknop op een toepassing en selecteer *Instellingen van traceringslogboek*.

   > **Opmerking**
   >
   > Deze toepassingen hebben instellingen voor traceringslogboeken: Fiorified BI-startpunt, CMC, Open Document, Promotiebeheer, Versiebeheer, Visueel verschil en Webservice.

   Het dialoogvenster *Instellingen van traceringslogboek* wordt weergegeven.
2. Selecteer een instelling in de lijst *Logboekniveau*.
3. Klik op *Opslaan en sluiten*.
4. Start de webtoepassingsserver opnieuw.

Het nieuwe niveau van het traceringslogboek wordt van kracht na de volgende aanmelding bij de webtoepassing.

Verwante informatie

Niveaus voor traceringslogboeken [pagina 694]

29.4.2 Traceringsinstellingen configureren via het bestand `BO_trace.ini`

Het bestand `BO_trace.ini` wordt met de `BOE`- en `dswsbobje.war`-bestanden geïmplementeerd op uw webtoepassingsserver. U kunt `BO_trace.ini` gebruiken om traceringsparameters op te geven voor BI-platformwebtoepassingen. Aangezien dit bestand niet altijd toegankelijk is, moet u de implementatie van de betreffende webtoepassing opheffen op de webtoepassingsserver.

1. Gebruik Wdeploy om de implementatie van de webtoepassing op uw webtoepassingsserver op te heffen. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.
   - Als u de Tomcat-webtoepassingsserver gebruikt die bij de BI-platforminstallatie wordt geleverd, hoeft u de implementatie van de webtoepassingen niet op te heffen. U kunt de bestanden rechtstreeks wijzigen.
     - Het bestand voor traceringsconfiguratie voor het bestand `BOE.war` bevindt zich in: `<INSTALLATIEMAP>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - Het bestand voor traceringsconfiguratie voor het bestand `dswsbobje.war` bevindt zich in `<INSTALLATIEMAP>\Tomcat\webapps\dswsbobje\WEB-INF\conf`.

   > **Opmerking**
   >
   > Sla stap 2 over als u de gebundelde Tomcat-webtoepassingsserver gebruikt.

2. Roep een vooraf geïmplementeerde versie van het bestand `BO_trace.ini` op:
   - De standaardlocatie van een vooraf geïmplementeerde versie van het configuratiebestand voor het bestand `BOE.war` is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - De standaardlocatie van een vooraf geïmplementeerde versie van het configuratiebestand voor het bestand `dswsbobje.war` is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Open het bestand `BO_trace.ini`.
   - In Windows is de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - In Unix is de standaardlocatie `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/conf/`.
4. Wijzig de servertraceringsparameters. De volgende parameters worden gebruikt voor het configureren van servertracering:

Parameter	Mogelijke waarden	Beschrijving
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Hiermee wordt het ernstniveau van logboekberichten bepaald. Het standaardernstniveau van logboekberichten is **`log_error`**. Het ernstniveau van logboekberichten volgt

Parameter	Mogelijke waarden	Beschrijving
		een hiërarchie, waarbij **log_information** het hoogste niveau is en **log_none** het laagste. Wanneer u een ernstniveau voor logboekberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u het ernstniveau van het logboek instelt op **log_warning**, worden berichten zoals **log_warning**, **log_error** en **log_fatal** naar het logboekbestand geschreven. **Opmerking** **log_information** en **log_warning** kunnen worden ingekort tot **log_info** en **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Hiermee wordt het ernstniveau van traceringsberichten bepaald. Het standaardernstniveau van traceringsberichten is **trace_error**. Het ernstniveau van traceringsberichten volgt een hiërarchie, waarbij **trace_debug** het hoogste niveau is en **trace_none** het laagste. Wanneer u een ernstniveau voor traceringsberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u het ernstniveau van traceringsberichten bijvoorbeeld op **trace_path** instelt, worden berichten zoals **trace_path**, **trace_info** en **trace_error** naar het logboekbestand geschreven. **Opmerking** **trace_information** kan worden ingekort tot **trace_info**.

5. Sla het bestand `BO_trace.ini` op en sluit het.

6. Gebruik WDeploy om het `WAR`-bestand te implementeren op de computer waarop de webtoepassingsserver wordt gehost.

De gewijzigde traceringsinstellingen worden geïmplementeerd nadat de volgende keer bij de webtoepassing wordt aangemeld.

29.4.2.1 Tracering configureren voor een specifieke webtoepassing

Het bestand `BO_trace.ini` is samen met de `BOE`- en `dswsbobje.war`-bestanden geïmplementeerd op de webtoepassingsserver. U kunt `BO_trace.ini` gebruiken om traceringsparameters op te geven voor BI-platformwebtoepassingen. Aangezien dit bestand niet altijd toegankelijk is, moet u de implementatie van de betreffende webtoepassing opheffen op de webtoepassingsserver. Hieronder volgen webtoepassingen en de bijbehorende `WAR`-bestanden:

Webtoepassing	WAR-bestand	Vooraf geïmplementeerde locatie
Central Management Console	`BOE.war`	`<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
BI-startpunt	`BOE.war`	`<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Open Document	`BOE.war`	`<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
Webservice	`dswsbobje.war`	`<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

1. Gebruik Wdeploy om de implementatie van de webtoepassing op uw webtoepassingsserver op te heffen. Zie de *Implementatiehandleiding voor SAP BusinessObjects Business Intelligence-platformwebtoepassingen* voor meer informatie over het gebruik van WDeploy om de implementaties van webtoepassingen ongedaan te maken.
   - Als u de Tomcat-webtoepassingsserver gebruikt die bij de BI-platforminstallatie wordt geleverd, hoeft u de implementatie van de webtoepassingen niet op te heffen. U kunt het bestand rechtstreeks wijzigen.
     - Het bestand voor traceringsconfiguratie voor het bestand `BOE.war` bevindt zich in: `<INSTALLATIEMAP>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - Het bestand voor traceringsconfiguratie voor het bestand `dswsbobje.war` bevindt zich in `<INSTALLATIEMAP>\Tomcat\webapps\dswsbobje\WEB-INF\conf`.

> **Opmerking**
>
> Sla stap 2 over als u de gebundelde Tomcat-webtoepassingsserver gebruikt.

2. Roep een vooraf geïmplementeerde versie van het bestand `BO_trace.ini` op:
   - De standaardlocatie van een vooraf geïmplementeerde versie van het configuratiebestand voor het bestand `BOE.war` is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - De standaardlocatie van een vooraf geïmplementeerde versie van het configuratiebestand voor het bestand `dswsbobje.war` is `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Open het bestand `BO_trace.ini`.
   - In Windows is de standaardlocatie `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - In Unix is de standaardlocatie `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/conf/`.
4. Gebruik een `if`-instructie om traceringsinstellingen voor een specifieke webtoepassing op te geven. Bijvoorbeeld:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

Het proces moet worden opgegeven om de traceringsinstelling op een specifieke webtoepassingsserver toe te passen. De volgende webtoepassingen zijn beschikbaar na de eerste installatie:

Webtoepassing	Naam van apparaat
BI-startpunt	**`WebApp_BIlaunchpad`**
Central Management Server	**`WebApp_CMC`**
OpenDocument	**`WebApp_OpenDocument`**

De volgende parameters worden gebruikt voor het configureren van tracering op webtoepassingsservers:

Parameter	Mogelijke waarden	Beschrijving
`sap_log_level`	**`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`**	Hiermee wordt het ernstniveau van logboekberichten bepaald. Het standaardernstniveau van logboekberichten is **`log_error`**. Het ernstniveau van logboekberichten volgt een hiërarchie, waarbij **`log_information`** het hoogste niveau is en **`log_none`** het laagste. Wanneer u een ernstniveau voor logboekberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u

Parameter	Mogelijke waarden	Beschrijving
		het ernstniveau van het logboek instelt op **log_warning**, worden berichten zoals **log_warning**, **log_error** en **log_fatal** naar het logboekbestand geschreven. **Opmerking** **log_information** en **log_warning** kunnen worden ingekort tot **log_info** en **log_warn**.
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	Hiermee wordt het ernstniveau van traceringsberichten bepaald. Het standaardernstniveau van traceringsberichten is **trace_error**. Het ernstniveau van traceringsberichten volgt een hiërarchie, waarbij **trace_debug** het hoogste niveau is en **trace_none** het laagste. Wanneer u een ernstniveau voor traceringsberichten instelt, worden alle berichten van dat niveau en lager weergegeven. Als u het ernstniveau van traceringsberichten bijvoorbeeld op **trace_path** instelt, worden berichten zoals **trace_path**, **trace_info** en **trace_error** naar het logboekbestand geschreven. **Opmerking** **trace_information** kan worden ingekort tot **trace_info**.

5. Sla het bestand `BO_trace.ini` op en sluit het.
6. Gebruik WDeploy om het `WAR`-bestand te implementeren op de computer waarop de webtoepassingsserver wordt gehost.

29.5 Tracering configureren voor clienttoepassingen van BI-platform

Tracering kan op de volgende clients worden geactiveerd:

- Universe-ontwerpprogramma
- Hulpprogramma voor informatieontwerp
- Web Intelligence Rich Client

U kunt tracering voor deze onderdelen configureren door de INI-bestanden voor elk van de clienttypen te bewerken. Deze INI-bestanden werken precies hetzelfde als het BO_trace.ini-bestand dat elders in dit hoofdstuk wordt beschreven. Zie Servertracering configureren via het bestand BO_trace.ini [pagina 1072] voor meer informatie als u het INI-bestand wilt wijzigen.

De bestanden moeten zich in de werkmappen bevinden die voor deze toepassingen zijn geconfigureerd (standaard `<INSTALLATIEMAP>\SAP BusinessObjects`). Als deze nog niet bestaan, moet u ze misschien maken. De bestanden hebben de volgende namen:

- Hulpprogramma voor universe-ontwerp: `designer_trace.ini`.
- Hulpprogramma voor informatieontwerp: `BO_Trace.ini`
- Web Intelligence Rich Client: `WebIRichClient_trace.ini`

Raadpleeg de documentatie voor deze producten voor meer informatie.

29.6 Uitgebreide tracering van foutmeldingen configureren.

Voor sommige toepassingen zoals SAP BusinessObjects Web Intelligence kunt u tracering inschakelen om logboekbestanden te genereren die uitgebreide informatie bevatten over foutmeldingen die in de toepassing optreden.

> **Opmerking**
>
> Deze logboekbestanden zijn ontworpen om te worden gebruikt door SAP Support-servicemedewerkers. De bestandsindeling van het logboek is JSON.

U schakelt de verslagbestanden met uitgebreide informatie in door het volgende bestand in uw SAP BusinessObjects BI-installatie aan te passen: `extended_info.properties`.

29.7 Logboekbestanden uitgebreide informatie van foutmelding inschakelen

U wilt uitgebreide informatie ophalen over foutmeldingen die in een toepassing optreden. Hiervoor moet u de logboekbestanden met uitgebreide informatie van foutmelding inschakelen.

> **Opmerking**
>
> In SAP BusinessObjects BI Suite versie 4.2 SP5 wordt deze functionaliteit alleen ondersteund voor SAP BusinessObjects Web Intelligence.

1. Open het volgende bestand op uw SAP BusinessObjects BI-installatie: `extended_info.properties`.

   De standaardlocatie is:

   - In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - In UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. Stel de parameters als vereist in:

Parameter	Mogelijke waarden	Beschrijving
`output.format`	• Json • geen	Bestuurt de indeling van de gegenereerde bestanden. **Opmerking** Als u de indeling op geen instelt, wordt er geen bestand gegenereerd.
`output.size`	`<size><unit>` waarbij `<size>` een positief geheel getal is en `<unit>` 'g' voor gigabytes of 'm' voor megabytes is. **Opmerking** De standaardeenheid is kilobytes.	De totale grootte van alle bestanden die een toepassing kan genereren. Wanneer de grootte wordt overschreden, worden de oudere bestanden verwijderd.

De logboekbestanden worden in dezelfde map als de traceringsbestanden gegenereerd. De standaardlocatie is:

- In Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`
- In UNIX: `<INSTALLDIR>/sap_bobj/logging/`

Bestanden hebben de naam `<application_name>_<error_id>_exinfo.<format>`

De toepassingsnaam is de naam van de toepassing waarin de fout is opgetreden. De fout-ID wordt willekeurig gegenereerd. De bestandsindeling is de indeling die in het configuratiebestand is opgegeven.

> **Opmerking**
>
> De enige mogelijke bestandsextensie is `.json`

Een afzonderlijk logboekbestand wordt gegenereerd voor elke melding die in de opgegeven toepassing optreedt

30 Integratie in SAP Solution Manager

30.1 Integratieoverzicht

Er zijn ondersteuningsfuncties toegevoegd aan het BI-platform voor integratie met SAP Solution Manager. De volgende onderdelen van SAP Solution Manager™ kunnen worden gebruikt om ondersteuning voor uw BI-platformimplementatie te bieden:

- Solution Landscape Directory
- Solution Manager Diagnostics
- Introscope by CA Wily
- SAP Passport

> **Opmerking**
>
> Voor toegang tot de SAP-ondersteuningsportal voor SAP BusinessObjects gaat u naar: https://support.sap.com/home.html

30.2 Controlelijst voor SAP Solution Manager-integratie

In de volgende tabel wordt beknopt weergegeven welke onderdelen zijn vereist om SAP Solution Manager in staat te stellen ondersteuning te bieden voor het BI-platform.

SAP Solution Manager-ondersteuning	Vereist voor het BI-platform
SLD-registratie	• SAPHOSTAGENT moet geïnstalleerd zijn voor registratie van BI-platformservers. **Opmerking** Het installatieprogramma van het BI-platform registreert servers automatisch als SAPHOSTAGENT al geïnstalleerd is. • Er moet een connect.key-bestand worden gemaakt voor de gegevensleverancier die op de back-end-servers rapporteert. • (Optioneel) Voor SLD-registratie met WebSphere 6.1 of 7 moet het registratiehulpprogramma SLDREG op elke WebSphere-webtoepassingsserver worden geïnstalleerd. Raadpleeg SAP Note 1482727 voor meer informatie. • (Optioneel) Voor SLD-registratie met SAP NetWeaver 7.2 installeert u SLDREG op elke NetWeaver-host. Raadpleeg SAP Note 1018839 voor meer informatie. • (Optioneel) Voor SLD-registratie met Apache Tomcat moet SLDREG op elke Tomcat-server zijn geïnstalleerd. Raadpleeg SAP Note 1508421 voor meer informatie.
SMD-integratie	• De SMD-agent (DIAGNOSTICS.AGENT) moet worden gedownload en op alle hosts van BI-platformservers worden geïnstalleerd. • De gebruikersaccount SMAdmin moet ingeschakeld zijn in het BI-platform.
Prestatie-instrumentatie	• Introscope-agent moet worden geconfigureerd om een verbinding met Enterprise Manager te kunnen maken. Gebruik het installatieprogramma van BI-platform of de tijdelijke aanduidingen van het CMC-knooppunt om de verbindingen te configureren. • De SMD-agent moet worden geïnstalleerd. • Het BI-platform moet worden geconfigureerd om een verbinding met de SMD-agent te kunnen maken. Gebruik het installatieprogramma van BI-platform of de tijdelijke aanduidingen van het CMC-knooppunt om de verbindingen te configureren.
SAP-paspoort	• U moet het SAP Passport-clienthulpprogramma downloaden en installeren.

30.3 Registratie van systeemlandschapsmap beheren

30.3.1 Registratie van het BI-platform in het systeemlandschap

De System Landscape Directory (SLD) is een centrale gegevensopslagplaats met systeemlandschapsgegevens die relevant zijn voor het beheer van de softwarelevenscyclus. De map bevat een beschrijving van het systeemlandschap (de systemen en softwareonderdelen die momenteel zijn geïnstalleerd). SLD-gegevensleveranciers registreren de systemen op de SLD-server en houden de informatie up-to-date. Beheer- en bedrijfstoepassingen gebruiken de informatie die in de SLD is opgeslagen, om taken in een computeromgeving voor samenwerking uit te voeren.

De gegevensleverancier van de SLD (System Landscape Directory) is de toepassing die verantwoordelijk is voor de registratie van de BI-platformservers op de SLD-server. Er is een specifieke gegevensleverancier beschikbaar voor elke installatie van het platform om over de volgende onderdelen te rapporteren:

- BI-platformservers
- Webtoepassingen en -services die op de WebSphere-webtoepassingsserver worden gehost.

> **Opmerking**
>
> SAP NetWeaver heeft een ingebouwde SLD-DS-leverancier die de NetWeaver-toepassingsserver registreert, evenals gehoste webtoepassingen en -services. Deze SLD-DS is relevant voor BI-platformimplementaties die in een SAP NetWeaver-omgeving zijn geïntegreerd.

De SLD-DS die over de BI-platformservers rapporteert, vereist dat het SLDREG-programma is geïnstalleerd en geconfigureerd. Het SLDREG-programma wordt geïnstalleerd wanneer u het hulpprogramma SAPHOSTAGENT installeert. Raadpleeg de sectie over voorbereiding in de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over het oproepen en installeren van de SAPHOSTAGENT. Wanneer SLDREG is geïnstalleerd, moet u een `connect.key`-bestand maken om een verbinding met de SLD-server tot stand te kunnen brengen.

Raadpleeg de *Implementatiehandleiding voor webtoepassing* voor meer informatie over het configureren van de specifieke gegevensleverancier voor Websphere.

Tijdens de installatie van het BI-platform wordt de informatie die vereist is voor registratie van het BI-platform, opgeslagen in een configuratiebestand. Dit bestand bevat informatie die door de SLD-gegevensleverancier wordt gebruikt om een verbinding met de database van BI-platform tot stand te brengen.

30.3.1.1 Een connect.key-bestand voor de SLD-gegevensleverancier maken

Voordat u een `connect.key`-bestand voor de SLD-gegevensleverancier kunt maken, moet u de SAPHOSTAGENT downloaden en installeren. Zie de sectie over voorbereiding in de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie.

> **Opmerking**
>
> Het `connect.key`-bestand is vereist voor SLD-registratie bij de gegevensleverancier die op BI-platformservers rapporteert.

1. Open een opdrachtregelconsole.
2. Navigeer naar het standaardinstallatiepad van SAPHOSTAGENT.
   - Op Windows: `Program Files\SAP\hostctrl\exe`
   - Op Unix: `/usr/sap/hostctrl/exe`
3. Voer de volgende opdracht uit:

   ```
   sldreg -configure connect.key
   ```
4. Voer de volgende configuratiegegevens in:
   - Gebruikersnaam

- Wachtwoord
- Host
- Poortnummer
- Geef op dat HTTP gebruikt moet worden

Met het hulpprogramma `sldreg` wordt het bestand connect.key gemaakt, dat automatisch gebruikt wordt door de gegevensleverancier om informatie door te geven aan de SLD-server.

30.3.2 Wanneer wordt SLD-registratie geactiveerd?

Het SLD-registratieproces wordt in de volgende scenario's aangeroepen door de gegevensleverancier die op de back-end-servers van BI-platform rapporteert:

- Een serverknooppunt op uw implementatie van BI-platform is opnieuw opgestart.
- Er wordt een nieuwe server of een knooppunt aan de implementatie toegevoegd.
- Er wordt een server of een knooppunt verwijderd.

> **Opmerking**
>
> Wanneer er een server of knooppunt wordt verwijderd, wordt de inhoud op de SLD-server niet gewijzigd door het SLD-registratieproces. Als u de SLD-server wilt bijwerken wanneer er een server of knooppunt is verwijderd, verwijdert u het systeem van de SLD en stuurt u het opnieuw door het BI-platform opnieuw te starten.

De gegevensleverancier voor registratie van de WebSphere-SLD kan handmatig worden aangeroepen of worden ingesteld om op vastgestelde tijden te worden uitgevoerd, bijvoorbeeld elke 24 uur. Raadpleeg SAP Note 482727 voor meer informatie over het configureren van deze gegevensleverancier.

30.3.3 Opschoning SLD vóór patchinstallaties

Gegevens uit vorige versies van BI-platform worden in de SLD-server na een patchinstallatie opgeslagen en veroorzaken problemen bij het vaststellen van de diagnose van het product via SAP Solution Manager. Volg om dit probleem te voorkomen de onderstaande stappen op de basiscomputer voordat patchinstallaties worden gestart:

> **Opmerking**
>
> De functie is beschikbaar voor versies 4.2 SP3 en hoger.

1. Ga naar `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.
2. Voer het batchbestand bobjsldds.bat met opgeschoonde parameters uit (`-clean`).

   > **Opmerking**
   >
   > Het systeem creëert een XML-bestand met vooraf gedefinieerde parameters dat voor opschoning naar de SLD-server wordt gepusht. Er wordt opnieuw opgeschoond nadat u SIA opnieuw hebt gestart.

30.3.4 SLD-verbindingen registreren

Configuratiebestand van gegevensleverancier

Voor implementaties van BI-platform wordt een configuratiebestand gemaakt dat wordt gebruikt voor SLD-registratie. Dit bestand, `sldparserconfig.properties`, bevindt zich in de volgende map: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

SLD-verbindingen registreren

Verbindingen tussen de SLD-server en de gegevensleverancier op de BI-platformimplementatie worden beheerd via het hulpprogramma `sldreg` en het bestand `connect.key`.

> **Opmerking**
>
> De naam van het logboekbestand wordt opgegeven als een eigenschap in het bestand `sldparserconfig.properties`.

Het logboekbestand voor de SLD-gegevensleverancier die op de back-end-servers van BI-platform rapporteert, bevindt zich standaard op de volgende locatie: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. Het bestand wordt elke keer dat de gegevensleverancier wordt uitgevoerd, overschreven.

De logboekbestanden voor `sldreg` bevinden zich standaard op de volgende locatie: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. De namen van de sldreg-logboekbestanden kunnen niet worden gewijzigd en gebruiken de volgende indeling: `sldreg_<Tijdstempel>.log`.

Telkens wanneer de gegevensleverancier sldreg aanroept, wordt er een nieuw logboekbestand gemaakt.

30.3.5 Virtuele hostnaam

Wanneer *Server Intelligence Agent* opnieuw wordt gestart, wordt een gegevensleverancierbestand gegenereerd voor elk knooppunt. Het bestand wordt ingevoerd in de System Landscape Directory en later door SAP Solution Manager gebruikt. In Business Intelligence-platform 4.2 Support Package 4 en eerder is de fysieke hostnaam toegevoegd aan het gegevensleverancierbestand. In Business Intelligence-platform 4.2 Support Package 5 kunt u een virtuele hostnaam definiëren in het bestand *sldparserconfig.properties*, zodat u er zeker van bent dat het gegevensleverancierbestand de virtuele hostnaam gebruikt.

> **Opmerking**
>
> Standaard maakt het gegevensleverancierbestand gebruik van de fysieke hostnaam als het bestand ‘sldparserconfig.properties’ geen virtuele hostnaam bevat.

Volg de onderstaande stappen om de virtuele hostnaam toe te voegen aan sldparserconfig.properties:

1. Ga naar `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.
2. Bewerk het bestand sldparserconfig.properties.
3. Voeg de volgende parameter toe: `virtualHostName = <Virtual Hostname>`.
4. Sla het bestand op.
5. Start *Server Intelligence Agent* opnieuw op om er zeker van te zijn dat de wijzigingen worden gebruikt door het gegevensleverancierbestand.

> **Opmerking**
>
> De wijzigingen kunnen ook worden gebruikt door de onderstaande opdracht uit te voeren:
>
> In Windows: `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` in `<INSTALLATIEMAP>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
>
> In Unix: `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` in `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds`.

30.4 Solution Manager Diagnostics-agenten beheren

30.4.1 Overzicht van Solution Manager Diagnostics

Het SMD-onderdeel (Solution Manager Diagnostics) van SAP Solution Manager biedt volledige functionaliteit om een compleet systeemlandschap centraal te analyseren en bewaken. Het BI-platform kan door de SMD-server gecontroleerd worden als er een SMD-agent is geïnstalleerd. De SMD-agent (`DIAGNOSTICS.AGENT`) verzamelt informatie voor de SMD, die dan gebruikt kan worden voor analyse van hoofdoorzaken. De informatie die wordt verzameld en naar de SMD-server wordt verzonden, bestaat onder meer uit de configuraties van back-end-servers en de locatie van de serverlogboekbestanden.

30.4.2 Met SMD-agents werken

Het BI-platform installeert niet de SMD-agent. U kunt de agent (`DIAGNOSTICS.AGENT`) downloaden vanaf de volgende locatie: https://support.sap.com/swdc.

Informatie over het installeren en configureren van de agent vindt u op: http://service.sap.com/diagnostics

Richtlijnen voor het werken met de SMD-agent

Hieronder vindt u enkele richtlijnen wanneer u SMD-agents gebruikt om het BI-platform te controleren:

- De installatievolgorde van het bewaakte systeem en de agent is niet van belang. U kunt de SMD-agent voor of na installatie en implementatie van het BI-platform installeren.
- Wanneer u een SMD-agent installeert, moet u een aantekening maken van de hostnaam en luisterpoort. Deze informatie is essentieel voor configuratie van het BI-platform als een gecontroleerd systeem. Als u de agent installeert voordat u het bewaakte systeem installeert, kunt u de configuratiegegevens tijdens de installatie van BI-platform opgeven. U kunt deze informatie ook later opgeven via tijdelijke aanduidingen voor de knooppunten in de Central Management Console in uw implementatie.
- Als de back-end-servers worden geïmplementeerd op een gedistribueerd systeem, moet u een SMD-agent op elke computer installeren die een back-end-server host.
- De SMD-agent is vereist voor prestatie-instrumentatie van niet-Java-servers.
- U moet de SMAdmin-gebruikersaccount activeren om de SMD-server toegang tot de CMS te verlenen.

30.4.3 SMAdmin-gebruikersaccount

Voor elke BI-platformimplementatie wordt een gebruikersaccount gemaakt om SMD-integratie te vergemakkelijken. Deze alleen-lezenaccount wordt gebruikt door de SMD-server voor aanmelding bij de CMS en om informatie over de serverconfiguratie en andere gegevens over de implementatie te verzamelen.

De SMAdmin-account is standaard uitgeschakeld.

30.4.3.1 De SMAdmin-account inschakelen

1. Selecteer in het beheergebied *Gebruikers en groepen* van de CMC de optie *Gebruikerslijst*.
   De lijst met gebruikers wordt weergegeven.
2. Zoek de *SMAdmin*-gebruikersaccount.
3. Klik op *Beheren* > *Eigenschappen*.
   Het dialoogvenster *Eigenschappen* wordt weergegeven.
4. Schakel het vakje *Account is uitgeschakeld* uit.
5. Klik op *Opslaan en sluiten*.

30.5 Prestatie-instrumentatie beheren

30.5.1 Prestatie-instrumentatie voor het BI-platform

U kunt CA Wily Introscope als onderdeel van SAP Solution Manager gebruiken om prestatie-instrumentatie in BI-platform te meten. Wanneer u BI-platform installeert, beschikt u over de volgende bronnen voor uw implementatie

- Introscope-agent: Introscope-agents verzamelen prestatiegegevens van back-end Java-servers van BI-platform. Agents verzamelen ook gegevens van de omringende computeromgeving. De agents rapporteren deze gegevens vervolgens bij de Enterprise Manager.
- De meegeleverde bestanden om het instrumentatieproces te vergemakkelijken. Eén set bestanden is bedoeld voor instrumentatie van niet-Java-servers, en de andere set bestanden voor instrumentatie van Java-servers. Het EM-onderdeel (Enterprise Manager) is vereist aan de kant van SAP Solution Manager. EM fungeert als centrale opslagplaats voor alle Introscope-prestatiegegevens die in een toepassingsomgeving zijn verzameld. De EM verwerkt de prestatiegegevens en stelt deze beschikbaar voor gebruikers voor productiecontrole en -diagnose.

30.5.2 Prestatie-instrumentatie instellen voor het BI-platform

Er zijn twee methoden om prestatie-instrumentatie in te stellen voor werkstromen die worden uitgevoerd op back-end-servers van BI-platform.

1. Tijdens de installatieset-up voor het BI-platform. U moet de hostnaam en de luisterpoort voor de SMD-agent weten. Zie de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie. Als u deze optie kiest, wordt instrumentatie standaard uitgevoerd wanneer u het gecontroleerde systeem hebt geïmplementeerd.
2. Na installatie van het BI-platform kunt u de configuratiegegevens aan de SMD-agent verstrekken via tijdelijke aanduidingen in de knooppunteigenschappen in de CMC (Central Management Console).

> **Opmerking**
>
> Voor instrumentatie van werkstromen op niet-Java-servers moet de SMD-agent (`DIAGNOSTICS.AGENT`) zijn geïnstalleerd.

Verwante informatie

Met SMD-agents werken [pagina 1088]

30.5.2.1 Knooppunten voor instrumentatie configureren

Voer de volgende instructies uit als u geen configuratiegegevens voor de SMD-agent en Enterprise Manager hebt opgegeven tijdens de installatie van het BI-platform.

1. Ga naar het gebied *Servers* in de CMC.
2. Klik op *Knooppunten* in het navigatievenster.
   Alle beschikbare knooppunten worden weergegeven.
3. Klik met de rechtermuisknop op het knooppunt waarvoor u instrumentatie wilt uitvoeren, en selecteer *Tijdelijke aanduidingen*.
   Het dialoogvenster Tijdelijke aanduidingen verschijnt.
4. Wijzig de waarde voor de volgende tijdelijke aanduidingen.

Tijdelijke aanduiding	Beschrijving
%IntroscopeAgentEnableInstrumentation%	Hiermee wordt instrumentatie op Java-servers in- of uitgeschakeld. Wordt ingesteld op ingeschakeld als u tijdens de installatie configuratiegegevens voor Enterprise Manager hebt opgegeven. Stel deze waarde in op `WAAR` om instrumentatie in te schakelen.
%IntroscopeAgentEnterpriseManagerHost%	Hostnaam voor de computer waarop Enterprise Manager is geïnstalleerd.
%IntroscopeAgentEnterpriseManagerPort%	Luisterpoort die door Enterprise Manager wordt gebruikt.
%IntroscopeAgentEnterpriseManagerTransport%	Communicatieprotocol dat door Enterprise Manager wordt gebruikt. Ondersteunde protocols zijn onder meer TCP, SSL, HTTP Tunnel en HTTPS.
%NCSInstrumentLevelThreshold%	Wordt gebruikt om het niveau van instrumentatie voor niet-Java-servers in te stellen. Stel deze waarde in op “0” als u instrumentatie wilt uitschakelen. Stel een willekeurige waarde hoger dan “0” in om instrumentatie in te schakelen.
%SMDAgentHost%	De hostnaam van de computer waarop de SMD-agent (`DIAGNOSTICS.AGENT`) is geïnstalleerd.
%SMDAgentPort%	De luisterpoort die door de SMD-agent wordt gebruikt.

5. Klik op *Opslaan en sluiten*.
6. Start het knooppunt opnieuw.

Nadat het knooppunt opnieuw is gestart, worden de opgegeven nieuwe waarden naar alle beheerde servers doorgevoerd.

30.5.3 Prestatie-instrumentatie voor de weblaag

Instrumentatiegegevens voor weblaagonderdelen zijn niet opgenomen in het BI-platform.

30.5.4 Logboekbestanden van instrumentatie

Wanneer uw implementatie van BI-platform is geconfigureerd om instrumentatie uit te voeren, worden berichten op specifieke locaties vastgelegd. U kunt de instrumentatiestatus controleren via de logboekbestanden.

Voor instrumentatie op back-end Java-servers bevindt zich een logboekbestand in de volgende map: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs`. Er wordt voor elk Java-proces een afzonderlijk `LOG`-bestand gemaakt. De map bevat ook `AutoProbe.log`-bestanden waarmee wordt opgegeven welke methoden voor instrumentatie zijn geladen.

Voor instrumentatie van back-end niet-Java-servers bevinden zich logboekbestanden in de volgende map: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/logging/`. In UNIX bevinden de bestanden zich in de map `<sap_bobj>\logging`. Logboekbestanden voor instrumentatie voor niet-Java-servers worden opgeslagen als `TRC`-bestanden.

Voor instrumentatie op webtoepassingsservers bevindt zich een logboekbestand in de volgende map: `<INSTALLATIEMAP>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Er staan twee typen logboekbestanden in deze map: `Introscope.log` en `Autoprobe.log`.

30.6 Tracering met SAP Passport

Naast de tracering van BI-platformonderdelen, zoals servers en webtoepassingen, kan het traceringsmechanisme ook de tracering van een specifieke actie ondersteuning. Met een end-to-end traceringsanalyse wordt de prestatie van één overdracht geanalyseerd. Dankzij de consolidatie van alle traceringsgegevens voor een specifieke actie kunnen SAP-ondersteuningsmedewerkers alle traceringsgegevens zien zonder afgeleid te worden door traceringsgegevens die verwant zijn aan andere acties.

Ga voor meer informatie naar 1861180.

SAP Passport

Het mechanisme dat end-to-end tracering ondersteunt voor het BI-platform is een hulpprogramma genaamd SAP Passport™. Het clienthulpprogramma SAP-paspoort voegt een unieke id toe aan alle HTTP-aanvragen voor een specifieke werkstroom en deze id wordt doorgestuurd naar alle servers die in de werkstroom worden gebruikt. SAP-ondersteuningsmedewerkers kunnen end-to-end tracering samenstellen voor de werkstroom aan de hand van deze unieke id.

> **Opmerking**
>
> Traceringslogboekniveaus die in de CMC en het configuratiebestand `BO_trace.ini` worden opgegeven, worden gebruikt als ze hoger zijn dan de niveaus die zijn opgegeven in het clienthulpprogramma SAP Passport `SAPClientPlugin.exe`.

U kunt het hulpprogramma Passport vinden in de logboeken voor de back-end-servers, webtoepassingen en logboeken van de webservices.

Het clienthulpprogramma SAP Passport is niet geïnstalleerd als onderdeel van het BI-platform. Ga naar https://support.sap.com/swdc om het hulpprogramma te openen en downloaden.

31 Beheer van opdrachtregels

31.1 Unix-scripts

Deze sectie bevat een beschrijving van de beheerprogramma's en scripts die worden geleverd bij de Unix-distributie van het BI-platform. Deze sectie is voornamelijk bedoeld als naslagwerk. Op verschillende plaatsen in deze handleiding worden verschillende concepten en configuratieprocedures voor UNIX in meer detail besproken.

> ⓘ Opmerking
>
> Alleen de gebruiker die het BI-platform heeft geïnstalleerd, heeft de rechten om shellscripts op het BI-platform uit te voeren.

De Unix-distributie van het BI-platform wordt geleverd met verschillende scripts die samen alle configuratieopties omvatten die beschikbaar zijn in de Windows-versie van de CCM (Central Configuration Manager). De distributie bevat ook enkele scripts die toegang bieden tot specifieke Unix-opties of dienen als sjabloon voor uw eigen scripts. Ten slotte bevat de distributie enkele secundaire scripts die worden gebruikt door het BI-platform. De diverse scripts worden afzonderlijk beschreven en waar nodig worden ook de opdrachtregelparameters besproken.

> ⓘ Opmerking
>
> Bij het invoeren van Unix-opdrachtregelparameters moet u speciale shelltekens een andere betekenis of meerdere andere betekenissen geven. Als bijvoorbeeld het uitroepteken "!" in een wachtwoord wordt gebruikt, moet u het uitroepteken een andere betekenis geven, als volgt: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

31.1.1 Scriptprogramma's

In deze sectie worden de beheerscripts beschreven die u kunt gebruiken wanneer het BI-platform wordt uitgevoerd onder UNIX. In de rest van deze sectie worden de concepten toegelicht die ten grondslag liggen aan de taken die u met deze scripts kunt uitvoeren. In deze naslagsectie vindt u de belangrijkste opdrachtregelparameters en hun argumenten.

31.1.1.1 Ccm.sh

Het script `ccm.sh` wordt geïnstalleerd naar de map `<INSTALLATIEMAP>/sap_bobj` van uw installatie. Met dit script beschikt u over een opdrachtregelversie van de Central Configuration Manager. Deze sectie bevat de opdrachtregelparameters en enkele voorbeelden.

> **Opmerking**
>
> Argumenten tussen rechte haken [ ] zijn optioneel.

> **Opmerking**
>
> Als u niet zeker weet wat de naam van de Server Intelligence Agent is, opent u het bestand `ccm.config` en gebruikt u de waarde die achter de optie `-name` staat.

> **Opmerking**
>
> Het script `ccm.sh` kan alleen worden gestart door de gebruiker die de installatie van het BI-platform heeft uitgevoerd.

- Argumenten met de aanduiding **`<overige verificatiegegevens>`** worden beschreven in de tweede tabel.

CCM-parameter	Geldige argumenten	Beschrijving
`-help`	n.v.t.	Help-informatie weergeven op de opdrachtregel.
`-start`	`all` of **`<sianame>`**	Elke Server Intelligence Agent starten als een proces. Met de optie `all` worden alle knooppunten op de computer gestart, inclusief knooppunten op verschillende clusters.
`-stop`	`all` of **`<sianame>`**	Alle Server Intelligence Agents stoppen door hun processen te beëindigen. Met de optie `all` worden alle knooppunten op de computer gestart, inclusief knooppunten op verschillende clusters.
`-restart`	`all` of **`<sianame>`**	Alle Server Intelligence Agents stoppen door hun processen te beëindigen en vervolgens alle Server Intelligence Agents opnieuw starten. Met de optie `all` worden alle knooppunten op de computer gestart, inclusief knooppunten op verschillende clusters.
`-managedstart`	**`<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>`**	Een server starten.
`-managedstop`	**`<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>`**	Een server stoppen.

CCM-parameter	Geldige argumenten	Beschrijving
-managedrestart	**<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>**	Een server stoppen en vervolgens opnieuw starten.
-managedforceterminate	**<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>**	De server onmiddellijk stoppen zonder dat de verwerkingsverzoeken worden voltooid.
-enable	**<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>**	Een gestarte server inschakelen, zodat de server zich kan aanmelden bij het systeem en gaat luisteren op de toegewezen poort. Gebruik de volledige servernaam.
-disable	**<volledig gekwalificeerde servernaam><[overige verificatiegegevens]>**	Een server uitschakelen zodat deze niet meer reageert op verzoeken van het BI-platform, maar nog wel gestart is als een proces. Gebruik de volledige servernaam.
-display	**< [overige verificatiegegevens]>**	Hiermee wordt de huidige status van alle servers in het cluster gerapporteerd, inclusief de servernamen, de hostnamen, de proces-id's en beschrijvingen. Daarnaast wordt aangegeven of de servers actief, ingeschakeld of uitgeschakeld zijn.

De tabel hieronder bevat de parameters die het argument vormen dat wordt aangegeven met **<[overige verificatiegegevens]>**.

> **Opmerking**
>
> Voor verhoogde beveiliging moet u altijd de referenties van een account met Enterprise-verificatie opgeven. Andere typen verificatie worden niet ondersteund.

Verificatieoptie	Geldige argumenten	Beschrijving
-cms	**<cmsname:port#>**	Geef aan bij welke CMS u zich wilt aanmelden. Als u niets opgeeft, wordt de lokale computer en de standaardpoort (6400) ingesteld.
-username	**<gebruikersnaam>**	Geef een account op die beheerdersrechten aan het BI-platform verleent. Als u niets opgeeft, wordt de standaardaccount Administrator gebruikt.

Verificatieoptie	Geldige argumenten	Beschrijving
`-password`	`<password>`	Geef het bijbehorende wachtwoord op. Als u niets opgeeft, wordt een leeg wachtwoord gebruikt. **Opmerking** Als u het argument `-password` wilt opgeven, moet u ook het argument `-username` gebruiken.

De CCM leest de startopdrachten en andere configuratiewaarden uit het bestand `Ccm.config`.

Verwante informatie

Ccm.config [pagina 1098]

31.1.1.1.1 Voorbeelden

Met deze twee opdrachten worden alle BI-platformservers gestart en ingeschakeld. De Central Management Server (CMS) wordt gestart op de lokale computer en met de standaardpoort (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

Met deze twee opdrachten worden alle BI-platformservers gestart en ingeschakeld. De CCM activeert alle servers in het cluster, waarbij de CMS wordt uitgevoerd op MACHINE01 en poort 6701:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Met deze twee opdrachten worden alle BI-platformservers gestart en ingeschakeld met de beheerdersaccount `SysAdmin` en het opgegeven wachtwoord:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Met deze opdracht wordt u aangemeld met de opgegeven beheerdersaccount, waarna een Adaptive Job Server wordt uitgeschakeld die op een tweede computer wordt uitgevoerd:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.1.1.1.2 Ccm.config

Dit configuratiebestand bevat de startopdrachten en andere waarden die worden gebruikt door CCM wanneer u opdrachten uitvoert. Dit bestand wordt onderhouden door de CCM zelf en door de andere scriptprogramma's van het BI-platform. U hoeft dit bestand meestal alleen te wijzigen wanneer u de opdrachtregel van een Server Intelligence Agent wilt aanpassen. Het is uiterst raadzaam een back-up van dit bestand te maken voordat u het handmatig bewerkt.

Verwante informatie

Overzicht van opdrachtregels [pagina 1104]

31.1.1.2 Cmsdbsetup.sh

Het script `cmsdbsetup.sh` staat in de map `<sap_bobj>` van uw installatie. Voer het script uit om een tekstprogramma te starten waarmee u de volgende taken kunt uitvoeren:

- Een CMS-systeemdatabase configureren
- Een CMS-systeemdatabase opnieuw initialiseren
- Gegevens kopiëren uit een andere gegevensbron
- De clustersleutel wijzigen
- De naam van het cluster wijzigen

> **Opmerking**
>
> Maak een back-up van uw huidige CMS-systeemdatabase en de inhoud van uw Input en Output File Repositories voordat u dit script uitvoert. Zie “Een back-up maken van uw systeem en dit herstellen” voor meer informatie. Raadpleeg ook de sectie over het onderbrengen van CMS-servers in clusters in het hoofdstuk “Serveronderhoud” van *SAP BI-platform Beheerdershandleiding* voor aanvullende informatie over CMS-clusters en het configureren van de CMS-database.

U wordt gevraagd de naam van de Server Intelligence Agent (SIA) in te voeren. De naam van uw SIA kunt u vinden in de opdrachteigenschappen van de SIA in het bestand `ccm.config`. De huidige naam van de SIA staat achter de optie `-name`. U kunt ook optie 8 gebruiken met het bestand `serverconfig.sh`.

Verwante informatie

CMS-servers onderbrengen in clusters [pagina 428]
Overzicht van back-up en herstel [pagina 550]

31.1.1.3 Serverconfig.sh

Het script `serverconfig.sh` staat in de map `<sap_bobj>` van uw installatie. Voer dit script uit om een tekstprogramma te starten waarmee u de volgende bewerkingen kunt uitvoeren:

- Een knooppunt toevoegen
- Een knooppunt verwijderen
- Een knooppunt wijzigen
- Een knooppunt verplaatsen
- Back-up maken van serverconfiguratie
- Serverconfiguratie herstellen
- Weblaagconfiguratie wijzigen
- Alle knooppunten weergeven

31.1.1.3.1 Knooppunten toevoegen/verwijderen/wijzigen/weergeven op UNIX

1. Ga naar de map `<INSTALLATIEMAP>/sap_bobj` in uw installatie.
2. Voer de volgende opdracht uit:

   ```
   ./serverconfig.sh
   ```

   Er verschijnt een lijst met mogelijke opties:

   1. Een knooppunt toevoegen
   2. Een knooppunt verwijderen
   3. Een knooppunt wijzigen
   4. Een knooppunt verplaatsen
   5. Back-up maken van serverconfiguratie
   6. Serverconfiguratie herstellen
   7. Weblaagconfiguratie wijzigen
   8. Alle knooppunten weergeven
3. Typ het nummer van de actie die u wilt uitvoeren.
4. Als u een server toevoegt, verwijdert of wijzigt, wordt u gevraagd aanvullende gegevens in te voeren.

31.1.2 Scriptsjablonen

31.1.2.1 Startservers

Het script `startservers` wordt geïnstalleerd naar de map `<INSTALLATIEMAP>/sap_bobj` van uw installatie. Dit script kan fungeren als sjabloon voor uw eigen scripts: het is in feite een voorbeeld van een script dat u zelf kunt maken om de BI-platformservers te starten door een reeks CCM-opdrachten uit te voeren. Zie Ccm.sh [pagina 1094] voor meer informatie over het schrijven van CCM-opdrachten voor uw servers.

31.1.2.2 Stopservers

Het script `stopservers` wordt geïnstalleerd naar de map `<INSTALLATIEMAP>/sap_bobj` van uw installatie. Dit script kan fungeren als sjabloon voor uw eigen scripts: het is in feite een voorbeeld van een script dat u zelf kunt maken om de BI-platformservers te stoppen door een reeks CCM-opdrachten uit te voeren. Zie Ccm.sh [pagina 1094] voor meer informatie over het schrijven van CCM-opdrachten voor uw servers.

31.1.3 Scripts die door het BI-platform worden gebruikt

Deze secundaire scripts worden vaak op de achtergrond uitgevoerd wanneer u de belangrijkste scripthulpprogramma's van het BI-platform uitvoert; u hoeft ze niet zelf uit te voeren.

bobjrestart.sh

Dit script wordt intern door de CCM uitgevoerd om Server Intelligence Agent-knooppunten te beheren. U mag dit script niet zelf uitvoeren.

Env.sh

Het script `env.sh` wordt geïnstalleerd in de map `<sap_bobj/setup>` van de installatie. Met dit script worden de omgevingsvariabelen van het BI-platform ingesteld die vereist zijn voor sommige andere scripts. BI-platformscripts voeren env.sh waar nodig uit. Raadpleeg de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie.

Env-locale.sh

Het script `Env-locale.sh` wordt gebruikt voor het converteren van de tekenreeksen van een scripttaal tussen verschillende typen codering (zoals UTF8, EUC of Shift-JIS). Dit script wordt indien nodig automatisch uitgevoerd door `Env.sh`.

Initlaunch.sh

Het script `initlaunch.sh` voert het script `env.sh` uit om de BI-platformomgevingsvariabelen in te stellen en voert vervolgens eventuele opdrachten uit die u als opdrachtregelargument hebt toegevoegd voor het script. Dit script is voornamelijk bedoeld voor het opsporen van fouten door SAP BusinessObjects.

Postinstall.sh

Het script `postinstall.sh` wordt geïnstalleerd in de map `<SCRIPTMAP>` van de installatie. U moet dit script niet zelf uitvoeren.

Setup.sh

Het script `setup.sh` wordt geïnstalleerd in de hoofdmap van de installatie. Voer het script uit om een tekstprogramma te starten waarmee u de installatie van BI-platform kunt configureren. Dit script wordt automatisch uitgevoerd wanneer u het BI-platform installeert. U wordt gevraagd de gegevens in te voeren die nodig zijn om het BI-platform de eerste keer in te stellen.

Uitgebreide informatie over de verwerking van het installatiescript tijdens de installatie van het BI-platform vindt u in de *Installatiehandleiding voor SAP BusinessObjects Business Intelligence-platform*.

Setupinit.sh

Het script `setupinit.sh` wordt geïnstalleerd in de map `</sap_bobj/init>` van de installatie. Met dit script worden de uitvoeringsscripts gekopieerd naar de `rc#`-mappen voor geautomatiseerd opstarten. Als uw BI-platformservers met de computer waarop ze zijn geïnstalleerd, moeten starten en stoppen, voert u dit script uit nadat het script `setup.sh` is voltooid.

> **Opmerking**
>
> U hebt toegangsrechten voor de hoofdmap nodig om dit script te kunnen uitvoeren.

31.2 Windows-scripts

Deze sectie bevat een beschrijving van de beheerprogramma's en scripts die worden geleverd bij de Windows-distributie van het BI-platform. Deze sectie is voornamelijk bedoeld als naslagwerk. Op verschillende plaatsen in deze handleiding worden verschillende concepten en configuratieprocedures voor UNIX in meer detail besproken.

De Windows-distributie van het BI-platform omvat de Windows-versie van de CCM (Central Configuration Manager). Naast interactie met de gebruikersinterface kunt u kiezen om het uitvoerbare CCM-bestand vanaf de opdrachtregel uit te voeren met opties om uw servers te beheren.

31.2.1 ccm.exe

Het uitvoerbare bestand `ccm.exe` wordt geïnstalleerd in de map `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` van uw installatie. U kunt het

uitvoerbare bestand rechtstreeks vanaf de opdrachtregel uitvoeren om bepaalde bewerkingen uit te voeren. Deze sectie bevat de opdrachtregelparameters en enkele voorbeelden.

> **Opmerking**
>
> Er moeten een SIA (Server Intelligence Agent) en CMS (Central Management Server) actief zijn voordat u de opdrachtregelopties van `ccm.exe` kunt gebruiken voor interactie met een afzonderlijke server.

> **Opmerking**
>
> Argumenten tussen rechte haken [ ] zijn optioneel.

> **Opmerking**
>
> Argumenten met de aanduiding **`<overige verificatiegegevens>`** worden beschreven in de tweede tabel.

CCM-parameter	Geldige argumenten	Beschrijving
`-help`	n.v.t.	Help-informatie weergeven op de opdrachtregel.
`-managedstart`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	Een server starten.
`-managedstop`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	Een server stoppen.
`-managedrestart`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	Een server stoppen en vervolgens opnieuw starten.
`-managedforceterminate`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	De server onmiddellijk stoppen zonder dat de verwerkingsverzoeken worden voltooid.
`-enable`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	Een gestarte server inschakelen, zodat de server zich kan aanmelden bij het systeem en gaat luisteren op de toegewezen poort.
`-disable`	`all` of **`<volledige servernaam> <[overige verificatiegegevens]>`**	Een server uitschakelen zodat deze niet meer reageert op verzoeken van het BI-platform, maar nog wel gestart is als een proces.

CCM-parameter	Geldige argumenten	Beschrijving
`-display`	**`<[overige verificatiegegevens]>`**	Hiermee wordt de huidige status van alle servers in het cluster gerapporteerd, inclusief de servernamen, de hostnamen, de proces-id's en beschrijvingen. Daarnaast wordt aangegeven of de servers actief, ingeschakeld of uitgeschakeld zijn.

De tabel hieronder bevat de parameters die het argument vormen dat wordt aangegeven met **`<[overige verificatiegegevens]>`**.

> **Opmerking**
>
> Bij Enterprise-verificatie moet u altijd de referenties van een account opgeven.

Verificatieoptie	Geldige argumenten	Beschrijving
`-cms`	**`<cms-naam:poortnr.>`**	Geef aan bij welke CMS u zich wilt aanmelden. Als u niets opgeeft, wordt de lokale computer en de standaardpoort (6400) ingesteld.
`-username`	**`<gebruikersnaam>`**	Geef een account op die beheerdersrechten aan het BI-platform verleent. Als u niets opgeeft, wordt de standaardaccount Administrator gebruikt.
`-password`	**`<wachtwoord>`**	Geef het bijbehorende wachtwoord op. Als u niets opgeeft, wordt een leeg wachtwoord gebruikt. **Opmerking** Als u het argument `-password` wilt opgeven, moet u ook het argument `-username` gebruiken.
`-authentication`	**`<Verificatietype>`**	Geef het verificatietype op. Alleen **`secEnterprise`** wordt ondersteund.

De CCM leest de startopdrachten en andere configuratiewaarden uit het bestand `Ccm.config`.

31.2.1.1 Voorbeelden

In het volgende voorbeeld wordt ervan uitgegaan dat er een SIA (Server Intelligence Agent) en een CMS (Central Management Server) gestart en actief zijn. Voordat u de opdrachtregelopties van `ccm.exe` gebruikt

om met een afzonderlijke server te communiceren, kunt u de volgende Windows-opdracht gebruiken om de SIA-service te starten:

```
net start "Server Intelligence Agent (NODENAME)"
```

De SIA kan ook worden gestopt via `net stop "Server Intelligence Agent (NODENAME)"`.

Met deze opdracht worden alle servers van het BI-platform gestart:

```
ccm.exe -managedstart all
```

Met deze opdracht wordt een Adaptive Job Server gestart. De CMS is gestart op poort 6701 in plaats van op de standaardpoort:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Met deze opdracht wordt een Adaptive Job Server geactiveerd met een opgegeven beheerdersaccount met de naam `SysAdmin`:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

Met deze opdracht wordt u aangemeld met de opgegeven beheerdersaccount, waarna een Adaptive Job Server wordt uitgeschakeld die op een tweede computer wordt uitgevoerd:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.3 Opdrachtregels voor servers

31.3.1 Overzicht van opdrachtregels

In deze sectie worden de opdrachtregelopties behandeld waarmee de werking van elke BI-platformserver wordt geregeld.

Wanneer u een server start of configureert via de CMC (Central Management Console), wordt de server (opnieuw) gestart met een standaardopdrachtregel die de standaardopties en -waarden bevat. In de meeste gevallen hoeft u de standaardopdrachtregels niet meteen te wijzigen. Bovendien kunt u de meeste algemene instellingen via de diverse schermen voor serverconfiguratie in de CMC wijzigen. Deze sectie biedt een volledig overzicht van alle opdrachtregelopties die door elke server worden ondersteund. U kunt de opdrachtregel van elke server direct wijzigen als u de werking van het BI-platform verder moet aanpassen.

Wanneer de waarden in deze sectie tussen vierkante haakjes [ ] staan, zijn ze niet verplicht.

> **Opmerking**
>
> In de volgende tabellen worden de ondersteunde opdrachtregelopties weergegeven. BI-platformservers gebruiken een aantal interne opties die niet in deze tabellen worden weergegeven. Deze interne opties mogen niet worden gewijzigd.

31.3.1.1 Opdrachtregels voor servers weergeven of wijzigen

1. Gebruik de Central Management Console (CMC) om de server te stoppen.
2. Klik met de rechtermuisknop op de server en selecteer *Eigenschappen*.
3. Bewerk de opdrachtregel voor de server in het venster *Eigenschappen* en klik op *Opslaan en sluiten*.
4. Start de server.

31.3.2 Standaardopties voor alle servers

Deze opdrachtregelopties zijn van toepassing op alle servers van BI-platform, tenzij anders is aangegeven. Zie de rest van deze sectie voor de opties die specifiek voor de verschillende servertypen gelden.

Optie	Geldige argumenten	Werking
`-requestPort`	`<port >`	Hiermee geeft u de poort op waarop de server luistert. De server registreert deze poort bij de CMS. Als deze poort niet is opgegeven, kiest de server een vrije poort met een nummer hoger dan 1024. **Opmerking** Deze poort wordt voor verschillende doeleinden door verschillende servers gebruikt. Raadpleeg voordat u deze instelling wijzigt de sectie over het wijzigen van de standaardnummers voor serverpoorten in de *Beheerdershandleiding voor BI-platform.*
`-loggingPath`	`<absoluut pad>`	Geef het pad op waar logboekbestanden worden gemaakt.

31.3.2.1 Verwerking van UNIX-signalen

In UNIX verwerken de BI-platform-daemons de volgende signalen:

- `SIGTERM` resulteert in een goede afsluiting van de server (foutcode = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE` en `SIGILL` resulteren in een snelle afsluiting (afsluitcode = 1).

31.3.3 Central Management Server

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de CMS. In Windows is het standaardpad naar de server `<INSTALLATIEMAP>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

In UNIX is het standaardpad naar de server `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<platform>/boe_cmsd`.

Optie	Geldige argumenten	Werking
`-threads`	**`<getal>`**	Het aantal actieve threads dat door de CMS wordt gestart en gebruikt. Geldige waarden zijn tussen 12 en 150; de standaardwaarde is 50.
`-reinitializedb`		Hiermee wordt op de CMS de systeemdatabase verwijderd en wordt er een nieuwe database gemaakt met uitsluitend de standaardsysteemobjecten. Alle bestaande gegevens in de database gaan verloren wanneer de database opnieuw wordt gemaakt.
`-quit`		Hiermee wordt de CMS beëindigd na verwerking van de optie `-reinitializedb`.
`-receiverPool`	**`<aantal>`**	Hiermee geeft u het aantal threads op dat op de CMS wordt gemaakt om clientaanvragen te ontvangen. Een client kan een andere SAP Business Objects-server, de wizard Rapport publiceren, Crystal Reports of een eigen aangepaste clienttoepassing zijn. De standaardwaarde is 5. Deze waarde hoeft u meestal niet verhogen, tenzij u een aangepaste toepassing met veel clients maakt.

Optie	Geldige argumenten	Werking
`-maxobjectsincache`	`<aantal>`	Hiermee geeft u het maximale aantal objecten op dat door de CMS in de geheugencache wordt opgeslagen. Als u het aantal objecten verhoogt, wordt het aantal vereiste databaseaanroepen gereduceerd waardoor de prestaties van de CMS aanzienlijk worden verbeterd. Wanneer er echter te veel objecten in het geheugen worden geplaatst, kan dit tot gevolg hebben dat de CMS te weinig geheugen over heeft om query's te verwerken. De standaardwaarde is 100000.
`-ndbqthreads`	`<aantal>`	Hiermee geeft u het aantal CMS-werkthreads op dat aanvragen naar de database verzendt. Elke thread heeft een verbinding naar de database. Let dus goed op dat u niet de capaciteit van de database overschrijdt. De maximumwaarde moet in de meeste gevallen op 20 worden ingesteld.
`-oobthreads`	`<aantal>`	Als uw cluster meer dan acht CMS-clusterleden bevat, moet u controleren of de opdrachtregel voor elke CMS deze optie bevat. Geef het aantal CMS-services in uw cluster op. Hiermee weet u zeker dat het cluster zwaar netwerkverkeer aankan.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.4 Crystal Reports Processing Server en Crystal Reports Cache Server

De Crystal Reports Processing Server en de Crystal Reports Cache Server worden op ongeveer dezelfde manier vanaf de opdrachtregel beheerd. Met opties op de opdrachtregel bepaalt u of de server als Processing Server, Cache Server of als beide wordt gestart. Hieronder wordt aangegeven welke opties op slechts één type server van toepassing zijn.

In Windows zijn de standaardpaden naar de servers:

- `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\cacheserver.exe`.
- `<INSTALLATIEMAP>\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe`.

In UNIX zijn de standaardpaden naar de servers:

- `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_cachesd`.
- `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd`.

Optie	Geldige argumenten	Werking
`-cache`		Hiermee schakelt u de functionaliteit van de Cache Server in.
`-deleteCache`		Hiermee wordt de cachemap verwijderd telkens wanneer de server wordt gestart of gestopt.
`-report_ProcessExtPath`	**`<absolutepath>`**	Hiermee geeft u de standaardmap voor programma-uitbreidingen op.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.5 Job Servers

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de Adaptive Job Servers.

In Windows is het standaardpad naar de server `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`

Het standaardpad naar de server op UNIX is `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_jobsd`.

Optie	Geldige argumenten	Werking
`-dir`	**`<absoluut pad>`**	Hiermee geeft u de gegevensmap voor de Job Server op.
`-maxJobs`	**`<getal>`**	Hiermee stelt u in hoeveel gelijktijdige taken door de server worden verwerkt. De standaardwaarde is 5.

Optie	Geldige argumenten	Werking
`-requestJSChildPorts`	`<ondergrens-bovengrens>`	Hiermee geeft u het bereik van poorten op dat door secundaire processen in een firewallomgeving mag worden gebruikt. Met `6800-6805` bijvoorbeeld beperkt u de secundaire processen tot zes poorten. **Opmerking** Deze optie wordt pas actief als u ook de instelling `-requestPort` definieert.
`-report_ProcessExtPath`	`<absoluut pad>`	Hiermee geeft u de standaardmap voor programma-uitbreidingen op. Zie de*Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.6 Adaptive Processing Server

De Adaptive Processing Server gebruikt parameters die voor de SAP JVM (Java Virtual Machine) zijn gedefinieerd. Raadpleeg de SAP JVM-documentatie voor meer informatie.

31.3.7 Report Application Server

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de Reports Application Server.

In Windows is het standaardpad naar de server `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`

In UNIX is het standaardpad naar de server `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM>/ras/boe_crystalrasd`.

Optie	Geldige argumenten	Werking
`-ipport`	**`<poort>`**	Hiermee geeft u het poortnummer op dat moet worden gebruikt voor het ontvangen van TCP/IP-aanvragen als de server in zelfstandige modus wordt uitgevoerd (buiten het BI-platform).
`-report_ProcessExtPath`	**`<absoluut pad>`**	Hiermee geeft u de standaardmap voor programma-uitbreidingen op. Zie de*Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie.
`-ProcessAffinityMask`	**`<masker>`**	Gebruik een masker om precies op te geven welke CPU's door RAS worden gebruikt als deze op een computer met meerdere processors wordt uitgevoerd. Het masker heeft de notatie `0xffffffff`, waarbij elke `f` een processor aanduidt en de lijst met processors van rechts naar links wordt gelezen (dit betekent dat de laatste `f` de eerste processor aanduidt). Vervang elke `f` door een 0 (gebruik van CPU niet toegestaan) of `1` (gebruik van CPU toegestaan). Als u de RAS bijvoorbeeld uitvoert op een computer met 4 processors en de 3e en 4e processor wilt gebruiken, gebruikt u het masker `0x1100`. Als de tweede en derde processor moeten worden gebruikt, typt u `0x0110`. **Opmerking** RAS gebruikt de eerste toegestane processors in de reeks tot het maximumaantal van uw licentie is bereikt. Als u een licentie voor twee processors hebt, heeft `0x1110` hetzelfde resultaat als `0x0110`. **Opmerking** De standaardwaarde van het masker is `-1`, wat staat voor `0x1111`.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.8 Web Intelligence-verwerkingsserver

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de Web Intelligence-verwerkingsserver.

In Windows is het standaardpad naar de server `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`

In UNIX is het standaardpad naar de server `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<PLATFORM>/WIReportServer`.

Optie	Geldige argumenten	Werking
`-ConnectionTimeoutMinutes`	**`<minuten>`**	Hiermee geeft u op na hoeveel minuten een time-out van de server optreedt.
`-MaxConnections`	**`<getal>`**	Hiermee geeft u op hoeveel gelijktijdige verbindingen per keer maximaal worden toegestaan door de server.
`-DocExpressEnable`		Hiermee schakelt u het opslaan van Web Intelligence-documenten in het cachegeheugen in wanneer het document wordt weergegeven.
`-DocExpressRealTimeCachingEnable`		Hiermee schakelt u real-time caching van Web Intelligence-documenten in.
`-DocExpressCacheDurationMinutes`	**`<minuten>`**	Hiermee geeft u op hoe lang (in minuten) inhoud in het cachegeheugen wordt opgeslagen.
`-DocExpressMaxCacheSizeKB`	**`<kilobyte>`**	Hiermee geeft u de grootte van de documentcache op.
`-EnableListOfValuesCache`		Hiermee schakelt u de mogelijkheid in om per gebruikerssessie zoeklijsten in het cachegeheugen op te slaan.
`-ListOfValuesBatchSize`	**`<getal>`**	Hiermee geeft u het maximum aantal waarden op dat per batch zoeklijsten wordt geretourneerd.

Optie	Geldige argumenten	Werking
`-UniverseMaxCacheSize`	**`<getal>`**	Hiermee geeft u het aantal universes op dat in het cachegeheugen moet worden opgeslagen.
`-WIDMaxCacheSize`	**`<getal>`**	Hiermee geeft u het maximum aantal Web Intelligence-documenten op dat in het cachegeheugen kan worden opgeslagen.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.9 Input en Output File Repository Server

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de Input en Output File Repository Server.

Het standaardpad naar de servers op Windows is `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

Het standaardpad naar het programma dat beide servers op UNIX biedt, is: `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<platform>/boe_filesd`. De Server Intelligence Agent start standaard één exemplaar van `boe_filesd` voor de Input File Repository Server en één exemplaar voor de Output File Repository Server.

Optie	Geldige argumenten	Werking
`-rootDir`	`<absolutepath>`	Hiermee stelt u de hoofdmap in voor de diverse submappen en bestanden die door de server worden beheerd. Bestandspaden die worden gebruikt om naar bestanden in de File Repository Server te verwijzen, worden ten opzichte van deze hoofdmap geïnterpreteerd. **Opmerking** Alle Input File Repository Servers meten dezelfde hoofdmap delen en alle Output File Repository Servers moeten dezelfde hoofdmap delen (anders loopt u het risico op inconsistente exemplaren). Verder mag de hoofdmap voor de invoer niet gelijk zijn aan de hoofdmap voor de uitvoer. U wordt aangeraden de hoofdmappen te repliceren met een RAID-array of een alternatieve hardwareoplossing.
`-tempDir`	`<absolutepath>`	Hiermee stelt u de locatie in van de tijdelijke map die door de FRS wordt gebruikt om bestanden over te brengen. Gebruik deze opdrachtregeloptie als u de locatie van de tijdelijke FRS-map wilt bepalen of als de standaardnaam van de tijdelijke map die wordt gegenereerd door de FRS de padlimiet van het bestandssysteem overschrijdt (waardoor de FRS niet wordt gestart). **Opmerking** Geef voor deze optie geen bestaande map op. De opgegeven map wordt leeggemaakt wanneer de File Repository Server wordt gestart en wordt verwijderd wanneer de File Repository Server wordt afgesloten. Als u een bestaande map gebruikt, wordt deze dus leeggemaakt en verwijderd.
`-maxidle`	`<minutes>`	Hiermee geeft u op na hoeveel minuten een niet-actieve sessie wordt opgeruimd.

Optie	Geldige argumenten	Werking
`-legacymode`		Hiermee kunnen oudere versies van de SDK, of clients die ouder zijn dan release 4.0, volledige toegang tot het BI-platform verkrijgen.
`-vsaFileLoc`	`<absolutepath>`	Stel het absolute pad in op het bibliotheekbestand van de virusscanadapter. **Opmerking** Alle Input File Repository Servers meten dezelfde hoofdmap delen en alle Output File Repository Servers moeten dezelfde hoofdmap delen (anders loopt u het risico op inconsistente exemplaren).

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

31.3.10 Event Server

In deze sectie worden de opdrachtregelopties behandeld die specifiek zijn voor de Event Server.

Het standaardpad naar de server op Windows is `<INSTALLATIEMAP>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`.

Het standaardpad naar de server op Unix is `<INSTALLATIEMAP>/sap_bobj/enterprise_xi40/<platform>/boe_eventsd`.

Optie	Geldige argumenten	Werking
`-cleanup`	`<minuten>`	Hiermee geeft u op met welke frequentie (in minuten) de server de listenerproxy's moet opruimen. De waarde geeft aan hoeveel tijd tweemaal opschonen in beslag neemt. Als u bijvoorbeeld de waarde 10 opgeeft, worden de proxy's elke vijf minuten opgeschoond.

Verwante informatie

Standaardopties voor alle servers [pagina 1105]

32 Diagnostisch hulpprogramma voor gegevensopslagruimten

32.1 Overzicht van het diagnostisch hulpprogramma voor gegevensopslagruimte

Het diagnostische hulpprogramma voor gegevensopslagruimten is een opdrachtregelprogramma voor het scannen, diagnosticeren en herstellen van inconsistenties die zich voordoen tussen de CMS-systeemdatabase (Central Management Server) en de FRS-filestore (File Repository Server), en inconsistenties die zich voordoen in de metagegevens van InfoObjects die in de CMS-database zijn opgeslagen.

Het is niet gebruikelijk dat er tijdens de normale werking inconsistenties voorkomen in de CMS-systeemdatabase. Inconsistenties kunnen zich echter voordoen bij onverwachte gebeurtenissen, zoals noodherstel, herstel met behulp van een back-up of een netwerkstoring. Tijdens dergelijke gebeurtenissen kan het voorkomen dat de CMS-systeemdatabase wordt onderbroken bij het uitvoeren van een taak. Hierdoor kunnen er inconsistenties met de objecten in de CMS-systeemdatabase ontstaan.

Het diagnostische hulpprogramma voor gegevensopslagruimten scant de CMS-systeemdatabase en detecteert inconsistenties in objecten als rapporten, gebruikers, gebruikersgroepen, mappen, servers, universes, universeverbindingen, enzovoort.

De RDT scant op drie soorten inconsistenties.

- Inconsistenties tussen object en bestand.
  Dit type inconsistentie doet zich voor tussen InfoObjects in de CMS-database en de overeenkomstige bestanden op de File Repository Server. Het kan bijvoorbeeld voorkomen dat er voor een bestand dat in de FRS is opgeslagen geen object in de CMS-systeemdatabase is.
- Inconsistenties in InfoObject-metagegevens.
  Dit type inconsistentie komt voor in de objectdefinitie (metagegevens) van een InfoObject in de CMS-database. Een InfoObject kan bijvoorbeeld verwijzen naar een ander InfoObject dat niet voorkomt in de CMS-database.
- Relatie-inconsistenties
  Deze inconsistenties treden op wanneer er een relatie bestaat tussen twee InfoObjects, maar één ervan is verwijderd. Alleen relaties met de combinatie EnterpriseNode-Server, Service-Server of ServiceContainer-Server worden verwerkt.

Het diagnostische hulpprogramma voor gegevensopslagruimten voert twee functies uit, afhankelijk van de parameters die u opgeeft voor de uitvoering:

- Het hulpprogramma scant de CMS-systeemdatabase en de FRS-filestore, rapporteert inconsistenties en genereert een logboekbestand in XML-indeling met suggesties voor het herstellen van de inconsistenties.
- Het hulpprogramma scant en herstelt de inconsistenties die in de CMS-systeemdatabase en de FRS zijn gedetecteerd, en schrijft de uitgevoerde acties naar een logboekbestand in XML-indeling.

32.2 Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken

Het diagnostische hulpprogramma voor gegevensopslagruimten is beschikbaar op alle computers waarop de CCM (Central Configuration Manager) is geïnstalleerd. Dit opdrachtregelprogramma scant, detecteert en herstelt inconsistenties die zich voordoen tussen de CMS-systeemdatabase (Central Management Server) en de FRS-filestore (File Repository Server), of inconsistenties die voorkomen in de metagegevens van een InfoObject.

Het is beter om een back-up van de CMS-database en FRS-bestandsopslag te maken en het diagnostische hulpprogramma voor gegevensopslagruimten uit te voeren op de back-up terwijl de services van BI-platform niet actief zijn. Als dit niet mogelijk is, kan het diagnostische hulpprogramma voor gegevensopslagruimten op een actieve database worden uitgevoerd.

Als u het hulpprogramma op een actieve database wilt uitvoeren, moet u rekening houden met de volgende factoren:

- Wanneer het diagnostische hulpprogramma voor gegevensopslagruimten actief is, gebruikt het één databaseverbinding.
- Het hulpprogramma controleert alleen de consistentie van de database tot het tijdstip waarop het programma werd gestart. Inconsistenties die optreden terwijl het hulpprogramma actief is, worden niet geregistreerd of hersteld.
- Het is raadzaam dat er voor het verwerken van hulpprogrammatransacties meer geheugen beschikbaar is op de hostcomputer die het hulpprogramma uitvoert dan is aanbevolen.
  - Een database met 50.000 InfoObjects of minder moet een extra 350 MB beschikbaar hebben voor verwerking
  - Een database van 50.000 tot 400.000 InfoObjects moet een extra 1,7 GB beschikbaar hebben voor verwerking
  - Een database met tussen de 400.000 en 1.000.000 InfoObjects moet 4 GB extra beschikbaar hebben voor de verwerking.
- Het diagnostische hulpprogramma voor gegevensopslagruimten hoeft niet op uw CMS-server te worden uitgevoerd. Het effect op systeemprestaties kan worden verminderd door het hulpprogramma op een aparte computer uit te voeren.
- Het hulpprogramma kan een redelijke impact op databaseprestaties hebben.

De CMS-service hoeft niet actief te zijn voor het diagnostische hulpprogramma voor gegevensopslagruimten, aangezien het programma rechtstreeks met de CMS-database wordt uitgevoerd.

32.2.1 Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken

1. Als u het hulpprogramma op een Windows-computer gebruikt, opent u een opdrachtvenster en voert u de volgende opdracht uit.

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe <arguments>`, waarbij `<arguments>` de lijst met parameters is die u wilt opgeven.

2. Als u het hulpprogramma op een Unix-computer gebruikt, opent u een met /usr/bin/sh compatibele shell en voert u de volgende opdracht uit.

   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>`
   waarbij `<platform>` “linux64_x64”, “solaris_sparcv9”, “hpux_ia64” of “aix_rs6000_64” is, en `<arguments>` de lijst met parameters die u wilt opgeven.

   > **Opmerking**
   >
   > Bij het invoeren van Unix-opdrachtregelparameters moet u wellicht speciale shelltekens een andere betekenis of meerdere andere betekenissen geven. Als bijvoorbeeld het uitroepteken “!” in een wachtwoord wordt gebruikt, moet u het uitroepteken misschien een andere betekenis geven, als volgt: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

De gegevensopslagruimte wordt door het diagnostische hulpprogramma voor gegevensopslagruimten gescand op inconsistenties. Afhankelijk van de parameters die u opgeeft, worden inconsistenties gedetecteerd en naar het logboek geschreven of worden inconsistenties hersteld en de uitgevoerde acties naar het logboek geschreven.

Met de opdracht `Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` laat u een overzicht genereren van de inconsistenties die door het hulpprogramma worden gedetecteerd. Als u de gedetecteerde inconsistenties door het hulpprogramma laat herstellen, wordt ook het bestand `Repo_Repair_jjjj_mm_dd_hh_mm_ss.xml` gemaakt. In dit bestand wordt aangegeven welke objecten zijn hersteld en eventuele zwevende bestanden die zijn verwijderd. Inconsistenties die niet konden worden verholpen, worden ook weergegeven.

Het pad naar de logboekbestanden kunt u opgeven met de parameter `outputdir`. Als deze parameter niet is opgegeven, is de standaardmap voor logboekbestanden `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` in Windows en `./sap_bobj/enterprise_xi40/reposcan` in Unix.

> **Opmerking**
>
> De toepassing biedt ook een standaard XSL-bestand dat met het XML-bestand wordt gebruikt om een HTML-pagina te genereren. Het XSL-bestand wordt opgeslagen in`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` in Windows en `./sap_bobj/enterprise_xi40/reposcan` in Unix

Zie *Inconsistenties in de CMS-metagegevens* en *Inconsistenties tussen de CMS en de FRS* voor een overzicht van waarschuwingsberichten en de aanbevolen acties die door het diagnostische hulpprogramma voor gegevensopslagruimten worden uitgevoerd wanneer er inconsistenties worden gedetecteerd.

Verwante informatie

Inconsistenties in de CMS-metagegevens [pagina 1128]
Inconsistenties tussen de CMS en de FRS [pagina 1127]

32.2.2 Parameters voor het diagnostische hulpprogramma voor gegevensopslagruimten

De parameters in de volgende tabel zijn geldig voor het diagnostische hulpprogramma voor gegevensopslagruimten:

> **Opmerking**
>
> Opdrachtregelargumenten prevaleren tijdens de uitvoering boven waarden uit het parameterbestand.

> **Opmerking**
>
> Zie SAP Note 1916845 voor SAP HANA-databaseparameteropties.

Algemene parameters

Parameter	Optioneel of verplicht	Beschrijving
`dbdriver`	Verplicht	Het type stuurprogramma dat wordt gebruikt om verbinding te maken met de CMS-database. Geldige waarden zijn: • `db2databasesubsystem` • `maxdbdatabasesubsystem` • `mysqldatabasesubsystem` • `oracledatabasesubsystem` • `sqlserverdatabasesubsystem` • `sybasedatabasesubsystem` • `sqlanywheredatabasesubsystem`
`connect`	Verplicht	De verbindingsgegevens die worden gebruikt om verbinding te maken met de CMS-database. Bijvoorbeeld: `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"`

Parameter	Optioneel of verplicht	Beschrijving
`dbkey`	Verplicht	Voer de clustersleutel voor uw BI-platformimplementatie in. Als u de clustersleutel niet weet, kunt u deze opnieuw instellen door de volgende stappen uit te voeren: **Opmerking** Als de computer zich in een cluster bevindt, moet u deze stappen voor alle clusterleden uitvoeren. Maak een back-up van de CMS-database en -filestore voordat u verdergaat. 1. Start de CCM (Central Configuration Manager). 2. Klik in de CCM met de rechtermuisknop op de Server Intelligence Agent (SIA) en kies *Stoppen*. Ga pas door naar stap 3 als de SIA-status "Gestopt" is. 3. Klik met de rechtermuisknop op de SIA en kies *Eigenschappen*. 4. Klik op het tabblad Configuratie op *Wijzigen* naast *Configuratie van CMS-clustersleutel*. 5. Er wordt nu een waarschuwing weergegeven. Klik op Ja om verder te gaan. 6. Voer in het dialoogvenster *Clustersleutel wijzigen* dezelfde sleutel van 8 tekens in de velden *Nieuwe clustersleutel* en *Nieuwe clustersleutel bevestigen* in. **Opmerking** Het Diagnostisch hulpprogramma voor gegevensopslagruimte wordt niet uitgevoerd wanneer de parameter `dbkey` wordt weggelaten of als de clustersleutel onjuist is. **Opmerking** De clustersleutel die in de CCM wordt weergegeven, is gecodeerd, en kan niet worden gebruikt in de parameter `dbkey`. Meer informatie over clustersleutels vindt u in "Het BI-platform beveiligen" in de *Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform*.
`inputfrsdir`	Verplicht	Het bestandspad naar de invoer-FRS (File Repository Server). **Opmerking** Het opdrachtregelprogramma wordt uitgevoerd met de gebruikersaccount waarmee u bent aangemeld. Volledige toegang tot de bestandslocatie is vereist.

Parameter	Optioneel of verplicht	Beschrijving
`outputfrsdir`	Verplicht	Het bestandspad naar de uitvoer-FRS (File Repository Server). **Opmerking** Het opdrachtregelprogramma wordt uitgevoerd met de gebruikersaccount waarmee u bent aangemeld. Volledige toegang tot de bestandslocatie is vereist.
`outputdir`	Optioneel	Het bestandspad waarnaar het diagnostische hulpprogramma voor gegevensopslagruimten de logboekbestanden schrijft. De standaardwaarde is `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\reposcan` in Windows en `./sap_bobj/enterprise_xi40/reposcan` in Unix.
`count`	Optioneel	Het geschatte aantal fouten dat moet worden gescand. Dit draagt bij aan optimale prestaties. De hoogste waarde is 2e31 - 1. De waarde 0 wordt geïnterpreteerd als de gehele gegevensopslagruimte. De standaardwaarde is 1000.
`repair`	Optioneel	Alle gedetecteerde inconsistenties worden hersteld. Standaard worden de inconsistenties slechts gerapporteerd en niet hersteld. Als de parameter `-repair` in de opdrachtregel staat, meldt en repareert de RDT alle inconsistenties. **Let op** Met dit proces worden zwevende objecten of bestanden in de gegevensopslagdatabase verwijderd.
`scanfrs`	Optioneel	De CMS en de FRS worden al dan niet gescand op inconsistenties.
`scancms`	Optioneel	De CMS wordt gescand op inconsistenties tussen InfoObjects.
`submitterid`	Optioneel	De gebruikers-id waarmee ontbrekende of ongeldige id's voor geplande objecten worden vervangen. Als er geen waarde is opgegeven, worden ongeldige id's niet vervangen. Komt de opgegeven id niet voor in de CMS, dan wordt door het diagnostische hulpprogramma voor gegevensopslagruimten om een geldige id gevraagd. Deze parameter wordt alleen in de herstelmodus gebruikt.

Parameter	Optioneel of verplicht	Beschrijving
`startid`	Optioneel	Het object in de CMS-database waarvoor de scan moet worden gestart. Wanneer bijvoorbeeld de eerste 500 objecten in de gegevensopslagruimte al zijn gescand, kunt u **`-startid=501`** opgeven om bij het 501e object een nieuwe scan te starten. De standaardwaarde is **`1`**.
`optionsfile`	Optioneel	Het bestandspad naar een parameterbestand. Het parameterbestand is een tekstbestand met alle opdrachtregelopties en de bijbehorende waarden. Het bestand moet één parameter per regel bevatten. **Opmerking** Met deze optie kunt u op de bovenstaande manier al uw parameters instellen in een tekstbestand. Gebruik deze optie om naar het parameterbestand te verwijzen, zonder de parameters in te voeren op de opdrachtregel.
`syscopy`	Optioneel	Deze parameter wordt gebruikt wanneer u de gegevensopslagdatabase kopieert. U moet het hulpprogramma uitvoeren op de nieuwe kopie die u gemaakt hebt. Hiermee wordt de kopie bijgewerkt om clustervorming met de bronsysteemservers te voorkomen. Als u de kopie niet met het bronsysteem hoeft te communiceren, is dit niet nodig. Mag alleen worden gebruikt met de verplichte parameters en mag niet worden gecombineerd met andere optionele parameters in de lijst. **Opmerking** Voer het diagnostische hulpprogramma voor gegevensopslagruimten niet uit op uw bronsysteem met de parameter `syscopy`.
`trace`	Optioneel	Deze parameter genereert ook traceringen (registraties van gebeurtenissen die optreden tijdens de werking van een gecontroleerd onderdeel) en verzamelt ze in logboekbestanden die de extensie GLF hebben, op deze locatie: `<SAP_BOBJ_INST_DIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging`

Parameter	Optioneel of verplicht	Beschrijving
`scankind`	Optioneel	Voer het type InfoObject in dat u op inconsistenties wilt scannen. **Voorbeeld** SI_KIND - Web Intelligence-rapporten, Crystal Reports-rapporten Lijst met ondersteunde InfoObjects die kunnen worden gescand op inconsistenties omvat: • Folder • CrystalReport • Shortcut • User • UserGroup • Calendar • Connection • Category • ObjectPackage • Publication • PDF • RTF • TXT • Note • Word • Excel • Tenant • Profile • Program • Agnostic • Universe • Hyperlink • FullClient • PowerPoint • ScopeBatch • MetaData.DataConnection • Webi • QaaWS • LCMJob • Overload

Parameter	Optioneel of verplicht	Beschrijving
		• Xcelsius • BIWidgets • Mon.Probe • LiveOffice • MDAnalysis • VisualDiff • AO.Workbook • DSL.MetaDataFile • AFDashboardPage • AO.Presentation • CCIS.DataConnection • PlatformSearchQueue • MetaData.BusinessView • PlatformSearchIndex • PlatformSearchContentStore • PlatformSearchContentSurrogate **Opmerking** De uitvoer-XML van scankind geeft de lijst met inconsistenties met betrekking tot InfoObjects weer. Met andere woorden: de betreffende bestandsobjecten moeten niet worden vermeld.
`scandays`	Optioneel	Voer het aantal dagen waarvoor u wilt dat RepoScan op inconsistenties controleert. **Voorbeeld** Elk willekeurig reëel getal behalve 0. **Opmerking** Deze optie werkt op basis van de huidige systeemtijd.

Relaties worden niet gescand tijdens gedeeltelijke scans. Gedeeltelijke scans vinden plaats als een van de volgende drie opties wordt gebruikt:

- startid
- scankind
- scandays

Inconsistenties in de relaties

Waarschuwingsbericht	Inconsistentie	Suggestie	Actie
`Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)`	De rand van een relatie bestaat niet meer.	Sta toe dat de toepassing de relatie verwijdert.	Verwijderde relatie.

Als het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd in een actieve geclusterde CMS worden de volgende parameters gebruikt.

Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken voor een geclusterde CMS

Parameter	Optioneel of verplicht	Beschrijving
`requestport`	Optioneel	Het poortnummer dat door het diagnostische hulpprogramma voor gegevensopslagruimten wordt gebruikt om met de CMS te communiceren. Geldige waarden zijn gehele, positieve getallen. Standaard wordt de waarde gebruikt van het besturingssysteem van de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd.
`numericip`	Optioneel	Het numerieke IP-adres wordt al dan niet in plaats van de hostnaam gebruikt voor de communicatie tussen de CMS en de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd. Geldige waarden zijn **`True`** en **`False`**. De standaardwaarde is **`False`**.
`ipv6`	Optioneel	De ipv6-naam van de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd. Geldige waarden zijn tekenreeksen. De standaardwaarde is de hostnaam van de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd.
`port`	Optioneel	De ipv4-naam van de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd. Geldige waarden zijn tekenreeksen. De standaardwaarde is de hostnaam van de computer waarop het diagnostische hulpprogramma voor gegevensopslagruimten wordt uitgevoerd.
`threads`	Optioneel	Het aantal threads dat moet worden gebruikt. Geldige waarden zijn gehele, positieve getallen. De standaardwaarde is **`12`**.

De volgende parameters worden gebruikt wanneer het diagnostische hulpprogramma voor gegevensopslagruimten SSL toepast voor de communicatie met de CMS-database die wordt gescand.

Het diagnostische hulpprogramma voor gegevensopslagruimten gebruiken met SSL

Parameter	Optioneel of verplicht	Beschrijving
`protocol`	Optioneel	Het diagnostische hulpprogramma voor gegevensopslagruimten wordt al dan niet uitgevoerd met SSL. De enige geldige waarde is **`ssl`**.
`ssl_certdir`	Optioneel	De map waarin de SSL-certificaten zich bevinden.
`ssl_trustedcertificate`	Optioneel	De bestandsnaam van het certificaat.
`ssl_mycertificate`	Optioneel	De bestandsnaam van het ondertekende certificaat.
`ssl_mykey`	Optioneel	De naam van het bestand waarin de persoonlijke SSL-sleutel zich bevindt.
`ssl_mykey_passphrase`	Optioneel	De naam van het bestand waarin het SSL-wachtwoord zich bevindt.

Voorbeeld

Met het volgende Windowsvoorbeeld worden de CMS en de FRS op beide soorten inconsistenties gescand en worden de gedetecteerde inconsistenties hersteld.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect “UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306>”
-inputfrsdir “C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input”
-outputfrsdir    “C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Output”
-dbkey <cluster key>
-repair
```

Voorbeeld

Unixvoorbeeld:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

32.3 Inconsistenties tussen de CMS en de FRS

In de volgende tabel worden de inconsistenties beschreven die kunnen voorkomen tussen een CMS-database (Central Management Server) en de FRS (File Repository Servers), en die door het diagnostische hulpprogramma voor gegevensopslagruimten worden herkend.

- Waarschuwingsbericht
  Het waarschuwingsbericht dat naar het scanlogboek en het herstellogboek wordt geschreven.
- Inconsistentie
  Een beschrijving van de inconsistentie die voor het object is gedetecteerd.
- Suggestie
  De actie die door het diagnostische hulpprogramma voor gegevensopslagruimten wordt voorgesteld wanneer een inconsistentie wordt gedetecteerd. Deze bevindt zich in het scanlogboek.
- Actie
  De actie die door het diagnostische hulpprogramma voor gegevensopslagruimten is uitgevoerd om een inconsistentie te herstellen. Deze bevindt zich in het herstellogboek.

Waarschuwingsbericht	Inconsistentie	Suggestie	Actie
`<Objectnaam>`-object `<objecttype>` (object-id: `<id>`) verwijst naar bestanden die niet bestaan in de FRS (`<bestandsnaam>`).	Het object komt voor in de CMS-database, maar heeft geen bijbehorend bestand in de FRS.	Sta toe dat de toepassing dit object verwijdert. Objecten die onderliggende elementen van dit object zijn, worden ook verwijderd.	Dit object is uit de gegevensopslagruimte verwijderd.
Bestand `<bestandsnaam>` komt voor in de invoer- of uitvoer-FRS (File Repository Server), maar er is geen overeenkomstig InfoObject in de gegevensopslagruimte.	Het bestand komt voor in de FRS, maar heeft geen bijbehorend bestand in de CMS-database.	Sta toe dat de toepassing het niet-gekoppelde bestand verwijdert.	Geen actie ondernomen.
Object `<objectnaam>`, type `<objecttype>` (object-id = `<id>`) heeft bestand `<bestandsnaam>`. De grootte van het opgeslagen bestand is `<grootte>` bytes, wat niet overeenkomt met de feitelijke bestandsgrootte van `<grootte>` bytes.	De grootte van het bestand komt niet overeen met de bestandsgrootte van het InfoObject.	Sta toe dat de toepassing het object met de juiste bestandsgrootte bijwerkt.	Het object is bijgewerkt met de juiste bestandsgrootte.
Deze map bevat geen bestanden.	De FRS-map is leeg.	Sta toe dat de toepassing de map verwijdert.	De lege map is verwijderd.

32.4 Inconsistenties in de CMS-metagegevens

In de volgende tabel worden de inconsistenties beschreven die kunnen voorkomen in de metagegevens van de objecten in een CMS-systeemdatabase (Central Management Server) en door het diagnostische hulpprogramma voor gegevensopslagruimten worden herkend.

- Waarschuwingsbericht
  Het waarschuwingsbericht dat naar het scanlogboek en het herstellogboek wordt geschreven.
- Inconsistentie
  Een beschrijving van de inconsistentie die voor het object is gedetecteerd.
- Suggestie
  De actie die door het diagnostische hulpprogramma voor gegevensopslagruimten wordt voorgesteld wanneer een inconsistentie wordt gedetecteerd. Deze bevindt zich in het scanlogboek.
- Actie
  De actie die door het diagnostische hulpprogramma voor gegevensopslagruimten is uitgevoerd om een inconsistentie te herstellen. Deze bevindt zich in het herstellogboek.

Waarschuwingsbericht	Inconsistentie	Suggestie	Actie
Het bovenliggende object van `<Objecttype>`-object `<Objectnaam>` (Object-id = `<ID>`) ontbreekt (id van bovenliggend object = `<ID>`).	Het bovenliggende object-id van het object ontbreekt of is ongeldig.	Sta toe dat de toepassing het object naar de map BOE repareren verplaatst.	Het object en de onderliggende objecten zijn verplaatst naar de map BOE repareren.
Het eigenaarsobject `<Objecttype>`-object `<Objectnaam>` (object-id = `<ID>`) ontbreekt (id van eigenaarsobject = `<ID>`).	Het eigenaarsobject-id van het object ontbreekt of is ongeldig.	Sta toe dat de toepassing het object aan de beheerder toewijst.	Het object is toegewezen aan de beheerder.
Het verzendersobject `<Objecttype>`-object `<Objectnaam>` (object-id = `<ID>`) ontbreekt (id van verzendersobject = `<ID>`).	Het verzendersobject-id van het object ontbreekt of is ongeldig.	Welke aanbeveling door het diagnostische hulpprogramma voor gegevensopslagruimten wordt weergegeven, is afhankelijk van de vraag of u een waarde hebt opgegeven voor de parameter `-submitterid`. • Als u een waarde hebt opgegeven, is de aanbeveling "Sta toe dat de toepassing het object bijwerkt met de opgegeven verzenders-id".	Als u een waarde voor de parameter `-submitterid` hebt opgegeven, wordt deze waarde toegepast op de verzenders-id van het object. Als u geen waarde voor deze parameter hebt opgegeven, wordt er geen enkele actie uitgevoerd door het diagnostische hulpprogramma voor gegevensopslagruimten. Wanneer u het object opnieuw in een planning opneemt, wordt door de CMS een nieuwe id toegepast.

Waarschuwingsbericht	Inconsistentie	Suggestie	Actie
		• Geeft u deze parameter niet op, dan is de aanbeveling "Plan het object opnieuw of geeft een gebruikers-id op om de ongeldige verzenders-id te vervangen".	
Eigenschap `<Objecttype>`-object '`<Objectnaam>`' (object-id = `<ID>`) van laatste geslaagde exemplaar verwijst naar een ontbrekend object (object-id van laatste geslaagde exemplaar = `<ID>`).	Het laatste geslaagde exemplaar van het object ontbreekt of is ongeldig.	Sta toe dat de toepassing de eigenschap opnieuw berekent.	De eigenschap is opnieuw berekend.
Het kalenderobject van `<Objecttype>`-object '`<Objectnaam'>` (object-id = `<ID>`) ontbreekt (id van kalenderobject = `<ID>`).	Het object verwijst naar een kalender die niet bestaat.	Plan het object opnieuw met een bestaande kalender. Er kan geen actie worden ondernomen door deze toepassing.	Geen actie ondernomen.
De vereiste planningsservergroep van `<Objecttype>`-object '`<Objectnaam>`' (object-id = `<ID>`) ontbreekt (id van servergroepobject = `<ID>`).	De voorkeursserver bestaat niet.	Plan het object opnieuw en kies een bestaande servergroep. Er kan geen actie worden ondernomen door deze toepassing.	Geen actie ondernomen.
De lijst van `<Objecttype>`-object '`<Objectnaam>`' (object-id = `<ID>`) met wachtende gebeurtenissen bevat ontbrekende objecten (id's van gebeurtenisobject = `<ID>`).	De gebeurtenissen waarop dit object wacht, bestaan niet.	Plan het object opnieuw om te wachten op bestaande gebeurtenisobjecten. Er kan geen actie worden ondernomen door deze toepassing.	Geen actie ondernomen.
De gebeurtenissenlijst van `<objecttype>`-object '`<objectnaam>`' (object-id: `<ID>`) die moet worden gestart, bevat ontbrekende object(en) (gebeurtenisobject-id('s) = `<ID>`).	Dit object activeert een gebeurtenis die niet bestaat.	Sta toe dat de toepassing ontbrekende gebeurtenissen uit de lijst met te activeren gebeurtenissen van het object verwijdert.	De ontbrekende gebeurtenissen zijn verwijderd uit de lijst met te activeren gebeurtenissen van het object.
De toegangscontrolelijst van `<objecttype>`-object '`<objectnaam>`' (object-id `<ID>`) verwijst naar een ontbrekende principal (principalobject-id = `<ID>`).	Zwevende ACE (Access Control Entry).	Sta toe dat de toepassing de ontbrekende principal uit de toegangscontrolelijst van het object verwijdert.	De ontbrekende principal is verwijderd uit de toegangscontrolelijst van het object.

Waarschuwingsbericht	Inconsistentie	Suggestie	Actie
De toegangscontrolelijst van `<objecttype>`-object '`<objectnaam>`' (object-id = `<ID>`) verwijst naar een ontbrekend toegangsniveau (object-id van toegangsniveau = `<ID>`).	Zwevende ACE (Access Control Entry).	Sta toe dat de toepassing het ontbrekende toegangsniveau uit de toegangscontrolelijst van het object verwijdert.	Het ontbrekende toegangsniveau is verwijderd uit de toegangscontrolelijst van het object.
`<Objecttype>`-object `<objectnaam>` (object-id = `<ID>`) heeft meerdere Favorieten-mappen.	Een bepaalde gebruikersaccount heeft meerdere Favorieten-mappen.	Sta toe dat de toepassing meerdere mappen in één Favorieten-map consolideert.	Alle Favorieten-mappen zijn samengevoegd tot één Favorieten-map.
`<Objecttype>`-object `<objectnaam>` (object-id = `<ID>`) bevat ongeldige ingangen voor invoerbestand (`<Bestanden>`).	Het object bevat ongeldige ingangen in de lijst met invoerbestanden.	Laat het hulpprogramma de ongeldige vermeldingen van het object verwijderen uit de lijst met invoerbestanden.	De ongeldige vermeldingen zijn verwijderd uit de lijst met invoerbestanden van het object.
`<Objecttype>`-object `<objectnaam>` (object-id = `<ID>`) bevat ongeldige ingangen voor uitvoerbestand (`<Bestanden>`).	Het object bevat ongeldige ingangen in de lijst met uitvoerbestanden.	Laat het hulpprogramma de ongeldige vermeldingen van het object verwijderen uit de lijst met uitvoerbestanden.	De ongeldige vermeldingen zijn verwijderd uit de lijst met uitvoerbestanden van het object.
De vereiste cacheservergroep van `<objecttype>`-object '`<Objectnaam>`' (object-id = `<ID>`) ontbreekt (id van servergroepobject = `<ID>`).	De vereiste cacheservergroep ontbreekt in het object.	Plan het object opnieuw en kies een bestaande servergroep.	Geen actie ondernomen.
De vereiste verwerkingsservergroep van `<objecttype>`-object '`<objectnaam>`' (object-id = `<ID>`) ontbreekt (id van servergroepobject = `<ID>`).	De vereiste verwerkingsservergroep ontbreekt in het object.	Plan het object opnieuw en kies een bestaande servergroep.	Geen actie ondernomen.
De lijst van `<objecttype>`-object '`<objectnaam>`' (object-id = `<ID>`) met profielen bevat ontbrekende objecten (id's van profielobject = `<ID>`).	Het object bevat ontbrekende objecten in de lijst met profielen.	Werk uw publicatie bij met bestaande profielen. Er kan geen actie worden ondernomen door de toepassing.	Geen actie ondernomen.

32.5 Restful-SDK beheren in BOE WebApp

Om het BIPRWS WebApp-gedeelte van de BOE Webapp in 4.3 SP03 te activeren, stelt u de vlag in op *true* op de onderstaande locatie:

```
<BOE_INST_DIR>\SAP BusinessObjects\tomcat\webapps\BOE\WEB-
INF\internal\Global.properties
```

Stel `use.boe.internal.biprws=true` in.

Als de vlag is ingesteld op 'true', zijn interne toepassingen nu niet afhankelijk van de URL van de RESTful-toepassing of de vlag van het relatieve pad die is ingesteld in CMC.

De functie biedt voordelen omdat het helpt het volgende te voorkomen:

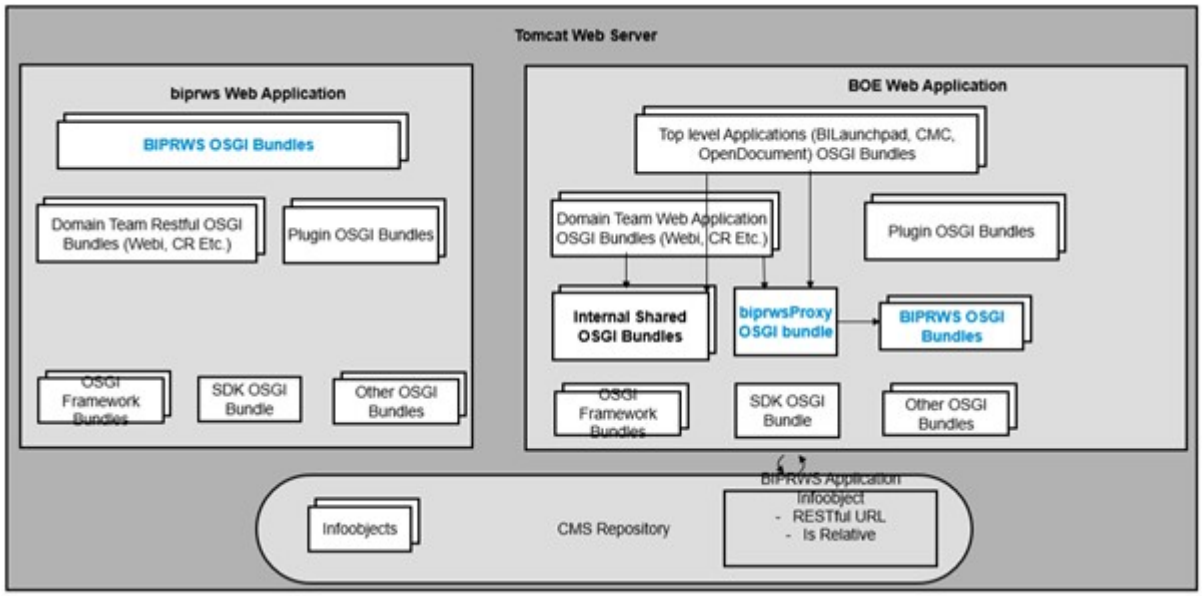
- CORS-problemen (Cross-Origin Resource Sharing)
- Problemen met interne en externe systeemverbindingen
- Pingen van BOE WebApp om de sessie actief te houden
- Proxy-gerelateerde problemen omdat er geen aparte configuratie is voor BIPRWS en BOE
- Problemen met clusters van webtoepassingen

De bestaande implementatie met BOE Webapp werkt naadloos na de upgrade.

Logboekfunctie:

zodra BIPRWS is samengevoegd met BOE WebApp, worden de logboeken gegenereerd als onderdeel van de locatie van het BI-startpunt of het CMC-toepassingslogboek.

Architectuur:



33 HSTS (HTTP Strict Transport Security)

33.1 HSTS (HTTP Strict Transport Security) configureren

HSTS (HTTP Strict Transport Security) is een beleidsmechanisme om websites te beschermen tegen man-in-the-middle aanvallen zoals protocoldowngrade-aanvallen en het kapen van cookies.

Het biedt webservers de mogelijkheid aan te geven dat webbrowsers (of andere gebruikersagents die aan de regels voldoen) automatisch met deze webbrowsers kunnen communiceren via HTTPS-verbindingen. Dit biedt TLS/SSL (Transport Layer Security), in tegenstelling tot onveilig HTTP-gebruik.

HSTS is een IETF Standards Track Protocol en wordt gespecificeerd in RFC 6797

Het HSTS-beleid wordt door de server aan de gebruiker-agent doorgegeven via een HTTP-antwoordkopveld met de naam 'Strict-Transport-Security'.

1. Dit beleid specificeert een periode waarin de gebruikersagent alleen op een veilige manier toegang tot de server kan krijgen.
2. Websites die gebruikmaken van HSTS accepteren vaak geen HTTP met duidelijke tekst, hetzij door verbindingen via HTTP te weigeren of gebruikers systematisch naar HTTPS te leiden (hoewel dit niet wordt vereist door de specificatie).
   Dit is om ervoor te zorgen dat een gebruikersagent die niet in staat is TLS uit te voeren mogelijk geen verbinding kan maken met de site.
3. De bescherming is alleen van toepassing nadat een gebruiker de site ten minste eenmaal heeft bezocht, waarbij hij zich baseert op het principe van vertrouwen bij het eerste gebruik.

Hoe werkt het

Wanneer een gebruiker een URL invoert of selecteert voor de site die HTTP specificeert, wordt de URL automatisch bijgewerkt naar HTTPS zonder dat er een HTTP-aanvraag wordt ingediend. Dit voorkomt dat de HTTP man-in-the-middle aanval plaatsvindt.

In 4.3 SP03 biedt SAP BOE ondersteuning voor de HSTS-regeling.

Voordat u HSTS configureert, moet uw toepassingsserver zijn geconfigureerd met SSL.

Voer de onderstaande stappen uit om ondersteuning voor HSTS in te schakelen:

1. Stop Tomcat.
2. Navigeer naar `E:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default`.
3. Open het bestand Global.properties en stel de onderstaande parameters in.
   1. `hsts.enabled` True/False. De standaardwaarde is false.
   2. `hsts.Include.SubDomains` True /False. Dit beïnvloedt alle subdomeinen van de domeinnaam.
   3. `hsts.MaxAge.Seconds` = 31536000.
   4. Standaardwaarde = 365 dagen.
4. Sla de wijzigingen op.

34 Bijlage Rechten

34.1 De rechtenbijlage

Deze rechtenbijlage bevat een opsomming en een beschrijving van de meeste rechten die kunnen worden ingesteld voor de objecten in het BI-platformsysteem. In geval u meerdere rechten nodig hebt om een taak op een object te kunnen uitvoeren, vindt u hier ook informatie over de aanvullende rechten en voor welke objecten u deze nodig hebt. Zie het hoofdstuk *Rechten instellen* in de *Beheerdershandleiding voor SAP BI-platform* voor meer informatie over het instellen van rechten.

34.2 Algemene rechten

De rechten in deze sectie zijn van toepassing op meerdere objecttypen. Voor veel van deze rechten is er ook een equivalent eigendomsrecht. Eigendomsrechten hebben alleen betrekking op de eigenaar van het object waarvoor rechten worden gecontroleerd.

De volgende rechten zijn alleen van toepassing op objecten die kunnen worden gepland:

- Het recht *De uitvoering van het document plannen*
- Het recht *Plannen namens andere gebruikers*
- Het recht *Plannen naar doelen*
- Het recht *Documentexemplaren weergeven*
- Het recht *Exemplaren verwijderen*
- Het recht *Documentexemplaren onderbreken en hervatten*
- Het recht *Exemplaren opnieuw plannen*

Recht	Beschrijving
Objecten weergeven	Hiermee kunt u objecten en hun eigenschappen weergeven. Als u niet over dit recht beschikt voor een object, wordt het object verborgen in het BI-platformsysteem. Dit recht is een basisrecht, dat vereist is voor alle taken.
Objecten toevoegen aan de map	Hiermee kunt u objecten toevoegen aan een map. Dit recht is ook van toepassing op objecten die zich als mappen gedragen, zoals Postvakken IN, de map `Favorieten` en objectpakketten.
Objecten bewerken	Hiermee kunt u de inhoud van een object en de eigenschappen van objecten en mappen bewerken.

Recht	Beschrijving
Rechten van gebruikers voor objecten wijzigen	Hiermee kunt u de beveiligingsinstellingen voor een object wijzigen.
De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen	Hiermee kunt u rechten of toegangsniveaus u hebt voor een object, toekennen aan anderen. U hebt hiervoor dit recht nodig voor de gebruiker en het object zelf. Zie het hoofdstuk "Rechten instellen" in de*Beheerdershandleiding voor SAP BusinessObjects Business Intelligence-platform* voor meer informatie over dit recht.
Servergroepen definiëren voor het verwerken van taken	Hiermee kunt u aangeven welke servergroep moet worden gebruikt wanneer objecten worden verwerkt. Dit recht is alleen van toepassing op objecten waarvoor u verwerkingsservers kunt opgeven. Als u een servergroep wilt opgeven, hebt u ook het recht *Objecten bewerken* nodig voor het object.
Objecten verwijderen	Hiermee kunt u objecten en hun exemplaren verwijderen.
Objecten kopiëren naar een andere map	Hiermee kunt u kopieën van objecten maken in andere mappen in de CMS. U hebt hiervoor ook het recht *Objecten aan de map toevoegen* nodig voor de doelmap. **Opmerking** Wanneer een object is gekopieerd, wordt de expliciete beveiliging van het object niet gekopieerd; het nieuwe object neemt de beveiligingsinstellingen van de doelmap over, maar beveiliging moet expliciet opnieuw worden ingesteld.
Inhoud herhalen	Hiermee kunt u objecten herhalen naar een ander systeem in een implementatie waarin Federatie is geactiveerd.
De uitvoering van het document plannen	Hiermee kunt u objecten plannen.
Plannen namens andere gebruikers	Hiermee kunt u objecten plannen voor andere gebruikers of groepen. De gebruiker of groep waarvoor u het object plant, wordt de eigenaar van het objectexemplaar. Als u een object voor andere gebruikers of groepen wilt plannen, hebt u ook de volgende rechten nodig: • Dit recht voor de gebruiker of groep. • Het recht *De uitvoering van het document plannen* voor het object
Plannen naar doelen	*Plannen naar doelen* is het bovenliggende recht van *Plannen naar FTP, SMTP, Postvak IN van BI, SFTP* en

Recht	Beschrijving
	Bestandssysteem. U moet het recht *Plannen naar doelen* selecteren in combinatie met het specifieke onderliggende recht om een object naar een specifiek doel te plannen. Bijvoorbeeld: selecteer de rechten *Plannen naar doelen* en *Plannen naar FTP* om een object naar een FTP-doel te plannen. Als u het BI-landschap bijwerkt vanuit BI 4.2 SP04 of een eerdere versie naar BI 4.2 SP05 of een latere versie, raadpleegt u SAP Notes 2675734, 2642221, 2626550 voor meer informatie over probleemoplossingen. Als u een object naar een ander doel wilt plannen, hebt u ook de volgende rechten nodig: • Het recht *De uitvoering van het document plannen* voor het gewenste object • Het recht *Objecten aan de map toevoegen* voor het Postvak IN van de ontvanger (als het doel een Postvak IN is) • Het recht *Objecten kopiëren naar een andere map* voor het gewenste object (als u een kopie naar een Postvak IN wilt sturen in plaats van een snelkoppeling) **Opmerking** Als het recht *Plannen naar doel* wordt toegewezen via een *Toegangsniveau* zoals de rollen *Volledig beheer* of *Plannen* in BI 4.2 SP04 of een eerdere versie, worden na een update naar BI 4.2 SP05 patch 03 of een latere versie de onderliggende doelrechten zoals *Plannen naar FTP, SMTP, SFTP, Postvak IN van BI* en *Bestandssysteem* ook toegekend. Voor *Toegangsniveaus* zoals *Weergeven op aanvraag* en bestaande rollen van het type *Aangepast* in BI 4.2 SP04 of een eerdere versie, worden na een update naar BI 4.2 SP05 patch 03 of een latere versie de onderliggende doelrechten niet standaard toegekend. U moet de rechten handmatig toekennen. Met de taak voor terugkerende planning die is gemaakt in BI 4.2 SP04 of een eerdere versie, worden objecten dus gepland in BI 4.2 SP05 patch 03 of een latere versie.
Plannen naar FTP	Hiermee kunt u een object naar een FTP-doel plannen.
Plannen naar SFTP	Hiermee kunt u een object naar een SFTP-doel plannen.
Plannen naar SMTP	Hiermee kunt u een object naar een SMTP-doel plannen.
Plannen naar bestandssysteem	Hiermee kunt u een object naar een bestandssysteemdoel plannen.
Plannen naar Postvak IN van BI	Hiermee kunt u een object naar een Postvak IN van BI-doel plannen.

Recht	Beschrijving
Documentexemplaren weergeven	Hiermee kunt u objectexemplaren weergeven. Dit recht is een basisrecht, dat vereist is voor alle taken die u uitvoert op objectexemplaren.
Exemplaren verwijderen	Hiermee kunt u alleen objectexemplaren verwijderen. Als u over het recht *Objecten verwijderen* beschikt, hebt u dit recht niet nodig voor het verwijderen van objectexemplaren.
Documentexemplaren onderbreken en hervatten	Hiermee kunt u actieve documentexemplaren onderbreken en hervatten.
Exemplaren opnieuw plannen	Hiermee kunt u objectexemplaren opnieuw plannen.
Opmerkingen toevoegen - BI-commentaar	Hiermee kan een gebruiker opmerkingen toevoegen aan een document met behulp van BI-commentaar.
Opmerkingen verwijderen - BI-commentaar	Hiermee kan een gebruiker opmerkingen verwijderen uit een document met behulp van BI-commentaar.
Door de gebruiker gecreëerde opmerkingen verwijderen - BI-commentaar	Hiermee kan een gebruiker door hemzelf gecreëerde opmerkingen verwijderen uit een document met behulp van BI-commentaar.
Opmerkingen wijzigen - BI-commentaar	Hiermee kan een gebruiker opmerkingen wijzigen in een document met behulp van BI-commentaar.
Door de gebruiker gecreëerde opmerkingen wijzigen - BI-commentaar	Hiermee kan een gebruiker door hemzelf gecreëerde opmerkingen wijzigen in een document met behulp van BI-commentaar.
Opmerkingen weergeven - BI-commentaar	Hiermee kan een gebruiker opmerkingen weergeven in een document met behulp van BI-commentaar.
Door de gebruiker gecreëerde opmerkingen weergeven - BI-commentaar	Hiermee kan een gebruiker door hemzelf gecreëerde opmerkingen weergeven in een document met behulp van BI-commentaar.
Opmerkingen verbergen - BI-commentaar	Hiermee kan een gebruiker opmerkingen verbergen in een document met behulp van BI-commentaar.

Recht	Beschrijving
Door de gebruiker gecreëerde opmerkingen verbergen - BI-commentaar	Hiermee kan een gebruiker door hemzelf gecreëerde opmerkingen verbergen in een document met behulp van BI-commentaar.
Opmerkingen tegelijk toevoegen - BI-commentaar	Hiermee kan een gebruiker de opmerkingen samen met het document migreren.

34.2.1 Doelrechten

Elk doel is gekoppeld aan een specifiek doelrecht. De BOE-beheerder moet ervoor zorgen dat de gebruikers de gewenste doelrechten hebben.

Voorheen kon een gebruiker met het recht *Plannen naar doelen* plannen naar alle beschikbare doelen.
Met ingang van release SP05 krijgen gebruikers individuele doelrechten, waarbij *Plannen naar doelen* alleen overeenkomt met *Standaard Enterprise-locatie*.

Nieuwe rechten worden geïntroduceerd onder de Algemene rechten voor elk doel:

- Plannen naar bestandssysteem
- Plannen naar FTP
- Plannen naar Postvak IN
- Plannen naar SFTP
- Plannen naar SMTP
- Plannen naar Google Drive

Zie Algemene rechten [pagina 1133] voor meer informatie over *Algemene rechten*.

De beheerder moet de respectieve individuele doelrechten aan gebruikers verlenen om deze doelopties te kunnen bieden. Zie 2621878. Als de gebruiker alleen het recht voor *Plannen naar doelen* heeft, kan die niet plannen naar de doelen FTP, Postvak IN, SFTP, SMTP en Bestandssysteem.

Als het recht *Plannen naar doelen* in een eerdere versie is toegewezen via Toegangsniveau, zoals met de rollen Volledig beheer of Plannen, worden na een upgrade naar 4.2 SP05 ook aanvullende (nieuw geïntroduceerde) rechten verleend. Dat betekent dat plannen naar elk doel zal slagen.

Als het recht is toegewezen via het toegangsniveau *Weergeven op aanvraag*, via een aangepaste rol of direct is toegewezen (individueel recht, geen rol), gaan alleen Plannen naar *Standaard Enterprise-locatie* door, en mislukken de andere doelen.

Zie Opties voor doelen en Eigenschappen van het e-maildoel voor meer informatie.

34.3 Rechten voor specifieke objecttypen

34.3.1 Maprechten

Als u het beheer van rechten wilt vereenvoudigen, is het raadzaam om rechten in te stellen voor mappen, zodat beveiligingsinstellingen worden overgenomen door de inhoud van de mappen. Maprechten bestaan uit:

- Algemene rechten voor het mapobject
- Typespecifieke rechten voor de mapinhoud (bijvoorbeeld het recht *De rapportgegevens afdrukken* voor Crystal Reports-rapporten)

34.3.2 Categorieën

De rechten in deze sectie zijn algemene rechten die een specifieke betekenis hebben in de context van openbare en persoonlijke categorieën.

> **Opmerking**
>
> Objecten in categorieën nemen geen rechten over die zijn ingesteld voor de categorieën.

Recht	Beschrijving
Objecten toevoegen aan de map	Hiermee maakt u nieuwe categorieën in categorieën. U hebt dit recht niet nodig om objecten toe te voegen aan een categorie.
Objecten bewerken	Hiermee kunt u het volgende doen: • De eigenschappen van categorieën wijzigen • De categorie in een andere categorie plaatsen als subcategorie • Objecten toevoegen aan de categorie • Objecten uit een categorie verwijderen Als u een categorie in een andere categorie wilt plaatsen als subcategorie, hebt u ook de volgende rechten nodig: • Het recht *Objecten verwijderen* voor de oorspronkelijke categorie • Het recht *Objecten toevoegen aan de map* voor de doelcategorie
Objecten verwijderen	Hiermee kunt u de categorie verwijderen.

34.3.3 Crystal Reports-rapporten

De rechten in deze sectie zijn alleen van toepassing op Crystal Reports-rapporten.

> **Opmerking**
>
> Deze rechten gelden uitsluitend voor Crystal Reports-rapporten in de BI-platformomgeving. Wanneer u Crystal Reports-rapporten naar een lokale schijf downloadt, hebben deze rechten geen effect. Om dit te voorkomen, kunt u het recht *Bestanden downloaden die zijn gekoppeld aan het object* weigeren voor het Crystal Reports-rapport.

Recht	Beschrijving
De rapportgegevens afdrukken	Hiermee kunt u het rapport afdrukken.
De gegevens van het rapport vernieuwen	Hiermee kunt u rapportgegevens vernieuwen.
De gegevens van het rapport exporteren	Hiermee kunt u rapportgegevens naar elke gewenste indeling exporteren wanneer u het rapport online weergeeft in de Crystal Reports-viewer. Als u rapportgegevens in RPT-indeling wilt exporteren, hebt u ook het recht *Bestanden downloaden die zijn gekoppeld aan het object* nodig.
Bestanden downloaden die zijn gekoppeld aan het object	Hiermee kunt u het volgende doen: • Het rapport exporteren in RPT-indeling • Het rapport openen in Crystal Reports Designer • Het rapport in RPT-indeling plannen naar externe doelen

34.3.4 Web Intelligence-documenten

De rechten in deze sectie zijn alleen van toepassing op Web Intelligence-documenten.

Recht	Beschrijving
Zoeklijsten gebruiken	Hiermee kunt u zoeklijsten gebruiken.
De rapportgegevens exporteren	Met deze opdracht kan een gebruiker rapportgegevens exporteren naar Tekst-, CSV-, Excel-, PDF- of HTML-indeling. Hiermee kunt u ook de afdrukopdracht gebruiken die een PDF-document genereert dat u kunt afdrukken.
Queryscript - weergeven inschakelen (SQL, MDX...)	Hiermee kunt u queryscripts weergeven (SQL en MDX).
Queryscript - bewerken inschakelen (SQL , MDX...)	Hiermee kunt u queryscripts bewerken (SQL en MDX). U kunt ook vrije SQL (FHSQL)-gegevensbronnen bewerken.

Recht	Beschrijving
Rapportgegevens vernieuwen	Hiermee kunt u documentgegevens vernieuwen.
Query bewerken	Hiermee kunt u query's in het document bewerken.
Zoeklijst vernieuwen	Hiermee kunt u zoeklijsten voor aanwijzingen vernieuwen tijdens het maken van de aanwijzing of tijdens het weergeven van het document. U hebt hiervoor ook het recht *Zoeklijsten gebruiken* nodig voor het document.
Verzenden naar	Hiermee kunt u documenten als hyperlinks in een e-mail verzenden, of naar de Scheduler of naar een Postvak IN van het BI-platform verzenden. Met dit recht kunnen gebruikers van Web Intelligence Rich Client ook documenten als e-mailbijlagen verzenden.

34.3.5 Gebruikers en groepen

U kunt rechten instellen voor gebruikers en groepen zoals u dit ook zou doen voor andere objecten in de BI-platformomgeving. De rechten in deze sectie zijn typespecifieke rechten die uitsluitend van toepassing zijn op gebruikers en groepen of algemene rechten die een specifieke betekenis hebben in de context van gebruikers en groepen.

> ⓘ Opmerking
>
> Gebruikers en subgroepen kunnen rechten overnemen van groeplidmaatschappen.

> ⓘ Opmerking
>
> Degene die een gebruikersaccount heeft gemaakt, wordt beschouwd als de eigenaar van de account. Nadat de gebruikersaccount echter is gemaakt, wordt de gebruiker voor wie de account is gemaakt ook als eigenaar beschouwd.

Recht	Beschrijving
Objecten bewerken	Hiermee kunt u het volgende doen: • Eigenschappen van de gebruiker of groep bewerken • Groepslidmaatschap beheren Als u een gebruiker of groep aan een andere groep wilt toevoegen, hebt u dit recht nodig voor de gebruiker of de groep en voor de doelgroep.

Recht	Beschrijving
Gebruikerswachtwoord wijzigen	Hiermee kunt u het volgende doen: • Het wachtwoord van uw gebruikersaccount wijzigen. U hebt hiervoor ook het recht *Objecten bewerken* voor uw gebruikersaccount nodig. • Het wachtwoord van de account van een andere gebruiker wijzigen. Hiertoe hebt u ook het recht *Objecten bewerken* en *Rechten van gebruikers voor objecten wijzigen* nodig voor de gebruikersaccount. **Opmerking** Dit recht heeft geen invloed op de volgende wachtwoordinstellingen: *Wachtwoord verloopt nooit* *Gebruiker moet wachtwoord bij volgende aanmelding wijzigen* *Gebruiker kan wachtwoord niet wijzigen* **Opmerking** Dit recht is niet van toepassing op gegevensbronreferenties voor SAP BusinessObjects-universes.
Abonneren op publicaties	Hiermee kunt u de gebruiker aan de publicatie toevoegen als ontvanger.
Plannen namens andere gebruikers	Hiermee kunt u objecten plannen namens een gebruiker, zodat deze de eigenaar van het objectexemplaar wordt. U hebt hiervoor ook het recht *Plannen namens andere gebruikers* nodig voor het object.
Gebruikersattributen toevoegen of bewerken	Hiermee kunt u de waarde van het e-mailadres van een gebruiker of aangepaste gebruikersattributen wijzigen. Dit recht is van toepassing op gebruikers.
Gebruikersattributen toevoegen of bewerken (recht van eigenaar)	HIermee kan de eigenaar van een gebruikersobject de waarde van het e-mailadres van de gebruiker of aangepaste gebruikersattributen wijzigen. Dit recht is van toepassing op gebruikers.
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu Voorkeuren te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid

Recht	Beschrijving
	(inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

34.3.6 Toegangsniveaus

De rechten in deze sectie zijn alleen van toepassing op toegangsniveaus.

Recht	Beschrijving
Toegangsniveau gebruiken voor beveiligingstoewijzing	Hiermee kunt u het toegangsniveau toewijzen wanneer u principals toevoegt aan ACL's voor objecten. Hiertoe hebt u ook het recht *Rechten van gebruikers voor objecten wijzigen* of *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* nodig voor de principal en het object. In geval het recht *De rechten die gebruikers hebben voor objecten, op een veilige manier wijzigen* is toegekend, moet hetzelfde toegangsniveau ook aan uzelf zijn toegekend voor het object.

34.3.7 Universe-rechten (.unv)

De rechten in deze sectie zijn van toepassing op universes gemaakt met het hulpprogramma voor universe-ontwerp of UNV-universes. De vermelde rechten zijn typespecifieke rechten die uitsluitend van toepassing zijn op universes of algemene rechten die een specifieke betekenis hebben in de context van universes.

> **Opmerking**
>
> Universe-rechten zijn alleen van toepassing wanneer u universes van de CMS naar het hulpprogramma voor universe-ontwerp importeert. Deze rechten zijn niet van toepassing wanneer de universe is opgeslagen op een lokale schijf.

Recht	Beschrijving
Objecten toevoegen aan de map	Hiermee kunt u toegangsbeperkingen en objecten toevoegen aan de universe. U hebt hiervoor ook het recht *Toegangsbeperkingen bewerken* nodig.
Objecten weergeven	Hiermee hebt u toegang tot de universe en kunt u deze bekijken.
Objecten bewerken	Hiermee kunt u het volgende doen:

Recht	Beschrijving
	• De universe in de CMC of in het hulpprogramma voor universe-ontwerp bewerken. • De universe vergrendelen en vergrendeling opheffen Als u de vergrendeling van een universe wilt opheffen, hebt u ook het recht *Universe ontgrendelen* nodig.
Objecten verwijderen	Hiermee kunt u de universe verwijderen.
Objecten vertalen	Hiermee kunt u vertaalde universe-objectnamen opslaan met het hulpprogramma voor vertaalbeheer. **Opmerking** U kunt de vertalingen ook opslaan als het recht *Objecten bewerken* expliciet aan u is toegewezen, zolang het recht *Objecten vertalen* niet expliciet wordt genegeerd.
Nieuwe zoeklijst	Hiermee kunt u het volgende doen: • Nieuwe zoeklijsten aan objecten koppelen • Bestaande zoeklijsten bewerken **Opmerking** Dit recht voorkomt niet dat u trapsgewijze zoeklijsten kunt maken.
Universe afdrukken	Hiermee kunt u de universe afdrukken.
Tabel- of objectwaarden tonen	Hiermee kunt u de waarden weergeven die zijn gekoppeld aan tabellen of objecten in de universe.
Toegangsbeperkingen bewerken	Hiermee kunt u toegangsbeperkingen (overloads) voor de universe bewerken.
Universe ontgrendelen	Hiermee kunt u het volgende doen: • De universe ontgrendelen als deze is vergrendeld door een andere gebruiker • De universe uit de CMS exporteren Als u de vergrendeling van een universe wilt opheffen, hebt u ook het recht *Objecten bewerken* nodig.
Gegevenstoegang	Hiermee kunt u gegevens ophalen uit de universe en documenten vernieuwen die op de universe zijn gebaseerd. U hebt dit recht hiertoe ook nodig voor het hulpprogramma voor universe-ontwerp, het document en de universe-verbinding.

Recht	Beschrijving
Query's maken en bewerken op basis van universe	Hiermee kunt u documenten maken en query's bewerken die op de universe zijn gebaseerd.

34.3.8 Universe-rechten (.unx)

De rechten in deze sectie zijn van toepassing op universes gemaakt met het hulpprogramma voor informatieontwerp of UNV-universes. De vermelde rechten zijn typespecifieke rechten die uitsluitend van toepassing zijn op universes of algemene rechten die een specifieke betekenis hebben in de context van universes.

> **Opmerking**
>
> Universe-rechten zijn alleen van toepassing op universes die naar een gegevensopslagruimte zijn gepubliceerd. Deze rechten zijn niet van toepassing wanneer de universe is opgeslagen in een lokale map.

Recht	Beschrijving
Objecten weergeven	Hiermee hebt u toegang tot de universe en kunt u deze bekijken.
Objecten bewerken	Hiermee kunt u de universe opnieuw publiceren.
Objecten verwijderen	Hiermee kunt u de universe verwijderen.
Universe ophalen	Hiermee kunt u een gepubliceerde universe ophalen en de onderliggende bronnen (bedrijfslaag en gegevensverzameling) bewerken in het hulpprogramma voor informatieontwerp. **Opmerking** Voor het hulpprogramma voor informatieontwerp moet het toepassingsrecht *Universes ophalen* verleend zijn.
Beveiligingsprofielen bewerken	Hiermee kunt u beveiligingsprofielen invoegen, bewerken en verwijderen voor de universe in de beveiligingseditor van het hulpprogramma voor informatieontwerp. **Opmerking** Dit recht is niet vereist voor het bekijken van beveiligingsprofielen of het wijzigen van aggregatieopties voor beveiligingsprofielen.

Recht	Beschrijving
Beveiligingsprofielen toewijzen	Hiermee kunt u beveiligingsprofielen toewijzen en ongedaan maken voor gebruikers en groepen in de beveiligingseditor van het hulpprogramma voor informatieontwerp.
Gegevenstoegang	Hiermee kunt u gegevens ophalen uit de universe en documenten vernieuwen die op de universe zijn gebaseerd. In het hulpprogramma voor informatieontwerp kunt u met dit recht een voorbeeld van de resultatenreeks bekijken in het queryvenster.
Query's maken en bewerken op basis van deze universe	Hiermee kunt u query's maken en bewerken die op de universe zijn gebaseerd. In het hulpprogramma voor informatieontwerp kunt u met dit recht het queryvenster openen en een query over de universe uitvoeren.
Opslaan voor alle gebruikers	Hiermee kunt u de universe voor alle gebruikers opslaan. **Opmerking** Voor het hulpprogramma voor informatieontwerp moet ook het toepassingsrecht *Opslaan voor alle gebruikers* aan u verleend zijn.

34.3.9 Toegangsniveaus voor universe-objecten

Wanneer gebruikers een universe maken met behulp van het hulpprogramma voor universe-ontwerp of een bedrijfslaag met het hulpprogramma voor informatieontwerp wordt er toegang op objectniveau toegewezen aan elk object in de universe. De toegangsniveaus voor objecten zijn:

Openbaar (standaard)
Beheerd
Beperkt
Vertrouwelijk
Persoonlijk

Zodra de universe in de gegevensopslagruimte gepubliceerd is, kunt u toegang verlenen aan universe-objecten op basis van toegangsniveaus voor objecten die zijn toegewezen in de toepassing. U kunt bijvoorbeeld het toegangsniveau Openbaar toewijzen aan de groep Iedereen. Hiermee kunnen gebruikers in de groep Iedereen de objecten zien in de universe die als Openbaar gekenmerkt is.

Elk toegangsniveau voor objecten biedt meer beveiligingsinstellingen dan het vorige niveau. Openbaar is het laagste niveau. Principals waaraan het toegangsniveau Openbaar verleend is, kunnen alleen objecten zien die als Openbaar gekenmerkt zijn. Principals waaraan het toegangsniveau Beheerd verleend is, kunnen objecten zien die als Openbaar of als Beheerd gekenmerkt zijn. Privé is het hoogste beveiligingsniveau en verleent principals toegang tot alle toegangsniveaus voor objecten, oftewel alle objecten in de universe.

> **Opmerking**
>
> Beveiligingsinstellingen voor toegang op objectniveau prevaleren boven beveiligingsinstellingen die door de universe zijn overgenomen.

> **Opmerking**
>
> Voor UNX-universes wordt er rekening gehouden met de beveiligingsinstellingen voor toegang op objectniveau en met de objectbeveiliging die door het beveiligingsprofiel is gedefinieerd. Zie de *Gebruikershandleiding Hulpprogramma voor informatieontwerp* voor meer informatie over beveiligingsprofielen.

Verwante informatie

Toegangsniveaus voor universe-objecten toewijzen [pagina 1146]

34.3.9.1 Toegangsniveaus voor universe-objecten toewijzen

Als u beveiliging voor universe-objecten wilt instellen op objectniveau, hebt u het recht *Rechten van gebruikers voor objecten wijzigen* nodig voor de universe.

1. Selecteer de universe in het gebied *Universes* van de CMS.
2. Klik op *Actie* > *Universe-beveiliging*.
3. In het dialoogvenster *Universe-beveiliging* voor de gebruiker of groep, selecteert u het toegangsniveau voor objecten in de keuzelijst *Beveiliging op objectniveau*

34.3.10 Verbindingsrechten

De rechten in deze sectie zijn typespecifieke rechten die van toepassing zijn op universe-verbindingen of algemene rechten die een specifieke betekenis hebben in de context van universe-verbindingen. Deze rechten zijn van toepassing op verbindingen die in de gegevensopslagruimte zijn gepubliceerd.

Relationele verbindingsrechten

Recht	Beschrijving
Objecten weergeven	Hiermee kunt u de verbinding weergeven.
Objecten bewerken	Hiermee kunt u de verbindingsparameters bewerken.

Recht	Beschrijving
Verbinding lokaal downloaden	Hiermee kunt u universes die op de verbinding in Web Intelligence Rich Client zijn gemaakt, in offline-modus gebruiken. Hiermee kunt u het lokale middleware-stuurprogramma in het hulpprogramma voor informatieontwerp gebruiken. Hiervoor selecteert u de lokale middleware-optie in de voorkeuren van het hulpprogramma voor informatieontwerp, omdat query's bij de database anders de servermiddleware gebruiken. U hebt dit recht ook nodig om een beveiligde verbinding in het hulpprogramma voor informatieontwerp te bewerken.
Objecten verwijderen	Hiermee kunt u de verbinding verwijderen.
Objecten kopiëren naar een andere map	Hiermee kunt u de verbinding van de ene map naar de andere kopiëren.
Gegevenstoegang	Hiermee kunt u inhoud ophalen uit de database die voor de verbinding is opgegeven. In het hulpprogramma voor informatieontwerp kunt u met dit recht door de tabelgegevens van de verbinding en de editors van gegevensverzamelingen bladeren. Hiermee kunt u ook een voorbeeld van de resultatenreeks weergeven in het queryvenster.
Verbinding gebruiken voor databaseprocedures	Hiermee kunt u de databaseprocedures gebruiken in de database die voor de universeverbinding is opgegeven. **Opmerking** Dit recht is alleen van toepassing op UNV-universes.
Verbinding gebruiken voor vrije SQL-scripts	Hiermee kunt u SQL-scripts op de verbinding uitvoeren.

OLAP-verbindingsrechten

Recht	Beschrijving
Objecten weergeven	Hiermee kunt u de verbinding weergeven.
Objecten bewerken	Hiermee kunt u de verbindingsparameters bewerken in de verbindingseditor van het hulpprogramma voor informatieontwerp.

Recht	Beschrijving
Objecten verwijderen	Hiermee kunt u de verbinding verwijderen.
Objecten kopiëren naar een andere map	Hiermee kunt u de verbinding van de ene map naar de andere kopiëren.
Verbinding lokaal downloaden	Hiermee kunt u universes die op de verbinding in Web Intelligence Rich Client zijn gemaakt, in offline-modus gebruiken.

34.3.11 Toepassingen

34.3.11.1 CMC

Recht	Beschrijving
Aanmelden bij de CMC en dit object in de CMC weergeven	Hiermee kan een gebruiker zich bij de CMC aanmelden
Toegang toestaan tot exemplaarbeheer	Hiermee krijgt een gebruiker toegang tot Exemplaarbeheer
Toegang toestaan tot relatiequery	Hiermee kan een gebruiker relatiequery's uitvoeren in de CMC
Toegang toestaan tot beveiligingsquery	Hiermee kan een gebruiker beveiligingsquery's uitvoeren in de CMC

34.3.11.2 Aan SAP Fiori aangepast BI-startpunt

Recht	Beschrijving
Aanmelden bij aan SAP Fiori aangepast BI-startpunt	Hiermee kan een gebruiker zich aanmelden bij het aan SAP Fiori aangepaste BI-startpunt
Ordenen	Hiermee kan een gebruiker objecten verplaatsen en kopiëren, objecten aan de map `Favorieten` toevoegen en snelkoppelingen naar objecten maken
Verzenden naar Postvak IN van Business Objects	Hiermee kan een gebruiker objecten naar de Postvakken IN van ontvangers in BI verzenden
Verzenden naar e-maildoel	Hiermee kan een gebruiker objecten naar ontvangers verzenden via e-mail

Recht	Beschrijving
Verzenden naar bestandslocatie	Hiermee kan een gebruiker objecten naar een bestandslocatie verzenden
Verzenden naar FTP-locatie	Hiermee kan een gebruiker objecten naar een FTP-locatie verzenden
Verzenden naar SFTP-locatie	Hiermee kan een gebruiker objecten naar een SFTP-locatie verzenden. SFTP-doel heeft soortgelijke eigenschappen als de FTP-doelpagina met een aanvullende fingerprintoptie die door de gebruiker moet worden opgegeven. De fingerprintoptie is bij elke SFTP-server beschikbaar in de eigenschappen. Matching/validatie van de fingerprint wordt in de backend uitgevoerd door CMS.

34.3.11.2.1 Rechten voor samenwerkingstoepassingen

Deze rechten zijn van toepassing op SAP Jam, als de toepassing in het BI-platform wordt geconfigureerd.

Recht	Beschrijving
Opmerkingen maken over documenten van eigenaar	Hiermee kan een gebruiker commentaar geven op documenten en exemplaren waarvan de gebruiker eigenaar is
Opmerkingen weergeven over documenten van eigenaar	Hiermee kan een gebruiker commentaar op documenten en exemplaren waarvan de gebruiker eigenaar is, weergeven
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing.

34.3.11.3 BI-werkruimten

Recht	Beschrijving
BI-werkruimten maken en bewerken	Hiermee kan een gebruiker nieuwe BI-werkruimten maken en bestaande BI-werkruimten bewerken
Modules maken en bewerken	Hiermee kan een gebruiker nieuwe modules maken en bestaande modules bewerken
BI-werkruimten bewerken	Hiermee kan een gebruiker bestaande BI-werkruimten bewerken (maar stelt een gebruiker niet in staat om nieuwe werkruimten te maken)
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

34.3.11.4 Web Intelligence

De toegangsrechten in deze sectie zijn van toepassing op de toepassing SAP BusinessObjects Web Intelligence (inclusief de Rich Client) en kunnen van invloed zijn op de viewers en queryvensters in deze toepassing.

Recht	Beschrijving
Gegevens: Gegevenstracering inschakelen	Hiermee kan een gebruiker gewijzigde gegevens traceren.
Gegevens: Opmaak van gewijzigde gegevens inschakelen	Hiermee kan een gebruiker een opmaak selecteren voor gewijzigde gegevens.
Algemeen: Toegang tot Desktop-client inschakelen	Hiermee kan een gebruiker Web Intelligence Desktop (Rich Client) gebruiken.
Desktop: Documenten exporteren	Hiermee kan een gebruiker in Web Intelligence Rich Client documenten exporteren naar de gegevensopslagruimte in het BI-platform.
Desktop: Documenten voor alle gebruikers opslaan	Hiermee kan een gebruiker in Web Intelligence Rich Client documenten lokaal en zonder beveiliging opslaan.
Documenten: Automatisch vernieuwen bij openen uitschakelen	Hiermee wordt voorkomen dat documenten, wanneer ze worden geopend, automatisch worden vernieuwd.

Recht	Beschrijving
Documenten: Automatisch opslaan inschakelen	Hiermee wordt het automatisch opslaan van documenten ingeschakeld, als automatisch opslaan in de CMC is geactiveerd door de beheerder.
Documenten: Maken inschakelen	Hiermee kan een gebruiker nieuwe documenten maken.
Algemeen: Voorkeuren voor Web Intelligence bewerken	Hiermee kan een gebruiker voorkeuren voor Web Intelligence in het BI-startpunt wijzigen.
Algemeen: Toegang tot webclient inschakelen	Hiermee kan een gebruiker de webclient Web Intelligence gebruiken.
Query: script bewerken dat uit universe is gegenereerd	Hiermee kan een gebruiker in het queryvenster de SQL- of MDX-queryscripts bewerken die uit de universe zijn gegenereerd.
Query: Vrije SQL bewerken	Hiermee kan een gebruiker vrije-SQL-queryscripts bewerken.
Query: script weergeven dat uit universe is gegenereerd	Hiermee kan een gebruiker in het queryvenster de SQL- of MDX-queryscripts weergeven die uit de universe zijn gegenereerd.
Query: Vrije SQL weergeven	Hiermee kan een gebruiker vrije-SQL-queryscripts weergeven.
Rapportage: Onderverdelingen maken en bewerken	Hiermee kan een gebruiker onderverdelingen maken en bewerken.
Rapportage: Regels voor voorwaardelijke opmaak maken en bewerken	Hiermee kan een gebruiker regels voor voorwaardelijke opmaak maken en bewerken.
Rapportage: Vooraf gedefinieerde berekeningen maken en bewerken	Hiermee kan een gebruiker vooraf gedefinieerde berekeningen maken en bewerken.
Rapportage: Invoerbesturingselementen en groepen maken en bewerken	Hiermee kan een gebruiker invoerbesturingselementen maken en bewerken.
Rapportage: Rapportfilters maken en bewerken en invoerbesturingselementen gebruiken	Hiermee kan een gebruiker rapportfilters maken en bewerken en de invoerbesturingselementen gebruiken.
Rapportage: Sorteerbewerkingen en classificaties maken en bewerken	Hiermee kan een gebruiker sorteerbewerkingen en classificaties maken en bewerken.
Rapportage: Formules, variabelen, groepen en verwijzingen maken	Hiermee kan een gebruiker formules, variabelen, groepen en verwijzingen maken.
Rapportage: Documentwijziging inschakelen	Hiermee kan een gebruiker de opmaak van rapporten bewerken. Zonder dit toegangsrecht is de Ontwerp-modus niet beschikbaar
Rapportage: Objecten samenvoegen	Hiermee kan een gebruiker met behulp van samengevoegde dimensies gegevens in rapporten en in gegevensbeheer synchroniseren.

Recht	Beschrijving
Rapportage: Rapporten, tabellen, diagrammen en cellen invoegen en verwijderen	• Hiermee kan een gebruiker rapporten, tabellen, diagrammen en cellen invoegen en verwijderen. • Hiermee wordt de dupliceringswerkstroom ingeschakeld (kopiëren/plakken).

34.3.11.5 Hulpprogramma voor universeontwerp

Recht	Beschrijving
Universe-integriteit controleren	Hiermee kan een gebruiker de integriteit van universes controleren
Structuurvenster vernieuwen	Hiermee kan een gebruiker het structuurvenster vernieuwen
Tabelbrowser gebruiken	Hiermee kan een gebruiker databasegegevens bekijken met behulp van de tabelbrowser
Universebeperkingen toepassen	Hiermee kan een gebruiker vooraf gedefinieerde universebeperkingen toepassen op gebruikers van een geïmporteerde universe.
Universe koppelen	Hiermee kan een gebruiker twee universes koppelen en de onderdelen delen
Verbindingen maken, wijzigen of verwijderen	Hiermee kan een gebruiker universe-verbindingen maken, wijzigen en verwijderen die in de gegevensopslagruimte van het BI-platform zijn opgeslagen als persoonlijke of gedeelde verbindingen
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

34.3.11.6 Hulpprogramma voor informatieontwerp

Recht	Beschrijving
Beveiligingsprofielen beheren	Hiermee kan een gebruiker de beveiligingseditor openen Als u met beveiligingsprofielen wilt werken, moet u ook rechten hebben voor de universe.
Projecten delen	Hiermee kan een gebruiker een lokaal project delen en een gedeeld project synchroniseren met het lokale project
Verbindingen maken, wijzigen of verwijderen	• Hiermee kan een gebruiker beveiligde verbindingen maken in en verwijderen uit de weergave Gepubliceerde bronnen • Hiermee kan een gebruiker verbindingen bewerken in de verbindingseditor • Hiermee kan een gebruiker verbindingen naar een gegevensopslagruimte publiceren
Universes publiceren	Hiermee kan een gebruiker universes naar een gegevensopslagruimte publiceren
Universes ophalen	Hiermee kan een gebruiker gepubliceerde universes ophalen in een lokaal project dat zal worden bewerkt
Opslaan voor alle gebruikers	Hiermee kan een gebruiker voor alle gebruikers opslaan bij het ophalen van universes
Statistieken berekenen	Hiermee kan een gebruiker tabellen en kolommen selecteren waarvoor statistieken moeten worden berekend en gepubliceerd
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

34.3.11.7 Meldingen

Recht	Beschrijving
Meldingen activeren	Hiermee kan een gebruiker meldingsgebeurtenissen activeren. Om een melding voor een document te activeren, zijn tevens de volgende rechten vereist: • De rechten "Weergeven" en "Plannen" voor het document • De rechten "Weergeven" en "Activeren" voor de bijbehorende gebeurtenis
Abonneren op objecten	Hiermee kan een gebruiker zich op een meldingsgebeurtenis abonneren. Om zich op een gebeurtenis te abonneren, zijn tevens de volgende rechten vereist: • Het recht "Weergeven" voor de bijbehorende gebeurtenis • Het recht "Abonneren" voor het eigen account van de gebruiker Om zich op een melding in een document te abonneren, zijn tevens de volgende rechten vereist: • Het recht "Weergeven" voor het document • Het recht "Exemplaar weergeven" voor het document • Het recht "Weergeven" voor de bijbehorende gebeurtenis • Het recht "Abonneren" voor het eigen account van de gebruiker
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

34.3.11.8 SAP BusinessObjects Mobile

Recht	Beschrijving
Aanmelden bij de SAP BusinessObjects Mobile-toepassing	Hiermee kan een gebruiker zich vanuit de Mobile-toepassing bij het BI-platform aanmelden en documenten bekijken
Abonneren op documentmeldingen	Hiermee kan een gebruiker zich abonneren op meldingen voor documenten en terugkerende exemplaren Als een gebruiker dit recht in het verleden heeft gehad, kan deze gebruiker nog steeds meldingen uit een abonnement ontvangen, zelfs als de gebruiker dit recht niet meer bezit. Gebruikers moeten het abonnement op een melding expliciet opzeggen als ze deze melding niet meer wilt ontvangen. Om zich te abonneren op documentmeldingen en terugkerende exemplaren voor planningen, moet een gebruiker het toegangsrecht "Volledig beheer" hebben voor de map `Systeemgebeurtenissen`, onder *Gebeurtenissen* in de CMC.
Documenten opslaan in lokale opslagruimte van apparaat	Hiermee kan een gebruiker documenten op een mobiel apparaat opslaan Als een gebruiker het recht "Documenten lokaal op het apparaat opslaan" in het verleden heeft gehad en documenten op het mobiele apparaat heeft opgeslagen, bestaan de documenten nog steeds op het apparaat (zelfs als de gebruiker dit recht niet meer heeft), maar worden ze niet gesynchroniseerd tijdens het synchronisatieproces.
Documenten vanaf apparaat verzenden als e-mail	Hiermee kan een gebruiker rapporten in een e-mailbericht versturen
Voorkeuren wijzigen voor objecten die de gebruiker bezit	Hiermee wordt het menu *Voorkeuren* weergegeven in een toepassingsobject Zonder dit toegangsrecht kan een gebruiker in geen enkele toepassing persoonlijke voorkeuren instellen en is er in toepassingen geen menu *Voorkeuren* te zien. Zonder dit recht kunnen gebruikers bijvoorbeeld geen maateenheid (inches of millimeters) selecteren om te gebruiken in rapporten in de toepassing Web Intelligence of BI-startpunt.

Zie de handleiding *SAP BusinessObjects Mobile installeren en implementeren* voor meer informatie.

34.3.11.9 Cockpit BI-beheerder

Rechten	Beschrijving
Toegang tot Cockpit BI-beheerder toestaan	Hiermee hebt u toegang tot Cockpit BI-beheerder in CMC
Toegang tot Toezicht toestaan	Hiermee hebt u toegang tot Toezicht in Cockpit BI-beheerder
Toegang tot Visueel verschil toestaan	Hiermee hebt u toegang tot Visueel verschil in Cockpit BI-beheerder
Visueel verschil - vergelijking maken	Hiermee kunt u nieuwe vergelijkingen maken tussen informatieobjecten in Visueel verschil
Visueel verschil - vergelijking verwijderen	Hiermee kunt u de vorige vergelijkingen in Visueel verschil verwijderen
Visueel verschil - vergelijking opnieuw uitvoeren	Hiermee kunt u de eerder gemaakte vergelijkingen opnieuw uitvoeren in Visueel verschil
Visueel verschil - vergelijking weergeven	Hiermee kunt u een vergelijking weergeven in Visueel verschil

35 Bijlage Servereigenschappen

35.1 Over de bijlage Servereigenschappen

In deze bijlage vindt u een overzicht en een beschrijving van de eigenschappen die voor de BI-platformservers kunnen worden ingesteld.

35.1.1 Algemene servereigenschappen

De servereigenschappen die in deze sectie aan de orde komen, zijn op alle servertypen van toepassing.

Poorteigenschappen aanvragen

Eigenschap	Beschrijving	Standaardwaarde
Servernaam	De naam van de server.	De standaardwaarde is de naam van het knooppunt waarop de server zich bevindt, plus de naam van de server.
ID, CUID	De korte id en de clusterunieke id van de server. Alleen-lezen.	Deze waarden worden automatisch gegenereerd.
Knooppunt	De naam van het knooppunt waar de server zich bevindt.	Deze waarde wordt opgegeven tijdens de installatie.
Beschrijving	De beschrijving van de server.	De standaardwaarde is de naam van de server.
Opdrachtregelparameters	De opdrachtregelparameters voor de server.	De standaardwaarde is afhankelijk van het type server.
Poort voor aanvragen	Hiermee wordt opgegeven via welke poort de server aanvragen ontvangt. In een omgeving met firewalls configureert u de server om naar aanvragen te luisteren op poorten die zijn geopend in de firewall. Als u een poort voor de server opgeeft, moet u ervoor zorgen dat de poort niet al in gebruik is door een ander proces. **Opmerking** Als *Automatisch toewijzen* is ingeschakeld, wordt de server gekoppeld aan een dynamisch toegewezen poort. Dit houdt in dat er een willekeurig poortnummer wordt toegewezen aan de server wanneer de server opnieuw wordt gestart.	Standaard is *Automatisch toewijzen* `ingeschakeld` en is *Poort voor aanvragen* leeg.

Eigenschap	Beschrijving	Standaardwaarde
Automatisch toewijzen	Hiermee wordt opgegeven of de server aan een dynamisch toegewezen poort wordt gebonden, wanneer de server opnieuw wordt gestart. Als u de server aan een specifieke poort wilt koppelen, schakelt u *Automatisch toewijzen* **`in`** en geeft u een geldige *poort voor aanvragen* op.	Standaard is deze optie**`ingeschakeld`**.

Eigenschappen voor automatisch starten

Eigenschap	Beschrijving	Standaardwaarde
Deze server automatisch starten wanneer Server Intelligence Agent wordt gestart	Geeft aan of de server automatisch moet worden gestart wanneer de Server Intelligence Agent (SIA) wordt gestart of opnieuw wordt gestart. Als deze optie is **`uitgeschakeld`** en de SIA wordt gestart of opnieuw gestart, wordt de server niet gestart.	De standaardwaarde is **TRUE**.

Eigenschappen voor Host Identifier

Eigenschap	Beschrijving	Standaardwaarde
Automatisch toewijzen	Hiermee wordt aangegeven of de server wordt gebonden aan een netwerkinterface die automatisch is toegewezen. Wanneer ingesteld op **ONWAAR**, wordt de server aan een specifieke netwerkinterface gebonden. Wanneer ingesteld op **WAAR**, accepteert de server aanvragen op het eerste beschikbare IP-adres. Op multihomed-computers kunt u de netwerkinterface opgeven waaraan u de server wilt koppelen door deze waarde op **ONWAAR** in te stellen en een geldige hostnaam of geldig IP-adres op te geven.	De standaardwaarde is **TRUE**.
Hostnaam	De hostnaam van de netwerkinterface waaraan de server wordt gekoppeld. Als er een hostnaam is opgegeven, accepteert de server aanvragen op alle IP-adressen die aan de hostnaam gekoppeld zijn.	Standaard is *Automatisch toewijzen* ingesteld op **WAAR** en is *Hostnaam* leeg.
IP-adres	Het IP-adres van de netwerkinterface waaraan de server wordt gekoppeld. Zowel het protocol IPv4 als IPv6 wordt ondersteund. Als er een IP-adres is opgegeven, accepteert de servers alleen aanvragen op het IP-adres.	Standaard is *Automatisch toewijzen* ingesteld op **WAAR** en is *IP-adres* leeg.

Eigenschappen voor configuratiesjabloon

Eigenschap	Beschrijving	Standaardwaarde
Configuratiesjabloon gebruiken	Hiermee wordt aangegeven of er een configuratiesjabloon gebruikt moet worden.	Standaard is deze optie **`uitgeschakeld`**.
Systeemstandaards herstellen	Hiermee wordt aangegeven of de oorspronkelijke standaardinstellingen voor deze server moeten worden hersteld.	De standaardwaarde is **FALSE**.

Eigenschap	Beschrijving	Standaardwaarde
Configuratiesjabloon instellen	Geeft aan of de instellingen van de actieve service moeten worden gebruikt als configuratiesjabloon voor alle services van hetzelfde type. Als deze optie is **`ingeschakeld`**, worden alle services van hetzelfde type dat u hebt opgegeven voor *Configuratiesjabloon gebruiken* onmiddellijk opnieuw geconfigureerd om de instellingen van de actieve service te gebruiken.	De standaardwaarde is **`FALSE`**.

Eigenschappen voor traceerlogboekservice

Eigenschap	Beschrijving	Standaardwaarde
Logboekniveau	Geeft de minimale ernst aan die berichten moeten hebben om te worden vastgelegd en de hoeveelheid informatie die in het logboekbestand van de server kan worden opgenomen. Mogelijke drempelniveaus van logboeken zijn: • *Niet opgegeven* • *Geen* • *Laag* • *Middelgroot* • *Hoog*	De standaardwaarde is **`Niet opgegeven`**.

35.1.2 Eigenschappen van kernservices

De categorie Kernservices omvat de volgende servers:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Containerserver voor webtoepassingen

Eigenschappen van Adaptive Job Server

Algemene eigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties. Voor betere prestaties zorgt u ervoor dat deze map zich op de lokale schijf bevindt. **Opmerking** U moet de server opnieuw starten om de wijzigingen door te voeren.	%DefaultDataDir%

De Adaptive Job Server kan verschillende services hosten. Elke service heeft de volgende eigenschappen

Service-eigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Maximumaantal gelijktijdige taken	Geeft het aantal onafhankelijke processen (onderliggende processen) aan dat de server gelijktijdig kan verwerken. U kunt het maximum aantal taken afstemmen op uw rapportageomgeving. De standaardinstelling is acceptabel voor de meeste rapportagescenario's. Welke instelling ideaal is voor uw rapportageomgeving, is afhankelijk van de hardwareconfiguratie, de databasesoftware en de rapportagevereisten.	5
Maximumaantal onderliggende aanvragen	Hiermee wordt het aantal taken opgegeven dat het onderliggende element zal verwerken voordat opnieuw gestart wordt.	100

Eigenschappen van Adaptive Processing Server

Algemene eigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Time-out van opstarten van service (seconden)	Geeft aan hoeveel seconden de server wacht op het starten van services. Als een service niet binnen de opgegeven tijd kan worden gestart, zijn er twee mogelijke oorzaken: • Een vereiste bron, zoals een database, is niet gevonden of de service heeft een poortconflict aangetroffen. • Het systeem werkt te traag. In het logbestand van de server kunt u nagaan wat de oorzaak is. Als de service niet binnen de opgegeven tijd kan worden gestart, kunt u overwegen deze waarde te verhogen.	1200

Eigenschappen van proxyservice voor clientcontrole

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van service voor beveiligingstokens

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van Inzicht in actieservice

Gegeven	Beschrijving	
Maximumaantal actieve verbindingen per gebruikerssessie	Het maximumaantal verbindingen met de SAP-server dat een bepaalde tijd beschikbaar is voor een gebruiker. Wanneer een gebruiker een rapport of dashboard opent dat RRI-functionaliteit heeft, wordt een verbinding met de SAP-server tot stand gebracht om de beschikbare RRI-doelen te bepalen.	20
Maximumaantal niet-actieve verbindingen per gebruikerssessie	Het aantal niet-actieve verbindingen dat open moet blijven en opnieuw gebruikt moet worden voor volgende RRI-verzoeken. Als u deze instelling verhoogt, worden er extra systeembronnen toegewezen.	20
Maximale wachttijd voor verbinding (in seconden)	Hoe lang het framework van Inzicht in actie moet wachten op antwoord van de SAP-server voordat een time-out optreedt (in seconden).	30

Eigenschappen van publicatieservice

Eigenschap	Beschrijving	Standaardwaarde
Grootte van threadpool	Hiermee wordt opgegeven hoeveel verwerkingsthreads voor bereikbatches tegelijk kunnen worden uitgevoerd. Als de waarde van deze eigenschap is ingesteld op “0”, wordt de grootte van de threadpool bepaald door een formule die is gebaseerd op het aantal CPU-kernen op de huidige computer.	0

Eigenschappen van vertaalservice

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van toezichtservice

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van service voor Platform zoeken

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van publicatienaverwerkingsservice

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van Central Management Server

> **Opmerking**
>
> Wijzigingen in deze servereigenschappen worden pas van kracht wanneer de server opnieuw wordt gestart.

Eigenschappen van Central Management-service

Eigenschap	Beschrijving	Standaardwaarde
Name Server-poort	Geeft de poort aan waarop de CMS luistert naar eerste naamserviceaanvragen.	6400
Aantal gevraagde systeemdatabaseverbindingen	Geeft het aantal CMS-systeemdatabaseverbindingen aan dat de CMS tot stand probeert te brengen. Als de server niet alle gewenste databaseverbindingen tot stand kan brengen, blijft de CMS werken maar zijn de prestaties niet optimaal, omdat er minder gelijktijdige aanvragen verwerkt kunnen worden. De CMS zal proberen extra verbindingen tot stand te brengen, totdat het gewenste aantal verbindingen is bereikt. Het gegeven *Tot stand gebrachte systeemdatabaseverbindingen* van de CMS toont het huidige aantal tot stand gebrachte verbindingen.	14
Automatisch opnieuw verbinding maken met systeemdatabase	Geeft aan of de CMS in het geval van een servicestoring automatisch moet proberen om de verbinding met de CMS-database te herstellen. Als deze optie is `uitgeschakeld`, kunt u de integriteit van de CMS-database controleren voordat de normale werking wordt hervat. De databaseverbinding kan pas worden hersteld wanneer de CMS opnieuw is gestart.	**TRUE**

Eigenschappen van Service voor eenmalige aanmelding

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding bij een gegevensbron. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken. Dit is van toepassing op gebruikers van Windows AD die rapporten uitvoeren die zijn geconfigureerd voor eenmalige aanmelding van Windows AD bij een gegevensbron.	86400

Eigenschappen van Event Server

Eigenschappen van Gebeurtenisservice

Eigenschap	Beschrijving	Standaardwaarde
Pollinginterval van gebeurtenis (in seconden)	Geeft aan hoeveel seconden de server moet zoeken naar een bestand waarmee een gebeurtenis wordt geactiveerd.	10 Het bereik van toegestane waarden is 1 tot 1200 seconden.
Opschoningsinterval (minuten)	Geeft aan hoe vaak opschoning moet worden uitgevoerd, in minuten.	20

Eigenschappen van Input File Repository Server

Eigenschappen van Input Filestore-service

Eigenschap	Beschrijving	Standaardwaarde
Map voor bestandsopslag	Geeft de map aan waarin objecten uit de bestandsopslagruimte worden opgeslagen. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	%DefaultInputFRSDir/%
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties. Voor betere prestaties is het raadzaam dat de *tijdelijke map* zich op hetzelfde bestandssysteem bevindt als de *map voor bestandsopslag*.	%DefaultInputFRSDir/temp%

Eigenschap	Beschrijving	Standaardwaarde
Maximale inactiviteitsduur (minuten)	Geeft de tijd aan dat de server wacht voordat niet-actieve verbindingen worden verbroken. Als er een te lage waarde voor deze instelling is opgegeven, kan het gevolg zijn dat de aanvraag van een gebruiker voortijdig wordt gesloten. Is er een te hoge waarde ingesteld, dan kunnen de systeembronnen zoals de verwerkingstijd en schijfruimte overmatig belast worden.	10
Maximumaantal pogingen voor bestandstoegang	Geeft het aantal keren aan dat de server moet proberen toegang te krijgen tot een bestand.	1
Locatie van bestand voor adapter virusscan	Geeft het absolute pad op van de locatie van het bestand voor de virusscanadapter.	

Eigenschappen van Output File Repository Server

Eigenschappen van Output Filestore-service

Eigenschap	Beschrijving	Standaardwaarde
Map voor bestandsopslag	Geeft de map aan waarin objecten uit de bestandsopslagruimte worden opgeslagen. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	%DefaultOutputFRSDir/%
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	%DefaultOutputFRS-Dir/temp%
Maximale inactiviteitsduur (minuten)	Geeft de tijd aan dat de server wacht voordat niet-actieve verbindingen worden verbroken. Als er een te lage waarde voor deze instelling is opgegeven, kan het gevolg zijn dat de aanvraag van een gebruiker voortijdig wordt gesloten. Is er een te hoge waarde ingesteld, dan kunnen de systeembronnen zoals de verwerkingstijd en schijfruimte overmatig belast worden.	10
Maximumaantal pogingen voor bestandstoegang	Geeft het aantal keren aan dat de server moet proberen toegang te krijgen tot een bestand.	1

Eigenschappen van Containerserver voor webtoepassingen

Algemene eigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Time-out van opstarten van service (seconden)	De tijd die door de WACS wordt gewacht op het starten van de gehoste services voordat een time-out optreedt Als de time-outtijd is verstreken, biedt de WACS geen services die nog niet zijn gestart. Op een trage computer kunt u een hogere waarde opgeven. Als u een te lage waarde opgeeft en de WACS niet wordt gestart vóór de time-out, herstelt u de standaardinstellingen van de WACS via de CCM (Central Configuration Manager).	1200

Eigenschappen van traceerlogboekservice

Eigenschap	Beschrijving	Standaardwaarde
Logboekniveau	Hiermee kunt u registratie inschakelen en het ernst- en detailniveau instellen op Geen (alleen essentiële gebeurtenissen worden geregistreerd), Laag (berichten voor opstarten, afsluiten, en aanvraag starten en beëindigen), Gemiddeld (fout-, waarschuwings- en de meeste statusberichten) of Hoog (Niets wordt uitgesloten. Alleen gebruiken voor foutopsporing. Het CPU-gebruik kan toenemen, wat van invloed kan zijn op de prestaties). De beschikbare menuopties zijn: • *Niet opgegeven* • *Geen* • *Laag* • *Middelgroot* • *Hoog*	Niet opgegeven

Eigenschappen van de Business Process BI-service

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van de service Opbouwfunctie voor query's

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

RESTful-webservice - Eigenschappen voor configuratie van systeemeigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Stapel met fouten weergeven	Wanneer deze optie is ingeschakeld, worden foutberichten van de RESTful-webservice voor foutopsporing in het foutlogboek opgenomen. De optie niet voor andere zaken gebruiken, of wanneer er een beveiligingsprobleem is waarbij details van het BI-platform worden onthuld.	Niet geselecteerd.
Standaardaantal objecten op één pagina	Het aantal items dat per pagina wordt weergegeven. Ontwikkelaars kunnen deze instelling overschrijven met de parameter &pageSize=<m> in de SDK van RESTful-webservices.	50
Time-out van Enterprise-sessietoken (minuten)	De verlooptijd waarover een aanmeldingstoken geldig blijft. Daarna moet een nieuw aanmeldingstoken worden gegenereerd.	60
Grootte van sessiepool	Het aantal sessies dat op elk willekeurig moment in de cache kan worden bewaard. Dit wordt gebruikt om de serverprestaties te verbeteren. De sessiepool plaatst RESTful-webservicesessies in cache zodat deze opnieuw kunnen worden gebruikt wanneer een gebruiker een ander verzoek verzendt met hetzelfde aanmeldingstoken in de HTTP-aanvraagheader.	1000
Time-out van sessiepool (minuten)	De tijd in minuten waarin sessies in cache verlopen.	2
HTTP Basic-verificatie inschakelen	Als deze instelling niet is ingeschakeld, moeten aanvragen van RESTful-webservices een aanmeldingstoken gebruiken. Is deze instelling ingeschakeld, dan moeten gebruikers hun naam en wachtwoord invoeren wanneer zij voor het eerst een RESTful-webservice-aanvraag indienen. Wanneer de instelling actief is, verschijnt het vervolgkeuzemenu *Standaardverificatieschema voor HTTP Basic*.	Niet geselecteerd.
Standaardverificatieschema voor HTTP Basic	Wanneer *HTTP Basic-verificatie inschakelen* is geselecteerd, is er keuze uit vier verificatietypen. Let erop dat namen en wachtwoorden als niet-gecodeerde tekst worden verzonden, tenzij HTTPS-opties worden gebruikt. Geldige waarden zijn: • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	Leeg. Als *HTTP Basic-verificatie inschakelen* echter is geselecteerd, wordt standaard *secEnterprise* gebruikt.

RESTful-webservice - Eigenschappen voor configuratie van Cross-Origin Resource Sharing

Eigenschap	Beschrijving	Standaardwaarde
Oorsprong toestaan	Met deze instelling krijgen gebruikers met CORS-browsers toegang tot Java-pagina's die meerdere domeinnamen moeten oproepen. Voeg alle domeinnamen toe en scheid ze met een komma. Bijvoorbeeld: http://origin1.server.com:8080, http://origin2.server.com:8080. Standaard hebben browsers toegang tot alle domeinen (*).	* (een asterisk)
Maximumleeftijd (minuten)	Dit is de maximumperiode waarin browsers HTTP-verzoeken in cache mogen plaatsen.	1440

RESTful-webservice - eigenschappen voor configuratie van vertrouwde verificatie

Eigenschap	Beschrijving	Standaardwaarde
Methode wordt opgehaald	Deze instelling is een menu waarin u instelt welke querymethode wordt gebruikt om aanmeldingstoken voor vertrouwde verificatie op te halen wanneer u de RESTful-webservice API `/logon/trusted` gebruikt. • *HTTP_HEADER* wordt gebruikt voor GET-query's met de aanvraagkop accept=application/xml (of application/json). • *QUERY_STRING* wordt gebruikt om een aanmeldingsnaam toe te voegen aan het eind van een URL-query met de RESTful-webservice API, bijvoorbeeld /logon/trusted/?user=johndoe. • *COOKIE* wordt gebruikt wanneer de aanmeldingsnaam wordt opgehaald uit een browsercookie. Het domein, de naam, de waarde en het pad moeten in de cookie zijn opgeslagen.	**HTTP_HEADER**
Parameter gebruikersnaam	Dit is de label dat wordt gebruikt om de vertrouwde gebruiker te identificeren bij het ophalen van een aanmeldingstoken.	**X-SAP-TRUSTED-USER**

Eigenschappen van BOE-webtoepassingsservice

Eigenschapstype	Beschrijving	Standaardwaarde
Verificatietype	Het verificatietype dat wordt gebruikt om gebruikers te verifiëren die zich aanmelden bij het BI-startpunt. Geldige waarden zijn: • *AD Kerberos* • *AD Kerberos SSO* • *Enterprise* • *LDAP*	*Enterprise*
Standaard AD-domein	Het standaard Active Directorydomein wordt gebruikt zodat gebruikers bij het aanmelden geen domein hoeven op te geven. Als het standaarddomein bijvoorbeeld is ingesteld op “mijndomein” en een gebruiker zich aanmeldt met de gebruikersnaam “gebruiker”, wordt “gebruiker@mijndomein.com” geverifieerd via de Active Directory-aanmelding.	Leeg

Eigenschapstype	Beschrijving	Standaardwaarde
Naam van service-principal	Een naam van service-principal (SPN) wordt door clients gebruikt voor de unieke identificatie van een exemplaar van een service. Bij de Kerberos-verificatieservice wordt een SPN gebruikt om een service te verifiëren.	Leeg
Keytab-bestand	Het volledige pad naar een keytab-bestand. Met een keytab-bestand kunt u Kerberos-filters configureren zonder dat het wachtwoord van de gebruikersaccount op de webtoepassingscomputer zichtbaar is.	Leeg

Eigenschappen van Webservices SDK en QaaWS

Eigenschap	Beschrijving	Standaardwaarde
Eenmalige aanmelding voor Kerberos/Active Directory instellen	Hiermee geeft u op of u eenmalige aanmelding via Kerberos AD wilt inschakelen voor Web Services SDK en QaaWS.	**FALSE**
Standaard AD-domein	Door het standaarddomein van Active Directory hoeven gebruikers geen domein op te geven bij het aanmelden.	Leeg
Naam van service-principal	Een naam van service-principal (SPN) wordt door clients gebruikt voor de unieke identificatie van een exemplaar van een service. Bij de Kerberos-verificatieservice wordt een SPN gebruikt om een service te verifiëren.	Leeg
Keytab-bestand	Het volledige pad naar een keytab-bestand. Met een keytab-bestand kunt u Kerberos-filters configureren zonder dat het wachtwoord van de gebruikersaccount op de webtoepassingscomputer zichtbaar is.	Leeg

Eigenschappen van HTTP-configuratie

Eigenschap	Beschrijving	Standaardwaarde
Binden aan alle IP-adressen	Geeft aan of alle netwerkinterfaces moeten worden gekoppeld Als uw server meer dan één netwerkinterface heeft en u aan een specifieke netwerkinterface wilt binden, schakelt u deze eigenschap uit.	**TRUE**
Binden aan hostnaam of IP-adres	Hiermee geeft u de netwerkinterface (IP-adres of hostnaam) op waarop de HTTP-service wordt aangeboden. U kunt alleen een waarde opgeven als u *Binden aan alle IP-adressen* uitschakelt.	`localhost`
HTTP-poort	De poort waarop de HTTP-service wordt aangeboden	6405 De waarden 1 tot en met 65535 zijn toegestaan.
Maximale HTTP-koptekstgrootte	De toegestane maximumgrootte, in bytes, van de HTTP-koptekst voor aanvraag en antwoord.	32768

Eigenschappen voor Configuratie van HTTP via proxy

Eigenschap	Beschrijving	Standaardwaarde
HTTP via proxy inschakelen	Hiermee geeft u aan of de connector HTTP via proxy moet worden ingeschakeld op de WACS. Dit is normaal ingeschakeld in implementaties met een reverse proxy.	**FALSE**

Eigenschap	Beschrijving	Standaardwaarde
Binden aan alle IP-adressen	Geeft aan of de HTTP via proxy-poort wordt gebonden aan alle netwerkinterfaces of niet.	**TRUE**
Binden aan hostnaam of IP-adres	Hiermee geeft u de netwerkinterface (IP-adres of hostnaam) op waarop de HTTP via proxy-service wordt aangeboden. U kunt alleen een waarde opgeven als u *Binden aan alle IP-adressen* uitschakelt.	`localhost`
HTTP-poort	De poort waarop de HTTP-service wordt aangeboden in een implementatie met een reverse proxy U kunt alleen een waarde opgeven als u *HTTP via proxy inschakelen* inschakelt.	6406 De waarden 1 tot en met 65535 zijn toegestaan.
Hostnaam van proxy	Het IPv4-adres, IPv6-adres, de hostnaam of de volledige domeinnaam van de proxyserver. U kunt alleen een waarde opgeven als u *HTTP via proxy inschakelen* inschakelt.	Leeg
Proxypoort	De poort van de forward- of reverse-proxyserver U kunt alleen een waarde opgeven als u *HTTP via proxy inschakelen* inschakelt.	0 De waarden 1 tot en met 65535 zijn toegestaan.
Maximale HTTP-koptekstgrootte	De toegestane maximumgrootte, in bytes, van de HTTP-koptekst voor aanvraag en antwoord.	32768

Eigenschappen van HTTPS-configuratie

Eigenschap	Beschrijving	Standaardwaarde
HTTPS inschakelen	Geeft aan of HTTPS/SSL-communicatie wordt ingeschakeld.	**FALSE**
Binden aan hostnaam of IP-adres	Hiermee geeft u de netwerkinterface (IP-adres of hostnaam) op waarop de HTTPS-service wordt aangeboden. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	`localhost`
HTTPS-poort	De poort waarop de HTTPS-service wordt aangeboden U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	443 De waarden 1 tot en met 65535 zijn toegestaan.
Hostnaam van proxy	Het IPv4-adres, IPv6-adres, de hostnaam of de volledige domeinnaam van de proxyserver. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	Leeg
Proxypoort	De poort van de forward- of reverse-proxyserver U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	0 De waarden 1 tot en met 65535 zijn toegestaan.
Protocol	Het coderingsprotocol dat moet worden gebruikt U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	TLS De toegestane waarden TLS of SSL.
Type certificaatopslag	Het type certificaatarchief waarin uw certificaten en persoonlijke sleutels zijn opgenomen. Dit is meestal *PCKS12*. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	PKCS12 De toegestane waarden zijn PKCS12 of JKS.
Locatie certificaatopslag	Het volledige pad naar het certificaatarchief. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	Leeg

Eigenschap	Beschrijving	Standaardwaarde
Wachtwoord voor toegang tot privésleutel	PKCS12-certificaatarchieven en JKS-keystorebestanden hebben persoonlijke sleutels die zijn beveiligd met een wachtwoord om toegang door onbevoegden of diefstal te voorkomen. Voer het wachtwoord in dat u hebt opgegeven op het moment waarop u de certificaatopslag hier hebt gegenereerd, zodat de WACS toegang heeft tot persoonlijke sleutels uit de certificaatopslag. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	Leeg
Certificaat-alias	De alias van het certificaat in het certificaatarchief. Als geen alias wordt opgegeven en het certificaatarchief meerdere certificaten bevat, wordt het eerste certificaat uit het archief gebruikt. U hoeft meestal geen waarde op te geven. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* inschakelt.	Leeg
Clientverificatie inschakelen	Als clientverificatie is ingeschakeld, kunnen alleen clients waarvan de sleutels zijn opgeslagen in de certificaatvertrouwenslijst, toegang krijgen tot de containerserver voor webtoepassingen. Andere clients worden geweigerd. U kunt alleen clientverificatie inschakelen als u *HTTPS inschakelen* inschakelt.	**FALSE**
Certificaat - bestandslocatie van vertrouwde lijst	Het volledige pad naar de certificaatvertrouwenslijst. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* en *Clientverificatie inschakelen* inschakelt.	Leeg
Certificaat - wachtwoord voor toegang tot privésleutel voor vertrouwde lijst	Het wachtwoord voor toegang tot de persoonlijke sleutels in de certificaatvertrouwenslijst. U kunt alleen een waarde opgeven als u *HTTPS inschakelen* en *Clientverificatie inschakelen* inschakelt.	Leeg
Maximale HTTP-koptekstgrootte	De toegestane maximumgrootte, in bytes, van de HTTP-koptekst voor aanvraag en antwoord.	32768

Eigenschappen voor gelijktijdigheid (per connector)

Eigenschap	Beschrijving	Standaardwaarde
Maximumaantal gelijktijdige aanvragen	Het aantal gelijktijdige HTTP- of HTTPS-aanvragen dat via elke connector (HTTP, HTTP via proxy of HTTPS) tegelijk kan worden verwerkt	**`150`** De waarden 1 tot en met 1000 zijn toegestaan.

Configuratie-eigenschappen voor Active Directory

Eigenschap	Beschrijving	Standaardwaarde
Locatie van bestand Krb5.ini	Het volledige pad naar een `krb5.ini`-bestand waarin Kerberos-configuratie-eigenschappen worden opgeslagen.	Leeg
Locatie van bestand bscLogin.conf	Het volledige pad naar een `bscLogin.config`-bestand.	Leeg

35.1.3 Eigenschappen van Connectivity-services

De categorie Connectivity-service omvat de volgende services:

- Eigen Connectivity-service (gehost op zelfstandige server)

- Eigen Connectivity-service (32-bits versie gehost op zelfstandige server)
- Adaptive Connectivity-service (gehost in APS)

Alle services delen dezelfde configuratie-instellingen.

Eigenschappen van service voor toegang tot Excel-gegevens

Eigenschap	Beschrijving	Standaardwaarde
Opschoontime-out voor toegang tot Excel-gegevens (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie wordt opgeschoond.	De standaardwaarde is 1200 seconden.
Wisseltime-out voor toegang tot Excel-gegevens (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie op de vaste schijf wordt gewisseld. Het is raadzaam een waarde op te geven die lager is dan de waarde voor de eigenschap *Opschoontime-out voor toegang tot Excel-gegevens (in seconden)*.	De standaardwaarde is 600 seconden.

Eigenschappen van servicebewerking

Eigenschap	Beschrijving	Standaardwaarde
	→ Onthouden U hoeft de server niet opnieuw op te starten nadat de volgende eigenschappen van servicebewerking zijn gewijzigd.	
Pooling van verbindingen	Hiermee wordt de verbindingspool in- of uitgeschakeld. Mogelijke waarden zijn: • Ingeschakeld - Met time-out • Ingeschakeld - Zonder time-out • Uitgeschakeld **ⓘ Opmerking** De verbindingspool is een cache-functionaliteit die de herbruikbare staat van verbindingen behoudt om zo de serverprestaties te verbeteren.	Ingeschakeld - Met time-out
Time-out voor verbindingspool	Hiermee wordt de maximale inactiviteitsduur voor verbindingen in de pool opgegeven (in minuten). **ⓘ Opmerking** Deze eigenschap is gelijk aan de parameter `Max Pool Time` van het bestand `cs.cfg`. Het uitschakelen van de pool is gelijk aan `Max Pool Time` wanneer deze is ingesteld op `0`. Het inschakelen van de pool zonder time-out is gelijk aan `Max Pool Time` wanneer deze is ingesteld op `-1`. Raadpleeg de *Handleiding voor gegevenstoegang* voor meer informatie.	`60`

Eigenschap	Beschrijving	Standaardwaarde
Standby-time-out voor tijdelijk object	Hiermee wordt het aantal minuten aangegeven dat een ongebruikt tijdelijk object op de server moet blijven staan. Hierna wordt het object verwijderd en worden de bronnen vrijgemaakt.	**60**
Timerinterval voor tijdelijk object	Hiermee wordt de tijd tussen activiteitcontroles opgegeven (in minuten). De server zoekt regelmatig naar kandidaatobjecten die verwijderd kunnen worden.	**5**
HTTP-segmentering inschakelen	Hiermee wordt de HTTP-segmentering in- of uitgeschakeld. **Opmerking** HTTP-segmentering is alleen van toepassing op drielaagse implementatie. Dit is van invloed op het openen en vernieuwen van documenten, omdat er voor grotere antwoorden minder heen-en-weer hoeft te worden gegaan bij het ophalen van grote documenten. Het uitschakelen van de HTTP-segmentering is gelijk aan de *HTTP-segmentgrootte* wanneer deze is ingesteld op **0**.	Ingeschakeld
HTTP-segmentgrootte	Hiermee wordt de grootte aangegeven van HTTP-antwoorden die worden afgegeven door de server (in kilobytes).	**64**

Eigenschappen voor tracering op laag niveau

Eigenschap	Beschrijving	Standaardwaarde
Onthouden U hoeft de server niet opnieuw op te starten nadat de volgende eigenschappen voor tracering op laag niveau zijn gewijzigd.		
Taaktracering inschakelen	Hiermee wordt de tracering ingeschakeld van verbindingsservertaken. **Opmerking** Hiervoor moet de eigenschap *Registratieniveau* ingesteld worden op *Hoog*.	Uitgeschakeld
Middleware-tracering inschakelen	Hiermee wordt de tracering van alle middleware ingeschakeld. Als u specifieke middleware wilt traceren, moet u het bestand `cs.cfg` configureren en de server opnieuw opstarten. **Opmerking** Hiervoor moet de eigenschap *Registratieniveau* ingesteld worden op *Hoog*.	Uitgeschakeld

Eigenschappen van actieve gegevensbronnen

Eigenschap	Beschrijving	Standaardwaarde
	⚠ Let op U moet de server opnieuw opstarten nadat de volgende eigenschappen van actieve gegevensbronnen zijn gewijzigd.	
Gegevensbron activeren	Hiermee kunt u de gegevensbronnen selecteren waar u verbindingen voor wilt maken. Deze eigenschap werkt als een filter voor stuurprogramma's. U kunt de actieve gegevensbronnen opgeven om de gewenste stuurprogramma's te laden. **⚠ Let op** Het standaardservergedrag is alle beschikbare stuurprogramma's laden. Gebruik deze instelling om de servers te specialiseren. Dit is vooral nuttig wanneer u meerdere CORBA-servers op uw netwerk implementeert. **→ Onthouden** Er worden alleen stuurprogramma's voor geselecteerde gegevensbronnen geladen. Alle andere worden genegeerd. Als u geen gegevensbronnen selecteert, laadt de server alle beschikbare stuurprogramma's. **ⓘ Opmerking** Controleer in de servergegevens of de geselecteerde gegevensbronnen zijn geactiveerd. De netwerklagen en databases worden weergegeven onder *Gegevens van verbindingsservice*.	Uitgeschakeld
Netwerklaag	Hiermee wordt de netwerklaag aangegeven die door de verbinding gebruikt wordt. **ⓘ Opmerking** Alleen de niet-gelokaliseerde naam wordt gebruikt. U kunt de lijst met beschikbare netwerklagen vinden in het bestand `driver.cfg`, dat zich bevindt in de map `<connectionserver-install-dir>\connectionServer\`.	• **ODBC** voor systeemeigen CORBA-servers • **JDBC** voor adaptieve CORBA-server

Eigenschap	Beschrijving	Standaardwaarde
Database	Hiermee wordt de database aangegeven die door de verbinding gebruikt wordt. **Opmerking** Alleen de niet-gelokaliseerde naam wordt gebruikt. Databasenamen kunnen reguliere expressies zijn als het om zuivere ASCII-tekenreeksen gaat. Patronen maken gebruiken van GNU regexp-syntaxis. Gebruik het patroon `.*` voor elk willekeurig teken. De expressie `MS SQL Server.*$` betekent bijvoorbeeld dat alle MS SQL Serverdatabases in gebruik zijn. Zie de PERL-website op http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions voor meer informatie over reguliere expressies.	Het veld is leeg totdat u een databasenaam invoert.

Eigenschappen van service voor toegang tot aangepaste gegevens

Eigenschap	Beschrijving	Standaardwaarde
Opschoontime-out voor toegang tot aangepaste gegevens (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie wordt opgeschoond.	De standaardwaarde is 1200 seconden.
Wisseltime-out voor toegang tot aangepaste gegevens (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie op de vaste schijf wordt gewisseld. Het is raadzaam een waarde op te geven die lager is dan de waarde voor de eigenschap *Opschoontime-out voor toegang tot aangepaste gegevens (in seconden)*	De standaardwaarde is 600 seconden.

Eigenschappen voor Service voor eenmalige aanmelding

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken.	De standaardwaarde is 86400 seconden.

Eigenschappen van service Promotiebeheer

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van ClearCase-service Promotiebeheer

Eigenschap	Beschrijving	Standaardwaarde
Geen configuratie-eigenschappen		

Eigenschappen van service voor Visueel verschil

Eigenschap	Beschrijving	Standaardwaarde
Geen configuratie-eigenschappen		

Verwante informatie

Algemene servereigenschappen [pagina 1157]

35.1.4 Eigenschappen van Crystal Reports-services

De categorie Crystal Reports Services omvat de volgende servers:

- Crystal Reports Cache Server
- Crystal Reports-verwerkingsserver
- Eigenschappen van Crystal Reports 2020 Report Application Server
- Crystal Reports 2020-verwerkingsserver

Eigenschappen voor Crystal Reports Cache Server

Eigenschappen die van toepassing zijn op Crystal Reports Cache Servers en Crystal Reports-verwerkingsservers, moeten op dezelfde waarde zijn ingesteld. Als bijvoorbeeld de instelling *Vernieuwen van viewer geeft altijd de huidige gegevens* op de Cache Server is **`ingeschakeld`**, moet dezelfde eigenschap ook zijn **`ingeschakeld`** op de verwerkingsserver.

> **Opmerking**
>
> Wijzigingen in deze servereigenschappen worden pas van kracht wanneer de server opnieuw wordt gestart.

Eigenschappen voor Crystal Reports Cache Service

Eigenschap	Beschrijving	Standaardwaarde
Vernieuwen van viewer geeft altijd de huidige gegevens	Geeft aan of alle pagina's in het cachegeheugen al dan niet moeten worden genegeerd en nieuwe gegevens rechtstreeks uit de database moeten worden opgehaald wanneer gebruikers een rapport expliciet vernieuwen. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen. Als u een waarde voor het rapportobject wilt instellen, selecteert u het rapport in de CMC, en klikt u op *Standaardinstellingen* > *Servergroep voor weergave*.	De standaardwaarde is **FALSE**.

Eigenschap	Beschrijving	Standaardwaarde
Rapportgegevens delen tussen clients	Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	Standaard is deze optie`ingeschakeld`.
Time-out niet-actieve verbinding (in minuten)	Geeft aan hoeveel minuten de Crystal Reports Cache Server wacht op aanvragen van een niet-actieve verbinding. In het algemeen is het niet nodig om de standaardwaarde te wijzigen.	De standaardwaarde is 20 minuten.
Time-out van beveiligingscache (in minuten)	Hiermee wordt aangegeven hoeveel minuten de server aanmeldingsreferenties, rapportparameters en gegevens over databaseverbindingen uit het cachegeheugen gebruikt om aanvragen te verwerken voordat er een query wordt uitgevoerd in de CMS.	De standaardwaarde is 20 minuten.
Oudste gegevens die op aanvraag aan een client worden gegeven (in seconden)	Geeft aan hoeveel seconden de server gegevens in het cachegeheugen gebruikt om te voldoen aan aanvragen van rapporten op aanvraag. Als de server een aanvraag ontvangt die kan worden voldaan met gegevens die voor een eerdere aanvraag zijn gegenereerd en als de tijd die is verstreken sinds die gegevens zijn gegenereerd korter is dan de waarde die hier is ingesteld, gebruikt de server deze gegevens opnieuw om aan de volgende aanvraag te voldoen. Door gegevens opnieuw te gebruiken worden de systeemprestaties aanzienlijk verbeterd als meerdere gebruikers dezelfde gegevens nodig hebben. Overweeg bij het instellen van deze waarde hoe belangrijk het is dat de gebruikers actuele gegevens ontvangen. Als het heel belangrijk is dat alle gebruikers de nieuwste gegevens ontvangen (bijvoorbeeld omdat belangrijke gegevens vaak worden gewijzigd), kunt u het opnieuw gebruiken van gegevens uitschakelen door de waarde op 0 in te stellen. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	De standaardwaarde is 0 seconden.
Maximale cachegrootte (KB)	Geeft de hoeveelheid vaste-schijfruimte (in kB) aan die wordt gebruikt om rapporten in het cachegeheugen te plaatsen. Een grotere cache kan nodig zijn als op de server grote hoeveelheden rapporten worden verwerkt of wanneer de rapporten bijzonder complex zijn.	De standaardwaarde is 256000 KB.

Eigenschap	Beschrijving	Standaardwaarde
Map met cachebestanden	Geeft de locatie aan van het cachebestand.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Java VM-argumenten	Hiermee worden de opdrachtregelargumenten opgegeven die verstrekt kunnen worden aan de JVM.	Standaard is deze waarde leeg.
DLL-naam	Hiermee wordt de naam opgegeven van de documentinvoegtoepassing die momenteel is geladen. Deze eigenschap is alleen-lezen.	rasprocReport

Eigenschappen voor Crystal Reports-verwerkingsserver

Eigenschappen die van toepassing zijn op Crystal Reports Cache Servers en Crystal Reports-verwerkingsservers, moeten op dezelfde waarde zijn ingesteld. Als bijvoorbeeld de instelling *Vernieuwen van viewer geeft altijd de huidige gegevens* op de Cache Server is **`ingeschakeld`**, moet dezelfde eigenschap ook zijn **`ingeschakeld`** op de verwerkingsserver.

> **Opmerking**
>
> Wijzigingen in deze servereigenschappen worden pas van kracht wanneer de server opnieuw wordt gestart.

Eigenschappen voor Crystal Reports-verwerkingsservice

Eigenschap	Beschrijving	Standaardwaarde
Time-out niet-actieve taak (in minuten)	Geeft de duur aan, in minuten, dat de Crystal Reports-verwerkingsserver wacht tussen aanvragen voor een bepaalde taak.	De standaardwaarde is 20 minuten.
Maximale levensduurtaken per onderliggend element	Geeft het maximum aantal taken aan dat elk onderliggend proces per levensduur kan verwerken.	De standaardwaarde is 1000.
Vernieuwen van viewer geeft altijd de huidige gegevens	Geeft aan of alle pagina's in het cachegeheugen al dan niet moeten worden genegeerd en nieuwe gegevens rechtstreeks uit de database moeten worden opgehaald wanneer gebruikers een rapport expliciet vernieuwen. Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen. Als u een waarde voor het rapportobject wilt instellen, selecteert u het rapport in de CMC, en klikt u op *Standaardinstellingen* > *Servergroep voor weergave*.	De standaardwaarde is **FALSE**.

Eigenschap	Beschrijving	Standaardwaarde
Rapportgegevens delen tussen clients	Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	Standaard is deze optie`ingeschakeld`.
Time-out niet-actieve verbinding (in minuten)	Geeft aan hoeveel minuten de Crystal Reports-verwerkingsserver wacht op aanvragen van een niet-actieve verbinding. In het algemeen is het niet nodig om de standaardwaarde te wijzigen.	De standaardwaarde is 20 minuten.
Maximum aantal gelijktijdige taken (0 voor automatisch)	Geeft het maximum aantal onafhankelijke taken aan dat gelijktijdig kan worden uitgevoerd op de Crystal Reports-verwerkingsserver. Als de waarde van deze eigenschap is ingesteld op "0", wordt door de server een geldige waarde toegepast op basis van de CPU en het geheugen van de computer waarop de server wordt uitgevoerd.	De standaardwaarde is 0.
Oudste gegevens die op aanvraag aan een client worden gegeven (in seconden)	Geeft aan hoeveel seconden de server gegevens in het cachegeheugen gebruikt om te voldoen aan aanvragen van rapporten op aanvraag. Als de server een aanvraag ontvangt die kan worden voldaan met gegevens die voor een eerdere aanvraag zijn gegenereerd en als de tijd die is verstreken sinds die gegevens zijn gegenereerd korter is dan de waarde die hier is ingesteld, gebruikt de server deze gegevens opnieuw om aan de volgende aanvraag te voldoen. Door gegevens opnieuw te gebruiken worden de systeemprestaties aanzienlijk verbeterd als meerdere gebruikers dezelfde gegevens nodig hebben. Overweeg bij het instellen van deze waarde hoe belangrijk het is dat de gebruikers actuele gegevens ontvangen. Als het heel belangrijk is dat alle gebruikers de nieuwste gegevens ontvangen (bijvoorbeeld omdat belangrijke gegevens vaak worden gewijzigd), kunt u het opnieuw gebruiken van gegevens uitschakelen door de waarde op 0 in te stellen. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	De standaardwaarde is 0.

Eigenschap	Beschrijving	Standaardwaarde
Maximum aantal op voorhand gestarte onderliggende elementen	Geeft het maximum aantal vooraf gestarte onderliggende processen aan dat door de server wordt ondersteund. Als deze waarde te laag is, maakt de server onderliggende processen zodra er aanvragen zijn gegenereerd en kunnen gebruikers vertraging ervaren. Is deze waarde te hoog, dan worden systeembronnen mogelijk onnodig verspild door niet-actieve onderliggende processen.	De standaardwaarde is 1 onderliggend proces.
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Pad naar Java-klasse	De naam en het pad van de Java-klassen die door de server zijn vereist.	%CommonJavaLibDir%/procCR.jar
Onderliggende Java VM-argumenten	Hiermee worden de opdrachtregelargumenten opgegeven die worden verstrekt aan de onderliggende processen die door de server gemaakt zijn.	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

Eigenschappen voor Service voor eenmalige aanmelding

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken.	De standaardwaarde is 86400 seconden.

Eigenschappen van Crystal Reports 2020 Report Application Server

Opmerking

Wijzigingen in deze eigenschappen worden pas van kracht wanneer de server opnieuw wordt gestart.

Eigenschappen van Crystal Reports 2020-service voor weergave en wijziging

Eigenschap	Beschrijving	Standaardwaarde
Toestaan dat rapporttaken verbinding met database blijven behouden totdat de rapporttaak wordt gesloten	Geeft aan of de rapporttaak in verbinding blijft met de database totdat het proces wordt uitgevoerd.	Standaard is deze optie `uitgeschakeld`.

Eigenschap	Beschrijving	Standaardwaarde
Omvang bladergegevens (records)	Geeft het aantal afzonderlijke records aan dat door de database wordt geretourneerd wanneer door de waarden van een bepaald veld wordt gebladerd. De gegevens worden in eerste instantie opgehaald uit het cachegeheugen van de client - als dit beschikbaar is - en vervolgens uit het cachegeheugen van de server. Als de gegevens zich in geen van beide caches bevinden, worden ze opgehaald uit de database.	De standaardwaarde is 100 records.
Time-out niet-actieve verbinding (in minuten)	Geeft aan hoeveel minuten de RAS (Report Application Server) wacht op aanvragen van een niet-actieve client voordat de time-out optreedt. Als u hier een te lage waarde instelt, kan een aanvraag van een gebruiker voortijdig worden gesloten. Een te hoge waarde kan de schaalbaarheid van de server nadelig beïnvloeden (als bijvoorbeeld het object `ReportClientDocument` niet expliciet wordt gesloten, wordt er door de server onnodig gewacht totdat een niet-actieve taak wordt gesloten).	De standaardwaarde is 30 minuten.
Batchgrootte (records)	Geeft aan hoeveel rijen uit de resultaatreeks tijdens elke gegevensoverdracht door de database worden geretourneerd. Als er bijvoorbeeld 500 records zijn aangevraagd en de batchgrootte is ingesteld op 100 records, worden de gegevens geretourneerd in vijf afzonderlijke batches van 100 rijen. Als u de prestaties van de RAS wilt verbeteren, hebt u inzicht nodig in de netwerkomgeving, de database en het type aanvraag, zodat u de juiste batchgrootte kunt instellen.	De standaardwaarde is 100 records.
Aantal databaserecords dat moet worden gelezen bij het bekijken of vernieuwen van een rapport (-1 voor onbeperkt)	Geeft het aantal databaserecords aan dat wordt gelezen wanneer een rapport wordt weergegeven of vernieuwd. Met deze instelling kunt u het aantal records beperken dat door de server uit de database wordt opgehaald wanneer een gebruiker een query of rapport uitvoert. Deze instelling is handig als u wilt voorkomen dat gebruikers rapporten op aanvraag uitvoeren die enorme hoeveelheden records als resultaat geven. Misschien wilt u dergelijke rapporten plannen om de rapporten sneller beschikbaar te maken voor gebruikers en om de belasting van de database door deze omvangrijke query's te reduceren.	De standaardwaarde is 20000 records.
Maximum aantal gelijktijdige rapporttaken (0 voor onbeperkt)	Geeft het maximum aantal onafhankelijke taken aan dat gelijktijdig kan worden uitgevoerd op de RAS.	De standaardwaarde is 75 taken.
Oudste gegevens die op aanvraag aan een client worden gegeven (in minuten)	Geeft aan hoe lang, in minuten, een rapport op aanvraag reageert op rapportgegevens die zich in het cachegeheugen bevinden.	De standaardwaarde is 20 minuten.

Eigenschap	Beschrijving	Standaardwaarde
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Eigenschappen voor Service voor eenmalige aanmelding

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken.	De standaardwaarde is 86400 seconden.

Eigenschappen voor Crystal Reports 2020-verwerkingsserver

Opmerking

Wijzigingen in deze eigenschappen worden pas van kracht wanneer de server opnieuw wordt gestart.

Eigenschappen van Crystal Reports 2020-verwerkingsservice

Eigenschap	Beschrijving	Standaardwaarde
Time-out niet-actieve taak (in minuten)	Geeft de duur aan, in minuten, dat de Crystal Reports-verwerkingsserver wacht tussen aanvragen voor een bepaalde taak.	De standaardwaarde is 20 minuten.
Maximale levensduurtaken per onderliggend element	Geeft het maximum aantal taken aan dat elk onderliggend proces per levensduur kan verwerken.	De standaardwaarde is 1000.
Vernieuwen van viewer geeft altijd de huidige gegevens	Geeft aan of alle pagina's in het cachegeheugen al dan niet moeten worden genegeerd en nieuwe gegevens rechtstreeks uit de database moeten worden opgehaald wanneer gebruikers een rapport expliciet vernieuwen. Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen. Als u een waarde voor het rapportobject wilt instellen, selecteert u het rapport in de CMC, en klikt u op *Standaardinstellingen* > *Servergroep voor weergave*.	De standaardwaarde is **FALSE**.

Eigenschap	Beschrijving	Standaardwaarde
Rapportgegevens delen tussen clients	Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. Geeft aan of rapportgegevens moeten worden gedeeld door verschillende clients. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	Standaard is deze optie`ingeschakeld`.
Time-out niet-actieve verbinding (in minuten)	Geeft aan hoeveel minuten de Crystal Reports-verwerkingsserver wacht op aanvragen van een niet-actieve verbinding. In het algemeen is het niet nodig om de standaardwaarde te wijzigen.	De standaardwaarde is 20 minuten.
Maximum aantal gelijktijdige taken (0 voor automatisch)	Geeft het maximum aantal onafhankelijke taken aan dat gelijktijdig kan worden uitgevoerd op de Crystal Reports-verwerkingsserver. Als de waarde van deze eigenschap is ingesteld op "0", wordt door de server een geldige waarde toegepast op basis van de CPU en het geheugen van de computer waarop de server wordt uitgevoerd.	De standaardwaarde is 0.
Oudste gegevens die op aanvraag aan een client worden gegeven (in seconden)	Geeft aan hoeveel seconden de server gegevens in het cachegeheugen gebruikt om te voldoen aan aanvragen van rapporten op aanvraag. Als de server een aanvraag ontvangt die kan worden voldaan met gegevens die voor een eerdere aanvraag zijn gegenereerd en als de tijd die is verstreken sinds die gegevens zijn gegenereerd korter is dan de waarde die hier is ingesteld, gebruikt de server deze gegevens opnieuw om aan de volgende aanvraag te voldoen. Door gegevens opnieuw te gebruiken worden de systeemprestaties aanzienlijk verbeterd als meerdere gebruikers dezelfde gegevens nodig hebben. Overweeg bij het instellen van deze waarde hoe belangrijk het is dat de gebruikers actuele gegevens ontvangen. Als het heel belangrijk is dat alle gebruikers de nieuwste gegevens ontvangen (bijvoorbeeld omdat belangrijke gegevens vaak worden gewijzigd), kunt u het opnieuw gebruiken van gegevens uitschakelen door de waarde op 0 in te stellen. **Opmerking** Deze eigenschap kan voor een rapportobject zelf worden ingesteld en kan per rapport verschillen; waarden die voor het rapportobject worden ingesteld, prevaleren boven de serverinstellingen.	De standaardwaarde is 0.

Eigenschap	Beschrijving	Standaardwaarde
Maximum aantal op voorhand gestarte onderliggende elementen	Geeft het maximum aantal vooraf gestarte onderliggende processen aan dat door de server wordt ondersteund. Als deze waarde te laag is, maakt de server onderliggende processen zodra er aanvragen zijn gegenereerd en kunnen gebruikers vertraging ervaren. Is deze waarde te hoog, dan worden systeembronnen mogelijk onnodig verspild door niet-actieve onderliggende processen.	De standaardwaarde is 1 onderliggend proces.
Tijdelijke map	Geeft de map aan waar tijdelijke bestanden worden gemaakt wanneer nodig. **Opmerking** Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen met verminderde prestaties.	%DefaultDataDir%/CrystalReports2020ProcessingServer/temp
Toestaan dat rapporttaken verbinding met database blijven behouden totdat de rapporttaak wordt gesloten	Geeft aan of de rapporttaak in verbinding blijft met de database totdat de taak wordt gesloten.	Standaard is deze instelling uitgeschakeld.
Aantal gelezen databaserecords bij voorbeeldweergave of vernieuwen (0 voor onbeperkt)	Geeft het aantal databaserecords aan dat wordt gelezen wanneer een rapport wordt weergegeven of vernieuwd. Met deze instelling kunt u het aantal records beperken dat door de server uit de database wordt opgehaald wanneer een gebruiker een query of rapport uitvoert. Deze instelling is handig als u wilt voorkomen dat gebruikers rapporten op aanvraag uitvoeren die enorme hoeveelheden records als resultaat geven. Misschien wilt u dergelijke rapporten plannen om de rapporten sneller beschikbaar te maken voor gebruikers en om de belasting van de database door deze omvangrijke query's te reduceren.	De standaardwaarde is 20000.

Eigenschappen voor Service voor eenmalige aanmelding

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken.	De standaardwaarde is 86400 seconden.

35.1.5 Eigenschappen van Analysis Services

De categorie van Analysis Services omvat de Adaptive Processing Server:

Eigenschappen voor Multi-Dimensional Analysis Service

Eigenschap	Beschrijving	Standaardwaarde
Maximum aantal clientsessies	Het maximumaantal MDAS-verbindingen dat gelijktijdig geopend kan zijn op de server. Wanneer het aantal open sessies dit aantal heeft bereikt, resulteren verdere pogingen om MDAS-sessies te starten in het foutbericht "server niet beschikbaar". U kunt deze waarde wijzigen en zo de prestaties van de MDAS optimaliseren, afhankelijk van uw behoeften en de beschikbare hardware. Een hogere waarde kan echter leiden tot prestatieproblemen voor zowel de MDAS als de database. De standaardwaarde van 15 sessies is een conservatieve schatting. Voor installaties met kleine gebruikersquery's kunt u deze waarde aanzienlijk verhogen, terwijl installaties met grote gebruikersquery's een lagere waarde vereisen.	De standaardwaarde is 15. Het geldige bereik is 1 tot 100.
Maximumaantal cellen dat door een query wordt geretourneerd	Hiermee wordt het aantal cellen aangegeven dat door een gebruiker wordt geretourneerd in één query. De gebruiker kan geen query uitvoeren waarmee een extreem laag aantal cellen wordt geretourneerd en waarbij veel geheugen wordt verbruikt. Als de query van de gebruiker deze cellimiet overschrijdt, ontvangt de gebruiker een foutbericht.	De standaardwaarde is 100000 cellen.
Maximumaantal leden dat bij filteren is geretourneerd	Hiermee wordt het aantal leden opgegeven dat wordt opgehaald bij het filteren op lid. Een groot aantal opgehaalde leden kan een groot deel van het geheugen in beslag nemen.	De standaardwaarde is 1000000 leden.

Eigenschappen van BEx-webtoepassingsservices

Eigenschap	Beschrijving	Standaardwaarde
Maximum aantal clientsessies	Het maximumaantal toegestane clientsessies op de service.	De standaardwaarde is 15 sessies.
SAP BW Master System	De naam van de OLAP-verbinding met het BW-systeem dat u in het BI-platform hebt gemaakt.	De standaardwaarde is SAP_BW.
RFC-doel van JCo-server	De naam van het RFC-doel van de JCo-server die u in het BW-systeem hebt ingevoerd.	Standaard is deze waarde leeg.
Gateway-host van JCo-server	De naam van de gateway-host van de JCo-server die u in het BW-systeem hebt gedefinieerd.	Standaard is deze waarde leeg.
Gateway-service van JCo-server	De naam van de gateway-service van de JCo-server die u in het BW-systeem hebt gedefinieerd.	Standaard is deze waarde leeg.
Verbindingsaantal van JCo-server	Geeft het aantal automatisch aangemaakte programma's op waarmee oproepen van ABAP naar Java voor de service kunnen worden verwerkt.	De standaardwaarde is 3 verbindingen.

35.1.6 Eigenschappen van Data Federator-services

De categorie van de Data Federator-services omvat de Adaptive Processing Server:

Eigenschappen van Data Federator-services

Eigenschap	Beschrijving	Standaardwaarde
Max. verbindingen	Hiermee wordt het maximumaantal verbindingen aangegeven dat is toegestaan op de server.	De standaardwaarde is 32767.
Grootte van uit te voeren threadpool	Hiermee wordt het maximumaantal query's opgegeven dat parallel kan worden uitgevoerd op een willekeurig moment.	De standaardwaarde is 10.
Standby-time-out voor verbinding	Hiermee wordt aangegeven na hoeveel seconden een inactieve verbinding wordt gesloten.	De standaardwaarde is 10800 seconden.
Instructie Standby-time-out	Hiermee wordt aangegeven na hoeveel seconden een inactieve query-instructie wordt gesloten.	De standaardwaarde is 600 seconden.

35.1.7 Eigenschappen van Web Intelligence Services

De categorie Web Intelligence Services omvat de volgende servers:

- Adaptive Processing Server
- Web Intelligence-verwerkingsserver

Instellingen voor Adaptive Processing Server

Opdrachtregelparameters

Eigenschap	Beschrijving	Standaardwaarde
Tot niveau weergeven	Hiermee wordt het niveau weergegeven tot waar gegevens worden opgehaald uit BEx-query's. Hiërarchieën worden standaard niet naar een gegeven niveau uitgevouwen. Niveau 00 is altijd het standaardniveau. U kunt deze werking wijzigen door deze parameter aan de opdrachtregel toe te voegen, maar als u de waarde te hoog instelt, haalt Web Intelligence alle hiërarchiegegevens op, wat van invloed kan zijn op de prestaties en stabiliteit van het systeem.	`-Dsap.sl.bics.expandToLevel=n` n kan een geheel getal tussen 0 en 99 zijn. Als n=0 of als deze parameter niet is opgegeven, gebruiken hiërarchieën niet de parameter Tot niveau weergeven.

Eigenschap	Beschrijving	Standaardwaarde
Variabeleselectie Selectieoptie	Geeft de selectieoptie voor variabeleselectie op. Als deze eigenschap op interval is ingesteld, is het tekstvak niet beschikbaar en kunnen gebruikers alleen in het dialoogvenster Aanwijzingen de begin- en eindwaarde invoeren. Als deze eigenschap op meer waarden is ingesteld, is het tekstvak "Type een waarde" beschikbaar en kunnen gebruikers waarden voor BW-selectieoptievariabelen invoeren. **Opmerking** Lokale installaties van Web Intelligence Rich Client worden niet bijgewerkt met deze eigenschap. Zie de "Installatiehandleiding voor Web Intelligence Rich Client" voor informatie over het bijwerken van het lokale register voor dergelijke installaties.	`-Dsap.sl.bics.variableComplexSelectionMapping=n` waarbij n een interval kan zijn of meerdere waarden kan hebben. **Opmerking** Tot aan BI 4.1 SP05 was interval de standaardwaarde voor deze optie. Als u deze eigenschap aan de instellingen voor Adaptive Processing Server toevoegt en op meerdere waarden instelt, moeten de volgende acties worden uitgevoerd voor bestaande documenten: • Een document moet worden gewist. • De standaardwaarden voor queryaanwijzingen moeten worden gewijzigd zodat deze compatibel zijn met de selectie van meerdere waarden.

Eigenschappen van Toezichtservice van Web Intelligence

Eigenschap	Beschrijving	Standaardwaarde
Controle activeren	Hiermee wordt opgegeven of controle voor de service is ingeschakeld.	**TRUE**
Vertraging van toezicht op thread-lus (in seconden)	Hiermee wordt de tijdsduur in seconden opgegeven tussen pogingen van de service om clients te 'pingen'.	300
Opschoontime-out voor standaardbron met toezicht (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie wordt opgeschoond.	1200
Wisseltime-out voor standaardbron met toezicht (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie op de vaste schijf wordt gewisseld. Het is raadzaam dat u een waarde opgeeft die lager is dan de waarde voor de eigenschap Opschoontime-out voor standaardbron met toezicht (in seconden).	600
Serviceprofilering inschakelen		**TRUE**
Toezicht op serviceactiviteit inschakelen		**TRUE**

Eigenschappen van Visualization-service

Eigenschap	Beschrijving	Standaardwaarde
Time-out voor opschonen van visualisatiesysteem (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie wordt opgeschoond.	1200
Time-out voor wisselen van visualisatiesysteem (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie op de vaste schijf wordt gewisseld. Het is raadzaam dat u een waarde opgeeft die lager is dan de waarde voor de eigenschap *Time-out voor opschonen van visualisatiesysteem (in seconden)*	600

Eigenschappen van Rebean-service

Eigenschap	Beschrijving	Standaardwaarde
Geen eigenschappen		

Eigenschappen van Service voor documentherstel

Eigenschap	Beschrijving	Standaardwaarde
Geen configuratie-eigenschappen		

Eigenschappen van DSL Bridge-service

Eigenschap	Beschrijving	Standaardwaarde
Time-out van opschonen van DSLBridge-engine (in seconden)	Hiermee wordt opgegeven hoeveel seconden de service wacht op een inactieve client, voordat de clientsessie wordt opgeschoond.	1200

Instellingen voor Web Intelligence-verwerkingsserver

De instellingen voor de Web Intelligence-verwerkingsserver zijn gegroepeerd in de volgende services:

- Information Engine-service
- Web Intelligence Core
- Web Intelligence Processing
- Web Intelligence Common

De instellingen voor drempelwaarden komen in afzonderlijke tabellen aan de orde.

Eigenschappen van Information Engine-service

Eigenschap	Beschrijving	Standaardwaarde
Zoeklijstcache inschakelen	Geeft aan of de cache is ingeschakeld voor zoeklijsten op de Web Intelligence-verwerkingsserver.	**TRUE**
Batchgrootte van zoeklijst (vermeldingen)	Geeft het maximum aantal vermeldingen (of waarden) voor elke zoeklijstbatch weer.	1000
Maximumgrootte aangepaste sortering (vermeldingen)	Geeft het maximum aantal vermeldingen in de aangepaste sortering weer.	100

Eigenschap	Beschrijving	Standaardwaarde
Maximumgrootte universecache (universes)	Geeft aan hoeveel universes kunnen worden opgeslagen in het cachegeheugen van de Web Intelligence-verwerkingsserver.	20
Maximumgrootte zoeklijst (in vermeldingen)	Geeft het maximum aantal vermeldingen (of waarden) voor elke zoeklijst weer.	50000

Eigenschappen van de Web Intelligence-kernservice

Eigenschap	Beschrijving	Standaardwaarde
Time-out vóór recycling (in seconden)	Geeft aan hoeveel seconden de server niet-actief kan zijn voordat deze door de Server Intelligence Agent (SIA) wordt gestopt en opnieuw wordt gestart wanneer het totaal aantal verwerkte documenten boven de waarde komt die is ingesteld voor de eigenschap *Maximum aantal documenten vóór recycling*.	1200
Time-out niet-actief document (in seconden)	Geeft aan hoeveel seconden wordt gewacht voordat de sessie van de Web Intelligence-verwerkingsserver wordt gewisseld. Wanneer de client in deze periode geen aanvragen genereert, wordt de sessie naar de vaste schijf verplaatst, waardoor er bronnen vrijkomen voor een actieve sessie.	300 Het geldige bereik is 100 tot 10000 seconden.
Pollinginterval server (in seconden)	Geeft het interval aan, in seconden, dat moet verstrijken voordat de server zoekt naar nieuwe threadaanvragen. In de pollingfase voert de server opschoningsacties uit, zoals het wisselen van ongebruikte documenten, om het servergeheugen onder de bovenste drempelwaarde te houden.	120
Maximumaantal documenten per gebruiker	Geeft het maximum aantal actieve sessies (Web Intelligence-documenten) aan dat op elk willekeurig moment aan een gebruiker kan worden gekoppeld. Als de waarde 5 is, kan de gebruiker dus maximaal 5 actieve sessies tegelijkertijd gebruiken.	5 Het geldige bereik is 1 tot 20.
Maximumaantal documenten vóór recycling	Geeft aan hoeveel Web Intelligence-documenten kunnen worden verwerkt voordat wordt overwogen om de server te recyclen. Als het aantal verwerkte documenten is bereikt en de server niet actief is, wordt de server afgesloten en wordt door de Server Intelligence Agent (SIA) een nieuw exemplaar van de server gestart. Er treedt echter een vertraging op voordat er een nieuw exemplaar van de server wordt gestart. De vertraging wordt gedefinieerd door de eigenschap *Time-out vóór recycling*.	50
Fouten m.b.t. maximumgrootte documenttoewijzing toestaan	Geeft aan of de eigenschap `<Maximum aantal verbindingen>` beperkt is. Als deze eigenschap is ingeschakeld, wordt de waarde die is ingesteld voor de eigenschap `<Maximum aantal verbindingen>` herkend door de server; anders wordt de eigenschap genegeerd.	**TRUE**
Time-out niet-actieve verbinding (in minuten)	Geeft aan hoeveel minuten de server wacht op aanvragen van een niet-actieve verbinding. Als er een te lage waarde voor deze instelling is opgegeven, kan het gevolg zijn dat een aanvraag voortijdig wordt gesloten. Een te hoge waarde kan ertoe leiden dat aanvragen in de wachtrij worden geplaatst terwijl de server wacht totdat niet-actieve aanvragen worden gesloten.	20

Eigenschap	Beschrijving	Standaardwaarde
Maximumaantal verbindingen	Geeft het maximum aantal sessies aan dat gelijktijdig kan zijn geopend. Dit is een geschat aantal; bij deze instelling worden de inactieve sessies die worden gewisseld en de sessie die wordt gemaakt om het aantal sessies te analyseren, niet in beschouwing genomen. Als deze limiet is bereikt en er geen andere server beschikbaar is om de aanvraag te verwerken, wordt er een foutbericht weergegeven. **Opmerking** De eigenschap `<Fouten m.b.t. maximumgrootte documenttoewijzing toestaan>` moet zijn ingeschakeld om door de server te worden herkend.	200 Het geldige bereik is 5 tot 65535.
Geheugenanalyse inschakelen	Geeft aan of de functie voor geheugenanalyse is ingeschakeld. Als deze eigenschap is ingeschakeld, zijn de volgende eigenschappen actief en worden ze door de server herkend: • `<Maximale drempelwaarde geheugen>` • `<Bovenste drempelwaarde geheugen>` • `<Onderste drempelwaarde geheugen>` Wanneer het procesgeheugen van de server zich boven de waarde voor `<Bovenste drempelwaarde geheugen>` bevindt, is de enige bewerking die nog is toegestaan het opslaan van documenten. Wanneer het procesgeheugen zich boven de waarde voor `<Maximale drempelwaarde geheugen>` bevindt, worden alle bewerkingen gestopt en zijn deze mislukt.	**TRUE**
Onderste drempelwaarde geheugen (MB)	Geeft de onderste drempelwaarde voor het geheugenverbruik aan.	**3500**
Bovenste drempelwaarde geheugen (MB)	Geeft de bovenste drempelwaarde voor het geheugenverbruik aan.	**4500**
Maximale drempelwaarde geheugen (MB)	Geeft de maximale drempelwaarde voor het geheugenverbruik aan.	**6000**
Controle van APS-service inschakelen	Hiermee wordt controle van de server door de APS-service ingeschakeld, die wordt gehost op de Adaptive Processing Server.	**TRUE**
Fout bij opnieuw uitvoeren van APS-serviceping	Hiermee wordt opgegeven hoe vaak de server probeert de APS-service te bereiken alvorens te besluiten dat de service niet kan worden bereikt.	3
Threadperiode van APS-servicecontrole	Hiermee wordt de vertraging opgegeven tussen pogingen om de APS-service te bereiken.	300

Eigenschap	Beschrijving	Standaardwaarde
Huidige activiteitenlogboeken inschakelen	Hiermee wordt opgegeven of volledige traceringen in de logboekbestanden van de server worden gegenereerd. **Opmerking** Deze eigenschap moet alleen worden ingeschakeld tijdens het oplossen van problemen. Normaliter moet deze eigenschap zijn ingesteld op **ONWAAR**.	**FALSE**

Eigenschappen van Web Intelligence-verwerkingsservice

Eigenschap	Beschrijving	Standaardwaarde
Gebruik van HTTP URL inschakelen	Hiermee wordt aangegeven of de server bestanden kan oproepen die op een externe locatie zijn opgeslagen.	**TRUE**
Proxywaarde	Hiermee wordt het adres van de proxyserver van uw netwerk opgegeven. U hoeft alleen een waarde op te geven als uw netwerk een proxyserver heeft en u bestanden probeert op te roepen die op een externe locatie zijn opgeslagen.	Leeg

Eigenschappen van Algemene Web Intelligence-service

Eigenschap	Beschrijving	Standaardwaarde
Time-out van cache (in minuten)	Geeft aan hoeveel minuten wordt gewacht voordat de inhoud van de documentcache wordt leeggemaakt. De time-out is afhankelijk van de meest recente toegangsdatum per document.	4370
Opschoningsinterval documentcache (in minuten)	Geeft aan om de hoeveel minuten de documentcache wordt gescand en gecontroleerd aan de hand van de instellingen `<Maximumgrootte documentcache>`, `<Maximale verlaging opslagcapaciteit in documentcache>` en `<Maximumaantal documenten in cache>`.	120
Cache delen uitschakelen	Geeft aan of het delen van de cache is uitgeschakeld. Standaard is het delen van de cache ingeschakeld; dit betekent dat alle exemplaren van de Web Intelligence-verwerkingsserver dezelfde cache gebruiken. Als u echter liever per exemplaar van de Web Intelligence-verwerkingsserver een afzonderlijke cache gebruikt, schakelt u deze eigenschap in.	**FALSE**
Documentcache inschakelen	Geeft aan of de documentcache is ingeschakeld. Als de eigenschap is ingeschakeld, kunnen geplande Web Intelligence-documenten vooraf in de cache worden geladen.	**TRUE**
Real-time cache inschakelen	Geeft aan of de real-time cache is ingeschakeld. Als de eigenschap is ingeschakeld, kan de cache dynamisch worden geladen. Web Intelligence-documenten worden dan door de Web Intelligence-verwerkingsserver in de cache geplaatst wanneer ze worden weergegeven. De documenten worden ook in het cachegeheugen opgeslagen wanneer ze als een geplande taak worden uitgevoerd, mits de pre-cache in het document is ingeschakeld.	**TRUE**
Maximumgrootte documentcache (kB)	Geeft de maximale grootte van de documentcache weer. Wanneer deze limiet eenmaal is bereikt, wordt de documentcache leeggemaakt op basis van de eigenschap `<Maximale verlaging opslagcapaciteit in documentcache>`.	1000000

Eigenschap	Beschrijving	Standaardwaarde
Maximale verlaging opslagcapaciteit in documentcache (in procenten)	Geeft het percentage van de cache weer dat wordt vrijgemaakt om plaats te bieden aan nieuwe acties en resultaten. Documenten met de oudste "Tijd van laatste toegang" worden gewist.	70
Maximumgrootte tekststream (MB)	Geeft de maximale grootte aan van tekststreams die naar de Web Intelligence-client worden verzonden. **Opmerking** Als de waarde van de eigenschap *Maximumgrootte tekststream* is overschreden, wordt het Web Intelligence-document niet gemaakt en ontvangt de client een foutbericht.	5 Het geldige bereik is 1 tot 4095 MB.
Maximale grootte binaire stroom (MB)	Geeft de maximale grootte aan, in MB, van binaire stromen die naar de Web Intelligence-client worden verzonden. **Opmerking** Als de waarde van de eigenschap *Maximale grootte binaire stroom* is overschreden, wordt het Web Intelligence-document niet gemaakt en ontvangt de client een foutbericht.	50 Het geldige bereik is 1 tot 4095 MB.
Afbeeldingsmap	Geeft de locatie van de afbeeldingsmap aan.	Leeg
Map uitvoercache	Geeft de locatie van de cache aan.	Leeg

Algemene eigenschappen

Eigenschap	Beschrijving	Standaardwaarde
Verlooptijd van eenmalige aanmelding (in seconden)	Geeft de geldigheidsduur aan, in seconden, van een verbinding voor eenmalige aanmelding. Wanneer deze tijdsduur is verstreken, wordt de verbinding verbroken.	86400

Verwante informatie

Drempelwaarde voor geheugen Web Intelligence Server [pagina 1191]

35.1.7.1 Drempelwaarde voor geheugen Web Intelligence Server

In de volgende secties wordt beschreven wat er op een Web Intelligence-server gebeurt wanneer de waarde voor Maximale drempelwaarde geheugen, Bovenste drempelwaarde geheugen of Onderste drempelwaarde geheugen wordt bereikt.

Onderste drempelwaarde geheugen

Als de limiet voor `<Onderste drempelwaarde geheugen>` is bereikt, worden inactieve documenten door de server naar de harde schijf verplaatst en wordt er extra geheugen toegewezen aan actieve documenten. Elke gebruiker mag maximaal één actief document hebben in plaats van `<Maximumaantal documenten per gebruiker>`.

Bovenste drempelwaarde geheugen

Als deze `<Bovenste drempelwaarde geheugen>` is bereikt, worden de volgende serveracties uitgevoerd om bronnen vrij te maken en de server te beschermen:

- De server weigert nieuwe verbindingen en nieuwe clientaanroepen. Alleen het *opslaan* van Web Intelligence-documenten is toegestaan. Gebruikers die een actie aanvragen, ontvangen het bericht `Server bezet` en krijgen het advies om hun wijzigingen op te slaan.
- De server schoont het systeem op om voldoende bronnen vrij te maken, zodat de hoeveelheid toegewezen geheugen onder de limiet blijft die is ingesteld bij `<Bovenste drempelwaarde geheugen>`.
- De server probeert alleen-lezendocumenten te sluiten.
- Als er tijdens het opschonen van het systeem niet voldoende geheugen is vrijgemaakt, begint de server met het sluiten van documenten die in *Bewerkingsmodus* zijn. De server volgt hierbij het LIFO-principe: het meest recente actieve document wordt als eerste uit het geheugen verwijderd. De server gaat door met het sluiten van documenten totdat er een veilig niveau is bereikt; dit niveau is gebaseerd op de volgende berekening: `<Bovenste drempelwaarde geheugen>` - (20%*(`<Bovenste drempelwaarde geheugen>`)). Als de eigenschap Bovenste drempelwaarde geheugen bijvoorbeeld is ingesteld op 4500 MB, is het veilige niveau:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  De server kan geen documenten sluiten als er een clientaanroep actief is. Documenten die worden vernieuwd of worden geëxporteerd naar een andere indeling of waarvoor een andere tijdrovende bewerking wordt uitgevoerd worden niet gesloten wanneer de server deze drempelwaarde bereikt. Als de server onvoldoende geheugen kan herstellen en nog steeds boven de `<Bovenste drempelwaarde geheugen>` uitkomt, wordt hij opnieuw gestart.

Maximale drempelwaarde geheugen

Als de limiet <Maximale drempelwaarde geheugen> is bereikt, worden alle actieve bewerkingen afgebroken. Alle clientaanroepen worden beëindigd. Nadat een aanroep is beëindigd, wordt het bijbehorende document gesloten.

36 Bijlage Servergegevens

36.1 Informatie over de bijlage Servergegevens

In deze bijlage verwijst de term server, tenzij anders vermeld, naar een SAP BusinessObjects-server en niet naar de computer waarop het BI-platform is geïnstalleerd of wordt uitgevoerd.

Servergegevens zijn niet beschikbaar op servers die niet actief zijn.

Naast de gegevens die in deze bijlage worden beschreven, kan de toepassing Toezicht ook de volgende serverstatussen controleren:

Serverstatus	Beschrijving
Gezondheidsstatus	De Gezondheidsstatus geeft de algemene status van een server aan. Dit zijn de mogelijke waarden: • 0 = Rood (gevaar) • 1 = Oranje (waarschuwing) • 2 = Groen (gezond)
Ingeschakelde status van server	Deze status geeft aan of een server in- of uitgeschakeld is. Dit zijn de mogelijke waarden: • 0 = Uitgeschakeld • 1 = Ingeschakeld
Actieve status van server	Deze status geeft de actieve status van een server aan. Dit zijn de mogelijke waarden: • 0 = GESTOPT • 1 = WORDT GESTART • 2 = WORDT GEÏNITIALISEERD • 3 = ACTIEF • 4 = WORDT GESTOPT • 5 = MISLUKT • 6 = WORDT UITGEVOERD MET FOUTEN • 7 = WORDT UITGEVOERD MET WAARSCHUWINGEN

36.1.1 Algemene servergegevens

De volgende gegevens beschrijven de computer waarop de opgegeven server wordt uitgevoerd.

Computerspecifieke gegevens

Gegeven	Beschrijving
Computernaam	De hostnaam van de computer waarop de server wordt uitgevoerd.
Besturingssysteem	Het besturingssysteem van de computer waarop de server wordt uitgevoerd.
CPU-type	Het type CPU van de computer waarop de server wordt uitgevoerd. Dit gegeven is niet beschikbaar op Adaptive Processing Servers of Web Application Container Servers (WACS).
CPU's	Het aantal CPU's dat beschikbaar is voor de server. In multikernhardware kan dit gegeven het aantal logische CPU's aangeven, en niet het aantal fysieke processoren. Dit gegeven is niet beschikbaar op Adaptive Processing Servers of Web Application Container Servers (WACS).
Aantal kernen	Geeft het aantal kernen in een computer weer waarop de BI-platformserver wordt gehost.
RAM (MB)	De hoeveelheid geheugen in megabyte die beschikbaar is op de computer waarop de server wordt uitgevoerd. Dit gegeven is niet beschikbaar op Adaptive Processing Servers of Web Application Container Servers (WACS).
Plaatselijke tijd	De plaatselijke tijd.
Schijfgrootte (GB)	De grootte van de schijf waarop het BI-platform is geïnstalleerd, in gigabytes. Dit gegeven is niet beschikbaar op Adaptive Processing Servers of Web Application Container Servers (WACS).
Gebruikte schijfruimte (GB)	De hoeveelheid gebruikte schijfruimte, in gigabytes, waarop het BI-platform is geïnstalleerd. Hieronder valt schijfruimte die wordt gebruikt door andere programma's op de computer, en niet alleen de ruimte die wordt gebruikt door het BI-platform. Dit gegeven is niet beschikbaar op Adaptive Processing Servers of Web Application Container Servers (WACS).

Met de volgende gegevens wordt de opgegeven SAP BusinessObjects-server beschreven.

Serverspecifieke gegevens

Gegeven	Beschrijving
Name Server	De naam en het poortnummer van de CMS-server waarnaar deze server zijn adres publiceert.
Geregistreerde naam	De interne naam van de server. Dit is niet de naam die wordt weergegeven in het venster *Servers* van de CMC.
Versie	De versie van de server.
Starttijd	De tijd waarop de server voor de laatste keer is gestart.
PID	De unieke proces-id van de server. Het besturingssysteem van de computer waarop de server wordt uitgevoerd, genereert de PID. De PID kan worden gebruikt om de specifieke server te identificeren.
Hostnaam	Een door komma's gescheiden lijst van hostnamen die momenteel door de server worden gebruikt.
Host-IP-adres	Een door komma's gescheiden lijst van IP-adressen waarop de server naar aanvragen luistert.

Gegeven	Beschrijving
Poort voor aanvragen	Via deze poort ontvangt de server aanvragen van andere servers. Als de server naar verzoeken op meer dan één IP-adres luistert, is de poort voor aanvragen voor de server altijd hetzelfde. Als deze poort voor aanvragen door een ander proces wordt gebruikt, wordt de server niet gestart. Zorg dat deze poort niet door andere processen wordt gebruikt.
Serverthreads bezet	Het aantal servicethreads dat momenteel een aanvraag afhandelt. Als dit aantal gelijk is aan de maximumgrootte van de threadpool van de server, duidt dit erop dat het systeem aanvullende aanvragen niet gelijktijdig kan verwerken en dat nieuwe aanvragen moeten wachten totdat bezette threads weer beschikbaar worden.

Controlegegevens

Gegeven	Beschrijving
Huidig aantal controlegebeurtenissen in wachtrij	Het aantal controlegebeurtenissen dat door een controleobject is vastgelegd, maar dat nog niet is opgehaald door de CMS-controleur. Als dit aantal blijft toenemen, kan dit erop wijzen dat de functie Controle niet correct is geconfigureerd of dat het systeem zwaar belast is en controlegebeurtenissen sneller worden genereerd dan dat deze door de controleur kunnen worden opgehaald. **Opmerking** Wanneer u een server stopt, moet u deze eerst uitschakelen en wachten tot de gegegevens “0” bereiken. Anders blijven controlegebeurtenissen mogelijk in de wachtrij staan en bereiken deze Gegevensopslag controleren niet totdat de server opnieuw is gestart en de CMS navraag ervoor heeft gedaan.

Servicegegevens registreren in logboek

Gegeven	Beschrijving
Logboekmap	Op deze locatie zijn logboekbestanden voor de server beschikbaar.

36.1.2 Gegevens van Central Management Server

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor Central Management Servers (CMS).

Gegevens van Central Management Server

Gegeven	Beschrijving
Verbinding met controledatabase is tot stand gebracht	Geeft aan of de CMS een goede verbinding heeft met de controledatabase. Een waarde van “1” geeft aan dat er een verbinding is. Een waarde van “0” geeft aan dat er geen verbinding is met de controledatabase. Als de CMS een auditor is, moet deze waarde “1” zijn. Als de waarde “0” is, moet u nagaan waarom er geen verbinding met de controledatabase tot stand kan worden gebracht.

Gegeven	Beschrijving
CMS-controleur	Geeft aan of de CMS als controleur fungeert. Een waarde van “1” geeft aan dat de CMS als een controleur fungeert. Een waarde van “0” geeft aan dat de CMS niet als een controleur fungeert.
Naam verbinding controledatabase	De naam van de verbinding van de controledatabase. Dit hoeft niet de naam van de controledatabase zelf te zijn. Als dit gegeven leeg is, wil dit zeggen dat er geen verbinding met de controledatabase tot stand gebracht kan worden.
Naam gebruiker controledatabase	De naam van de gebruikersaccount die is gebruikt om verbinding te maken met de controledatabase.
Controledatabase laatst bijgewerkt op	De meest recente datum en tijd waarop de CMS met succes is gestart om gebeurtenissen uit een controleobject op te halen. Als de CMS een auditor is, moeten deze gegevens een tijd weergeven rond het tijdstip waarop het venster “Gegevens” is geladen. Als de waarde meer dan twee uur is voordat de pagina werd geladen, werkt de controle mogelijk niet goed.
Duur laatste pollingcyclus controlethread (seconden)	De duur van de laatste pollingcyclus in seconden. Dit geeft de maximale vertraging aan waarmee gebeurtenisgegevens de controledatabase hebben bereikt gedurende de vorige pollingcyclus. • Een waarde van minder dan 20 minuten duidt op een gezond systeem. • Een waarde tussen de 20 minuten en 2 uur duidt op een drukbezet systeem. • Een waarde van ruim 2 uur duidt op een zeer drukbezet systeem. Als deze status blijft bestaan en u de vertraging te lang vindt, wordt u aanbevolen om uw implementatie bij te werken, zodat de controledatabase gegevens met een hogere snelheid ontvangt, of het aantal controlegebeurtenissen te verlagen dat door uw systeem wordt getraceerd.
Thread-gebruik controleren	Het percentage van de pollingcyclus dat door de CMS-controleur wordt gebruikt om gegevens uit controleobjecten te verzamelen. De overige tijd is rusttijd tussen polls. Als deze waarde de 100% bereikt, verzamelt de controleur nog steeds gegevens van de controleobjecten wanneer de volgende poll van start zou moeten gaan. Dit kan ertoe leiden dat de gebeurtenissen de controledatabase met vertraging bereiken. Als het threadgebruik regelmatig 100% bereikt en verschillende dagen op dit niveau blijft, wordt u aanbevolen om uw implementatie bij te werken, zodat de controledatabase gegevens met een hogere snelheid ontvangt, of het aantal controlegebeurtenissen te verlagen dat door uw systeem wordt getraceerd.
Geclusterde CMS-servers	Een lijst met de hostnamen en poortnummers van de actieve Central Management Servers in het cluster, door puntkomma's gescheiden.
Aantal sessies tot stand gebracht door gelijktijdige gebruikers	Het totaalaantal sessies voor gebruikers met een licentie voor gelijktijdige toegang.
Aantal sessies tot stand gebracht door gebruikers met naam	Het totale aantal sessies voor gebruikers met een licentie op naam.
Piekaantal gebruikerssessies na opstarten	Het piekaantal gelijktijdige gebruikerssessies dat de CMS heeft verwerkt sinds het opstarten.

Gegeven	Beschrijving
Aantal sessies tot stand gebracht door servers	Het aantal gelijktijdige sessies dat door BI-platformservers tot stand is gebracht met de CMS. Maak een aanvullende CMS als dit aantal hoger is dan 250.
Aantal sessies tot stand gebracht door alle gebruikers	Het aantal gelijktijdige gebruikerssessies dat door de CMS wordt verwerkt op het moment dat het venster *Gegevens* wordt geladen. Hoe groter dit aantal is, hoe groter het aantal gebruikers is dat het systeem gebruikt. Maak een aanvullende CMS als dit aantal hoger is dan 250.
Mislukte taken	Het aantal mislukte taken in het systeem.
Uitstaande taken	Het aantal taken dat is gepland, maar nog niet gereed om te worden uitgevoerd omdat de geplande tijd of gebeurtenis nog niet is geweest.
Actieve taken	Het aantal actieve taken.
Voltooide taken	Het aantal voltooide taken in het systeem.
Wachtende taken	Het aantal taken in het systeem die zijn gepland en wachten op beschikbare bronnen.
Gebruikerslicenties voor gelijktijdige toegang	Het aantal gebruikerslicenties voor gelijktijdige toegang zoals aangegeven door de sleutelcode.
Gebruikerslicenties op naam	Het aantal gebruikerslicenties op naam zoals aangegeven door de sleutelcode.
Builddatum	De builddatum van de CMS.
Naam van systeemdatabaseverbinding	De naam van de verbinding van de CMS-systeemdatabase. Dit hoeft niet de naam van de CMS-systeemdatabase zelf te zijn.
Servernaam van systeemdatabase	De naam van de server waarop de CMS-systeemdatabase wordt uitgevoerd. Dit hoeft niet de naam van de CMS-systeemdatabase zelf te zijn.
Gebruikersnaam voor systeemdatabase	De naam van de gebruikersaccount die is gebruikt om verbinding te maken met de CMS-systeemdatabase.
Naam gegevensbron	De naam van de verbinding van de CMS-systeemdatabase.
Buildnummer	Het buildnummer van de CMS. Op basis van dit nummer kunt u zien welke versie van SAP BusinessObjects Business Intelligence-platform u hebt geïnstalleerd.
Productversie	De productversie van de CMS.
Bronversie	De bronversie van de CMS.
Gemiddelde antwoordtijd voor toewijzingen na opstarten (msec)	De gemiddelde tijd in milliseconden die de CMS nodig heeft gehad om toewijzingen uit te voeren sinds het opstarten van de server. Een antwoordtijd van meer dan 1000 milliseconden kan erop wijzen dat de CMS of de CMS-systeemdatabase moet worden afgestemd.
Gemiddelde antwoordtijd voor query na opstarten (msec)	De gemiddelde tijd in milliseconden die de CMS nodig heeft gehad om query's uit te voeren sinds het opstarten van de server. Een antwoordtijd van meer dan 1000 milliseconden kan erop wijzen dat de CMS of de CMS-systeemdatabase moet worden afgestemd.
Langste antwoordtijd voor toewijzing na opstarten (msec)	De langste tijd in milliseconden die de CMS nodig heeft gehad om toewijzingen uit te voeren sinds het opstarten van de server. Een antwoordtijd van meer dan 10000 milliseconden kan erop wijzen dat de CMS of de CMS-systeemdatabase moet worden afgestemd.

Gegeven	Beschrijving
Langste antwoordtijd voor query na opstarten (msec)	De langste tijd in milliseconden die de CMS nodig heeft gehad om query's uit te voeren sinds het opstarten van de server. Een antwoordtijd van meer dan 10000 milliseconden kan erop wijzen dat de CMS of de CMS-systeemdatabase moet worden afgestemd.
Aantal toewijzingen na opstarten	Het aantal toewijzingen aan de CMS-systeemdatabase sinds het opstarten van de server.
Aantal query's na opstarten	Het totale aantal databasequery's sinds het opstarten van de server. Een groot aantal kan erop wijzen dat het systeem zeer actief of zwaar belast is.
Aantal gebruikersaanmeldingen na opstarten	Het aantal gebruikersaanmeldingen sinds de server is gestart. Een groot aantal kan erop wijzen dat het systeem zeer actief of zwaar belast is.
Tot stand gebrachte systeemdatabaseverbindingen	Het aantal verbindingen met de CMS-systeemdatabase dat door de CMS tot stand kon worden gebracht. Als een databaseverbinding wordt verbroken, probeert de CMS de verbinding te herstellen. Als het aantal tot stand gebrachte databaseverbindingen consistent lager is dan het aantal systeemdatabaseverbindingen dat is opgegeven voor de eigenschap *Aantal gevraagde systeemdatabaseverbindingen* (in de sectie *Central Management-service* van het venster *Eigenschappen*), kan dit erop wijzen dat de CMS geen aanvullende verbindingen kan verkrijgen en dat het systeem niet optimaal functioneert. Een mogelijke oplossing is de databaseserver te configureren zodat meer databaseverbindingen voor de CMS worden toegestaan.
Momenteel gebruikte systeemdatabaseverbindingen	Het aantal verbindingen met de CMS-systeemdatabase dat momenteel door de CMS wordt gebruikt. Het aantal verbindingen dat momenteel wordt gebruikt, kan lager zijn dan of gelijk zijn aan het aantal tot stand gebrachte systeemdatabaseverbindingen. Als het aantal tot stand gebrachte verbindingen en het aantal gebruikte verbindingen gedurende een bepaalde tijd hetzelfde zijn, kan dit wijzen op een probleem. Het verhogen van de waarde voor de eigenschap *Aantal gevraagde systeemdatabaseverbindingen* in het venster *Eigenschappen* kan de prestaties van de CMS verbeteren. Het afstemmen van de CMS-systeemdatabase helpt mogelijk ook om de prestaties te verbeteren.
Uitstaande systeemdatabaseverzoeken	Het aantal verzoeken voor de CMS-systeemdatabase dat op een beschikbare verbinding wacht. Als dit aantal hoog is, kunt u overwegen de waarde voor de eigenschap *Aantal gevraagde systeemdatabaseverbindingen* te verhogen. Het afstemmen van de CMS-systeemdatabase helpt mogelijk ook om de prestaties te verbeteren.
Aantal objecten in CMS-systeemcache	Het totale aantal objecten dat zich momenteel in de CMS-systeemcache bevindt.
Aantal objecten in CMS-systeemdatabase	Het totale aantal objecten dat zich momenteel in de CMS-systeemdatabase bevindt.
Bestaande gelijktijdige gebruikersaccounts	Het totale aantal bestaande gebruikers met een licentie voor gelijktijdige toegang tot het cluster.
Bestaande gebruikersaccount op naam	Het totale aantal bestaande gebruikers met een licentie op naam in het cluster.

36.1.3 Gegevens van verbindingsserver

De volgende gegevens zijn specifiek voor de verbindingsserver.

Gegevens van verbindingsservice

Gegeven	Beschrijving
Gegevensbronnen	Hiermee wordt in een tabel weergegeven welke gegevensbronnen geactiveerd zijn via de pagina *Eigenschappen*. Hiermee worden de volgende gegevens voor elke netwerklaag en elk databasepaar weergegeven: • *Status* (*Geladen* of *Mislukt!*): huidige status van het stuurprogramma • *Beschikbare verbindingen: aantal poolverbindingen dat gebruikt kan worden* • *Taken (CORBA): aantal taken dat wordt verwerkt (implementatie met twee lagen)* • *Taken (CORBA): aantal taken dat wordt verwerkt (weblaagimplementatie)* **Opmerking** Raadpleeg de *Handleiding voor gegevenstoegang* voor meer informatie over verbindingspools.

36.1.4 Gegevens van Event Server

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor Event Servers.

Gegevens van gebeurtenisservice

Gegeven	Beschrijving
Lijst met bewaakte bestanden	Een tabel waarin de lijst met bestanden wordt weergegeven die momenteel worden gecontroleerd door de Event Server. In de kolom “Bestandsnaam” worden de bestandsnaam en het -pad weergegeven. In de kolom “Tijdstip laatste melding” wordt de recentste tijdstempel weergegeven waarop de server een poll heeft uitgevoerd en heeft bepaald dat het bestand bestaat.
Bewaakte bestanden	Het totale aantal bestanden dat momenteel door de Event Server wordt bewaakt.

36.1.5 Gegevens van File Repository Server

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor Input en Output File Repository.

Gegevens van Filestore-service

Gegeven	Beschrijving
Actieve bestanden	Het aantal bestanden in de File Repository Server dat momenteel actief is.
Geschreven gegevens (MB)	Het totale aantal megabytes dat naar bestanden op de server is geschreven.

Gegeven	Beschrijving
Verzonden gegevens (MB)	Het totale aantal megabytes dat van bestanden op de server is gelezen.
Lijst met actieve bestanden	Een tabel waarin de bestanden in de File Repository weergegeven worden die momenteel openstaan.
Actieve verbindingen	Het totale aantal actieve verbindingen van clients met andere servers.
Vrije schijfruimte in hoofdmap (GB)	De totale hoeveelheid beschikbare ruimte (in gigabytes) op de schijf die het uitvoerbare bestand van de server bevat.
Vrije schijfruimte in hoofdmap (GB)	De totale hoeveelheid vrije schijfruimte (in gigabytes) op de schijf die het uitvoerbare bestand van de server bevat.
Totale schijfruimte in hoofdmap (GB)	De totale hoeveelheid ruimte (in gigabytes) op de schijf die het uitvoerbare bestand van de server bevat.
Vrije schijfruimte in hoofdmap (%)	De totale hoeveelheid beschikbare ruimte (in procent) op de schijf die het uitvoerbare bestand van de server bevat.

36.1.6 Gegevens van Adaptive Processing Server

In de volgende tabel worden de servergegevens beschreven, die worden weergegeven in het venster *Gegevens* voor Adaptive Processing Servers.

Gegevens van Adaptive Processing Server

Gegeven	Beschrijving
Threads in transportlaag	Het totale aantal threads in alle threadpools van de transportlaag.
Grootte van threadpool van transportlaag	Het totale aantal gedeelde threads in de transportlaag. Deze threads kunnen door alle gehoste services op de Adaptive Processing Server worden gebruikt.
Beschikbare processoren	Het aantal processors dat beschikbaar is voor JVM (Java Virtual Machine) waarop de server wordt uitgevoerd.
Maximumgeheugen (MB)	De maximale hoeveelheid geheugen, in megabyte, die de Java Virtual Machine probeert te gebruiken.
Vrij geheugen (MB)	De hoeveelheid geheugen, in megabyte, die beschikbaar is in de JVM voor het toewijzen van nieuwe objecten.
Totaal geheugen (MB)	De totale hoeveelheid geheugen, in megabyte, in de Java Virtual Machine. Deze waarde kan, afhankelijk van de hostomgeving, gedurende een bepaalde periode verschillen.
Percentage van CPU-gebruik (laatste 5 minuten)	Het percentage van het totale CPU-gebruik dat door de server is verbruikt gedurende de laatste vijf minuten. Als bijvoorbeeld een enkele thread één CPU van een uit vier CPU's bestaand systeem volledig gebruikt, bedraagt het gebruik 25%. Er wordt rekening gehouden met alle processen die aan de JVM zijn toegewezen. Een waarde boven de 80% kan duiden op een CPU-knelpunt.
Percentage van CPU-gebruik (laatste 15 minuten)	Het percentage van het totale CPU-gebruik dat door de server is verbruikt gedurende de laatste 15 minuten. Als bijvoorbeeld een enkele thread één CPU van een uit vier CPU's bestaand systeem volledig gebruikt, bedraagt het gebruik 25%. Er wordt rekening gehouden met alle processen die aan de JVM zijn toegewezen. Een waarde boven de 70% kan duiden op een knelpunt.

Gegeven	Beschrijving
Percentage gestopt systeem tijdens GC (laatste 5 minuten)	Het percentage gestopt systeem tijdens de laatste vijf minuten dat GC (Schijfopruiming) werd uitgevoerd. Bij deze status kunnen APS-services niet worden uitgevoerd wanneer de JVM een cruciaal stadium uitvoert of afval verzamelt, waarvoor exclusief toegang vereist is. Meestal geeft een lage waarde met een enkel cijfer het normale gedrag aan, zelfs bij belasting. Een waarde met twee cijfers gedurende een bepaalde periode kan een lage doorvoer aangeven en moet worden onderzocht.
Percentage gestopt systeem tijdens schijfopruiming (laatste 15 minuten)	Het percentage gestopt systeem tijdens de laatste vijftien minuten dat schijfopruiming werd uitgevoerd. Bij deze status kunnen APS-services niet worden uitgevoerd wanneer de JVM een cruciaal stadium uitvoert of afval verzamelt, waarvoor exclusief toegang vereist is. Meestal geeft een lage waarde met een enkel cijfer het normale gedrag aan, zelfs bij belasting. Een waarde met twee cijfers gedurende een bepaalde periode kan een lage doorvoer aangeven en moet worden onderzocht.
Aantal paginafouten tijdens schijfopruiming (laatste 5 minuten)	Het aantal paginafouten dat is opgetreden terwijl schijfopruiming de laatste vijf minuten werd uitgevoerd. Elke waarde hoger dan 0 geeft aan dat het systeem zwaar wordt belast en weinig geheugen vrij heeft.
Aantal paginafouten tijdens schijfopruiming (laatste 15 minuten)	Het aantal paginafouten dat is opgetreden terwijl schijfopruiming de laatste vijftien minuten werd uitgevoerd. Elke waarde hoger dan 0 geeft aan dat het systeem zwaar wordt belast en weinig geheugen vrij heeft.
Aantal complete GC's	Het aantal complete schijfopruimingen sinds de server is gestart. Een snelle toename van deze waarde kan duiden op een systeem dat weinig geheugen vrij heeft.
JVM-telling van vergrendelingsconflicten	Het aantal gesynchroniseerde objecten met threads die op toegang wachten. Elke waarde die consistent hoger is dan 0 kan wijzen op threads die niet opnieuw worden uitgevoerd. Voer een threaddump uit voor meer informatie over de oorzaak van dit probleem.
JVMS-foutopsporingsinformatie	Foutopsporingsinformatie over de SAP Java Virtual Machine, inclusief de status, poort en gekoppelde client, indien beschikbaar.
JVM-versiegegevens	Versiegegevens over de SAP Java Virtual Machine.
JVM-teller voor vergrendelde threads	Het aantal threads dat is vergrendeld. Elke waarde die hoger is dan 0 geeft aan dat threads niet opnieuw worden uitgevoerd. Voer een threaddump uit voor meer informatie over de oorzaak van dit probleem.
JVM-traceringsvlaggen	De traceringsvlaggen die momenteel zijn ingeschakeld voor de JVM. Dit geeft het traceringsniveau van de JVM aan.
Services	Een door komma's gescheiden lijst van de services die door de server worden gehost.

Gegevens van DSL Bridge-service

Gegeven	Beschrijving
DSLServiceMetrics.queryCount	Het aantal gegevensaanvragen dat openstaat tussen clients en de service
DSLServiceMetrics.activeConnectionCount	Het aantal verbindingen dat openstaat tussen clients en de service.
DSLServiceMetrics.activeSessionCount	Het aantal sessies dat openstaat tussen clients en de service.

Gegeven	Beschrijving
DSLServiceMetrics.activeOLAPConnectionCount	Het aantal verbindingen dat openstaat tussen OLAP-clients en de service.

Gegevens van proxyservice voor clientcontrole

Gegeven	Beschrijving
Aantal controlegebeurtenissen die zijn ontvangen na het starten van de server	Het aantal controlegebeurtenissen van de client dat door de server is ontvangen sinds deze is gestart. Dit gegeven kan worden gebruikt om te verifiëren of de clientcontrole op de juiste wijze is geconfigureerd. Waarden groter dan "0" geven aan dat de controlegebeurtenissen van client zijn doorgestuurd via deze service voor clientcontrole.

Servicegegevens voor Platform zoeken

Gegeven	Beschrijving
Aantal geslaagde uitpakpogingen sinds de service is gestart	Het aantal geslaagde pogingen voor het uitpakken van documenten sinds de service Platform zoeken is gestart.
Tijdstempel van laatste index-update	De datum en tijd waarop de index voor het laatst is bijgewerkt.
Tijdstempel van laatste generatie inhoudsopslag	De datum en tijd waarop de laatste inhoudsopslag is gegenereerd.
Aantal mislukte uitpakpogingen sinds de service is gestart	Het aantal mislukte pogingen voor het uitpakken van documenten sinds de service Platform zoeken is gestart.
Service beschikbaar	WAAR als de service beschikbaar is. Als dit niet het geval is, ONWAAR.
Indexering wordt uitgevoerd	WAAR als de indexering wordt uitgevoerd. Als dit niet het geval is, ONWAAR.
Aantal geïndexeerde documenten	Hier wordt het aantal documenten weergegeven die geïndexeerd zijn sinds de service is gestart.

Multi-Dimensional Analysis Service-gegevens

Gegeven	Beschrijving
Aantal sessies	Het huidige aantal verbindingen van MDAS-clients met de server.
Aantal kubussen	Het aantal gegevensbronnen dat gebruikt wordt voor het verstrekken van gegevens aan verbindingen waarvoor geen time-out is opgetreden.
Aantal query's	Het aantal gegevensaanvragen dat openstaat tussen MDAS-clients en de server.

Data Federator Service-gegevens

Gegeven	Beschrijving
Aantal actieve query's	Het totaalaantal actieve query's (die al dan niet geheugen gebruiken).
Aantal verbindingen	Het totaalaantal gebruikersverbindingen met de query-engine van Data Federator.
Totaalaantal bytes overgebracht van gegevensbronnen	Het aantal gegevens gelezen uit de gegevensbronnen (in bytes).
Totaalaantal records overgebracht van gegevensbronnen	Het totaalaantal rijen gelezen uit de gegevensbronnen.

Gegeven	Beschrijving
Totaalaantal bytes geproduceerd door queryuitvoering	De hoeveelheid gegevens geproduceerd als uitvoer van query's (in bytes).
Totaalaantal records geproduceerd door queryuitvoering	Het totaalaantal records geproduceerd als uitvoer van query's.
Aantal queries die geheugen verbruiken	Het totaalaantal actieve queries die geheugen verbruiken.
Totaalaantal bytes geheugen gebruikt door queryuitvoering	De hoeveelheid geheugen die momenteel door de actieve query's wordt verbruikt (in bytes).
Totaalaantal bytes schijfruimte gebruikt door queryuitvoering	De hoeveelheid schijfruimte die momenteel door de actieve query's wordt verbruikt (in bytes).
Aantal queries die schijfruimte gebruiken	Het totaalaantal actieve queries die schijfruimte gebruiken.
Aantal queries die op bronnen wachten	Het totaalaantal actieve query's die wachten op uitvoering.
Aantal actieve threads	Het totaalaantal actieve threads die gebruikt worden voor de uitvoer van query's.
Totaalaantal bytes geheugen gebruikt door metagegevenscache	De hoeveelheid geheugen die gebruikt wordt voor het in cache plaatsen van metagegevens, statistieken en connectorconfiguratie (in bytes).
Aantal mislukte query's	Het totaalaantal mislukte query's (uitzondering opgeworpen).
Aantal query's in de stap voor queryanalyse	Het totaalaantal actieve query's die zich momenteel in de stap voor queryanalyse bevinden.
Aantal query's in de stap voor queryoptimalisatie	Het totaalaantal actieve query's die zich momenteel in de stap voor optimalisatie bevinden.
Aantal query's in de stap voor queryuitvoering	Het totaalaantal actieve query's die zich momenteel in de stap voor uitvoering bevinden.
Aantal geladen connectors	Het totaalaantal geladen connectors in de service.
Aantal actieve verbindingen met geladen connectors	Het totaalaantal actieve verbindingen met connectors die in de service geladen zijn.
Data Federation Service is available	*WAAR* als de service beschikbaar is. Als dit niet het geval is, *FALSE*.

Gegevens van verbindingsservice

Gegeven	Beschrijving
Gegevensbronnen	Hiermee wordt in een tabel weergegeven welke gegevensbronnen geactiveerd zijn via de pagina *Eigenschappen*. Hiermee worden de volgende gegevens voor elke netwerklaag en elk databasepaar weergegeven: • Status ("Geladen" of "Mislukt"): de huidige status van het stuurprogramma. • Beschikbare verbindingen: het aantal poolverbindingen dat kan worden gebruikt. • Taken (CORBA): het aantal taken dat wordt verwerkt (in een implementatie met twee lagen). • Taken (HTTP): het aantal taken dat wordt verwerkt (in een implementatie met weblagen). Raadpleeg de *Handleiding voor gegevenstoegang* voor meer informatie over verbindingspools.

Gegevens van toezichtservice

Gegeven	Beschrijving
Gemiddelde berekeningstijd van controlestatus voor de laatste 15 cycli (msec)	De gemiddelde tijd die is vereist voor berekening van de controlestatus voor de laatste 15 cycli voor dit exemplaar van de toezichtservice.
Aantal door gebruiker gemaakte gegevens	Het totaalaantal door de gebruiker gemaakte gegevens in het cluster voor alle gebruikers.
Aantal controles	Het totaalaantal controles in het cluster, inclusief uit- en ingeschakelde controles.
serviceBean.monitoringAppPropEnabled	TRUE als de toezichtfunctie is ingeschakeld. Anders FALSE. Dit gegeven komt overeen met de instelling op de eigenschappenpagina van de toezichtservice in de CMC.
Vernieuwingsinterval voor toezichtgegevens (seconden)	Het vernieuwingsinterval dat momenteel wordt gebruikt door dit exemplaar van de toezichtservice. Tijdens het opstarten van de service wordt dit gegeven geïnitialiseerd naar de instelling op de eigenschappenpagina van de toezichtfunctie in de CMC op dat moment. Op andere tijdstippen kan dit gegeven dus afwijken van de huidige instelling op de CMC-pagina.
Service beschikbaar	TRUE als deze toezichtservice actief is. Anders FALSE. Slechts één toezichtservice is actief in het cluster.
Aantal gegevens waarvoor trending is uitgevoerd	Het totaalaantal gegevens dat momenteel wordt geregistreerd in de controledatabase.

Gegevens van BEx-webtoepassingsservice

Gegeven	Beschrijving
Aantal sessies	Een telling van het totaalaantal actieve sessies in een BEx-webtoepassingsservice.

36.1.7 Gegevens van containerserver voor webtoepassingen

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor containerservers voor webtoepassingen.

> **Opmerking**
>
> Voor containerserver voor webtoepassingen gelden ook alle gegevens die zijn beschreven in de sectie Gegevens van Adaptive Processing Server.

Gegevens van containerserver voor webtoepassingen

Gegeven	Beschrijving
Lijst met uitgevoerde WACS-connectors	Een lijst met alle actieve connectors op de server. Als u niet alle connectors (HTTP, HTTPS en HTTP via proxy) ziet, geeft dit aan dat de connector niet is ingeschakeld of dat deze is mislukt tijdens het opstarten.
Serverconnectors mislukt bij opstarten	Geeft aan of er connectors zijn mislukt. Bij een positieve uitslag kan minimaal één connector niet worden gestart. Bij een negatieve uitslag zijn alle connectors actief. Voer een server niet uit als een of meer connectors niet zijn gestart. Los de problemen met de server op om ervoor te zorgen dat alle connectors goed starten.

Verwante informatie

Gegevens van Adaptive Processing Server [pagina 1200]

36.1.8 Gegevens van Adaptive Job Server

Gegevens voor Job Server

Gegeven	Beschrijving
Ontvangen taakaanvragen	Het aantal taken dat op de server zou moeten zijn uitgevoerd.
Gelijktijdige taken	Het aantal taken dat momenteel op de server wordt uitgevoerd. Als het aantal hoog is, is de server bezet.
Piektaken	Het maximumaantal gelijktijdige taken dat tegelijkertijd is uitgevoerd op de server. Dit aantal gaat pas weer omlaag als de server opnieuw is gestart.
Mislukte pogingen om taak te maken	Het aantal taken dat is mislukt op de server.
Tijdelijke map	De map waarin tijdelijke bestanden worden gemaakt. Deze kan worden opgegeven in het venster *Eigenschappen* voor de server. Als deze map niet voldoende ruimte biedt, kunnen zich problemen voordoen.
Standaardinstellingen bestandssysteemdoel geldig	*TRUE* als de server documenten kan verzenden naar het bestandssysteem van het doel dat is opgegeven in het venster *Doel* voor de server. Als dit niet het geval is, *FALSE*.

Gegeven	Beschrijving
Standaardinstellingen van FTP-doel geldig	*TRUE* als de server documenten kan verzenden naar het doel van de FPT-server dat is opgegeven in het venster *Doel* voor de server. Als dit niet het geval is, *FALSE*.
Standaardinstellingen SFTP-doel geldig	*TRUE* als de server documenten kan verzenden naar het doel van de SFTP-server dat is opgegeven in het venster *Doel* voor de server. Als dit niet het geval is, *FALSE*. Er kunnen problemen optreden als de fingerprint niet overeenkomt met de SFTP-server.
Standaardinstellingen Postvak IN van doel geldig	*TRUE* als de server documenten kan verzenden naar het Postvak IN van het doel dat is opgegeven in het venster *Doel* voor de server. Als dit niet het geval is, *FALSE*.
Standaardinstellingen e-maildoel geldig	*TRUE* als de server documenten kan verzenden naar de e-mail van het doel dat is opgegeven in het venster *Doel* voor de server. Als dit niet het geval is, *FALSE*.
Planningsservices	Een tabel waarin de actieve services op de server worden weergegeven.
Onderliggende elementen	Een tabel waarin de actieve onderliggende processen op de server worden weergegeven.

In de volgende tabel worden de gegevens voor elke actieve planningsservice op de server weergegeven.

Servicegegevens plannen

Gegeven	Beschrijving
Planningsservice	De naam van de service.
Ontvangen taakaanvragen	Het aantal taken dat op de service zou moeten zijn uitgevoerd.
Gelijktijdige taken	Het aantal taken dat momenteel gelijktijdig op de service wordt uitgevoerd. Als het aantal hoog is, is de service bezet.
Piektaken	Het maximumaantal gelijktijdige taken dat tegelijkertijd is uitgevoerd op de service.
Toegestaan maximumaantal gelijktijdige taken	Het aantal onafhankelijke processen (onderliggende processen) dat de service gelijktijdig kan verwerken. Deze kan worden opgegeven in het venster *Eigenschappen* voor de server.
Mislukte pogingen om taak te maken	Het aantal taken dat is mislukt op de service.

In de volgende tabel worden de gegevens voor elk actief onderliggend proces op de server weergegeven.

Onderliggende gegevens

Gegeven	Beschrijving
Planningsservice	De naam van het onderliggende proces.
PID	De id van het onderliggende proces
Ontvangen taakaanvragen	Het aantal taken dat in het onderliggende proces zou moeten zijn uitgevoerd.
Gelijktijdige taken	Het aantal taken dat momenteel gelijktijdig in het onderliggende proces wordt uitgevoerd. Normaal gesproken moet dit aantal “1” zijn.

Gegeven	Beschrijving
Piektaken	Het maximumaantal gelijktijdige taken dat tegelijkertijd is uitgevoerd in het onderliggende proces.
Toegestaan maximumaantal taken	Het aantal gelijktijdige taken dat het onderliggende proces toestaat.
Comm.fouten	Het aantal communicatiefouten met de Adaptive Job Server dat is opgetreden. Als dit aantal groot is, wordt het onderliggende proces opnieuw gestart.
Bezig met initialiseren	*TRUE* als het onderliggende proces bezig is met initialiseren. Als dit niet het geval is, *FALSE*.
Bezig met afsluiten	*TRUE* als het onderliggende proces bezig is met afsluiten. Als dit niet het geval is, *FALSE*.

36.1.9 Crystal Reports Server-gegevens

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor Crystal Reports- en Crystal Reports 2020-verwerkingsservers.

Gegevens van Crystal Reports-verwerkingsserver

Gegeven	Beschrijving
Openstaande taken	Een tabel met taken die momenteel worden uitgevoerd op de server. De tabel omvat de id en naam van het document, de naam van de gebruikers die de taak uitvoeren, de datum waarop het document voor het laatst geopend is, en hoe lang de taak is uitgevoerd.
Aantal afgehandelde aanvragen	Het totaalaantal aanvragen dat de server heeft afgehandeld sinds de server is gestart.
Aantal open taken	Het aantal huidige taken dat de server en de bijbehorende onderliggende processen momenteel verwerken.
Objecttype	Het type InfoObject waar de server doorgaans mee te maken heeft. De waarde voor dit gegeven blijft ongewijzigd.
Gemiddelde verwerkingstijd (ms)	De gemiddelde tijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen die de server heeft ontvangen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Maximale verwerkingstijd (ms)	De maximumtijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Minimale verwerkingstijd (ms)	De minimumtijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Aantal aanvragen in wachtrij	Het aantal aanvragen dat wacht op verwerking of dat wordt verwerkt. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Dll-naam van object	De naam van de invoegtoepassing voor verwerking voor de server. De waarde van dit gegeven blijft ongewijzigd.

Gegeven	Beschrijving
Aantal open verbindingen	Het aantal verbindingen tussen de server en clients, die momenteel open-staan.
Percentage mislukte aanvragen	Het aantal aanvragen dat de server niet heeft kunnen verwerken als een percentage van de laatste 500 aanvragen die de server heeft ontvangen.
Gegevens overgebracht (KB)	Het totale aantal gegevens, in kilobytes, die zijn overgebracht naar clients sinds de server gestart is.
Aantal mislukte aanvragen	Het aantal aanvragen die de server niet heeft kunnen voltooien sinds de server gestart is.
Maximumaantal onderliggende processen	Het maximumaantal gelijktijdige onderliggende processen dat op de server wordt ondersteund.

In de volgende tabel worden de servergegevens beschreven, die worden weergegeven in het venster *Gegevens* voor Crystal Reports-cacheservers.

Gegevens van Crystal Reports-cacheserver

Gegeven	Beschrijving
Aantal treffers in cache (%)	Het percentage aanvragen, over de laatste 500 aanvragen, die zijn verwerkt met cachegegevens.
Verbonden verwerkingsservers	Een tabel met de Crystal Reports-verwerkingsservers in uw implementatie. In de tabel staat de naam van de server en het aantal verbindingen dat momenteel open is op de server.
Aantal afgehandelde aanvragen	Het totaalaantal aanvragen dat de server heeft afgehandeld sinds de server is gestart.
Objecttype	Het type InfoObject waar de server doorgaans mee te maken heeft. De waarde voor dit gegeven blijft ongewijzigd.
Gemiddelde verwerkingstijd (msec)	De gemiddelde tijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen die de server heeft ontvangen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Maximale verwerkingstijd (msec)	De maximumtijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Minimale verwerkingstijd (msec)	De minimumtijd, in milliseconden, die de server heeft besteed aan het verwerken van de laatste 500 aanvragen. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Aantal aanvragen in wachtrij	Het aantal aanvragen dat wacht op verwerking of dat wordt verwerkt. Als dit aantal consequent hoog is en groter wordt, kunt u overwegen extra servers op andere computers te maken.
Dll-naam van object	De naam van de invoegtoepassing voor verwerking voor de server. De waarde van dit gegeven blijft ongewijzigd.
Cachegrootte	De hoeveelheid gegevens, in kilobytes, die momenteel in cache zijn opgeslagen op de schijf.
Aantal open verbindingen	Het aantal verbindingen tussen de server en clients, die momenteel open-staan.

Gegeven	Beschrijving
Gegevens overgebracht (KB)	Het totale aantal gegevens, in kilobytes, die zijn overgebracht naar clients sinds de server gestart is.

In de volgende tabel worden de servergegevens beschreven die worden weergegeven in het venster *Gegevens* voor Crystal Reports 2020 Report Application Servers.

Gegevens van Crystal Reports 2020 Report Application Server

Gegeven	Beschrijving
metric_currentdoccount **Opmerking** Dit gegeven wordt weergegeven als "document_s_" op de toezichtpagina in de CMC.	Het aantal documenten dat momenteel wordt vewerkt door de server.
metric_totaldoccount **Opmerking** Dit gegeven wordt weergegeven als "document_s_" op de toezichtpagina in de CMC.	Het aantal documenten dat verwerkt is sinds de server gestart is.
metric_currentagentthreadcount **Opmerking** Dit gegeven wordt weergegeven als "agent thread_s_" op de toezichtpagina in de CMC.	Het aantal threads dat momenteel wordt verwerkt door de server.
metric_totalagentthreadcount **Opmerking** Dit gegeven wordt weergegeven als "agent thread_s_" op de toezichtpagina in de CMC.	Het aantal threads dat verwerkt is sinds de server gestart is.

36.1.10 Gegevens van Web Intelligence Server

Gegevens van Web Intelligence-vewerkingsservice

Gegeven	Beschrijving
Cachegrootte (KB)	Het huidige aantal gegevens, in kilobytes, dat is opgeslagen in de cache.
Aantal verouderde documenten in cache	Het aantal documenten dat, sinds de server gestart is, uit de cache verwijderd is omdat ze te oud waren.

Gegeven	Beschrijving
Aantal hoge cachemarkeringen	De keren dat de cache de toegestane maximumgrootte op de server heeft bereikt, sinds deze gestart is.
CPU-gebruik (%)	Het percentage van het totale CPU-gebruik dat de server verbruikt heeft sinds de server gestart is.
Totale CPU-tijd (seconden)	De totale CPU-tijd, in seconden, die door de server besteed is sinds deze gestart is.
Hoge drempelwaarde geheugen	De keren dat de hoge drempelwaarde van het geheugen bereikt is op de server, nadat deze gestart is.
Maximale drempelwaarde geheugen	De keren dat de maximale drempelwaarde van het geheugen bereikt is op de server, nadat deze gestart is.
Virtuele geheugengrootte (MB)	Het totale geheugen, in megabytes, dat aan de server is toegekend.
Huidig aantal clientaanroepen	Het huidige aantal CORBA-aanroepen dat door de server wordt verwerkt.
Aantal mislukte externe extensies	Het aantal keren dat het niet gelukt is vanuit de server verbinding te maken met een service voor externe extensies die wordt gehost door een Adaptive Processing Server.
Huidig aantal taken	Het huidige aantal taken dat door de server wordt uitgevoerd.
Totaalaantal clientaanroepen	Het totaalaantal CORBA-aanroepen dat de server heeft ontvangen, nadat deze gestart is.
Totaalaantal taken	Het totaalaantal taken dat op de server is uitgevoerd, nadat deze gestart is.
Duur van inactiviteit (seconden)	Het aantal seconden dat verstreken is nadat de server de laatste aanvraag van de client heeft ontvangen.
Huidig aantal actieve sessies	Het huidige aantal sessies dat aanvragen van clients kan accepteren.
Aantal documenten geopend vanuit de cache	Het aantal documenten waarvoor de laatste aanvraag rechtstreeks uit de cache is uitgelezen.
Aantal documenten	Het aantal documenten dat momenteel op de server geopend is.
Huidig aantal sessies	Het aantal sessies dat op de server gemaakt is.
Aantal documentwissels	Het aantal documenten waarvoor een opschoningsthread wisselaanvragen heeft gepland.
Aantal gewisselde documenten	Het aantal documenten dat gewisseld is door wisselaanvragen.
Aantal time-outs van sessie	Het aantal sessies waarvoor een time-out is opgetreden sinds de server is gestart.
Totaalaantal sessies	Het aantal sessies dat op de server gemaakt is sinds de server is gestart.
Aantal gebruikers	Het totaalaantal gebruikers dat met de server verbonden is.
Aantal actieve threads	Het aantal threads dat aanvragen verwerkt die zijn ontvangen door de server (asynchrone threadpool).
Totaalaantal threads	Het totaalaantal threads die zijn gemaakt nadat de server is gestart (asynchrone threadpool).

37 Appendix met tijdelijke aanduidingen voor servers en knooppunten

37.1 Tijdelijke plaatsaanduidingen voor server en knooppunt

Met uitzondering van *%SERVER_FRIENDLY_NAME%* en *%SERVER_NAME%* zijn deze tijdelijke aanduidingen van toepassing op alle servers op hetzelfde knooppunt.

> **Opmerking**
>
> De volgende tijdelijke plaatsaanduidingen kunnen worden bewerkt op knooppuntniveau. Beschrijvingen en standaardwaarden bevinden zich in de bovenstaande tabel. Tijdelijke plaatsaanduidingen die niet in de lijst staan, zijn alleen-lezen.
>
> - *%DefaultAuditingDir%*
> - *%DefaultDataDir%*
> - *%DefaultLoggingDir%*
> - *%IntroscopeAgentEnableInstrumentation%*
> - *%IntroscopeAgentEnterpriseManagerHost%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **Let op**
>
> Tijdelijke aanduidingen die niet voor bewerking zijn bedoeld, mogen op geen enkele manier worden gewijzigd. De systeembeheerder moet ervoor zorgen dat alleen de juiste persoon uit de beheerdersgroep (die bedoeld zijn voor het knooppuntbeheer) over de bewerkingsrechten voor het knooppunt beschikt. Alle andere gebruikers, inclusief andere leden van de beheerdersgroep, moeten worden beperkt tot het weergeven/beheren van de knooppuntobjecten door de juiste beveiligingsrechten toe te passen. Als een van de tijdelijke aanduidingen per ongeluk is beschadigd en CMS niet wordt weergegeven, raadpleegt u deze SAP Note: 3269127.

> **Opmerking**
>
> Zie SAP Knowledge Base Article 3278916 voor informatie over hoe het wijzigen van plaatsaanduidingen kan worden voorkomen om verstoring van het BI-landschap door kwaadwillenden te voorkomen.

Tijdelijke plaatsaanduiding

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%AuditingDatabaseConnection%	De controledatabaseverbinding die gebruikt wordt door de CMS.	Deze waarde wordt opgegeven tijdens de installatie.
%AuditingDatabaseDriver%	Het type databasestuurprogramma dat gebruikt wordt om verbinding te maken met de controledatabase.	De standaardwaarde in Windows is: sqlserverauditdbss.
%BINDIR%	De map waarin de 64-bits binaire bestanden van SAP BusinessObjects Business Intelligence-platform staan.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/`
%BINDIR32%	De map waarin de 32-bits binaire bestanden van SAP BusinessObjects Business Intelligence-platform staan.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/`
%CACHESERVER_EXE%	De naam van het uitvoerbare bestand voor de Crystal Reports-cacheserver.	Onder Windows: `crcache.exe`. Onder UNIX: `boe_crcached.bin`.
%CMS_EXE%	De naam van het uitvoerbare bestand voor de Central Management Server.	Onder Windows: `cms.exe`. Onder UNIX: `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	De naam van het uitvoerbare bestand voor de 32-bits verbindingsserver.	Op Windows: `ConnectionServer32.exe`. Op UNIX: `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	De hoofdmap van de verbindingsserver.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer`
%CONNECTIONSERVER_EXE%	De naam van het uitvoerbare bestand voor de 64-bits verbindingsserver.	Onder Windows: `ConnectionServer.exe`. Onder UNIX: `ConnectionServer`.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%CRCPP_BINDIR%	De map waarin de binaire bestanden van de Crystal Reports C++-server zich bevinden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Onder UNIX lijkt de map op het volgende pad: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRCPP_DefaultWorkingDir%	De standaardwerkmap voor Crystal Reports C++-servers.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Onder UNIX lijkt de map op het volgende pad: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`.
%CRYSTALRAS_EXE%	De naam van het uitvoerbare bestand voor de Report Application Server.	Onder Windows: `crystalras.exe`. Onder UNIX: `boe_crystalrasd`.
%CR_ODBCINI%	Het pad naar de map met het bestand `.odbc.ini`.	Onde UNIX, `<INSTALLDIR>/bobje/odbc.ini`. Onder Windows is deze tekenreeks leeg.
%CommonJavaBundlesDir%	De map met gedeelde OSGI-bundels.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bundles`.
%CommonJavaLibDir%	De map met algemene Java-bibliotheken.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib`.
%DLLEXT%	De standaardextensie van een `DLL`- of `SO`-bestand.	Onder Windows: `.dll`. Onder UNIX: `.so`.
%DLLPATH%	De naam van de omgevingsvariable die aangeeft in welke mappen wordt gezocht naar uitvoerbare bestanden op de computer waarop SAP BusinessObjects Business Intelligence-platform is geïnstalleerd.	Onder Windows: “Path”. Onder UNIX: “LD_LIBRARY_PATH”.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%DLLPATH32%	Op 32-bits Solaris-systemen: de naam van de omgevingsvariable die aangeeft in welke mappen wordt gezocht naar uitvoerbare bestanden op de computer waarop SAP BusinessObjects Business Intelligence-platform is geïnstalleerd.	Op Solaris-computers: "LD_LIBRARY_PATH_32". Deze tijdelijke plaatsaanduiding is een lege tekenreeks op andere besturingssystemen.
%DLLPATH64%	Op 64-bits Solaris-systemen: de naam van de omgevingsvariable die aangeeft in welke mappen wordt gezocht naar uitvoerbare bestanden op de computer waarop SAP BusinessObjects Business Intelligence-platform is geïnstalleerd.	Op Solaris-computers: "LD_LIBRARY_PATH_64". Deze tijdelijke plaatsaanduiding is een lege tekenreeks op andere besturingssystemen.
%DLLPREFIX%	Het standaardvoorvoegsel van een `DLL`- of een `SO`-bestand.	Onder UNIX, "lib". Deze tijdelijke plaatsaanduiding is een lege tekenreeks op Windows-systemen.
%DLLPRELOAD%	De naam van de omgevingsvariabele LD_PRELOAD voor het platform.	Onder UNIX: *LD_PRELOAD*. Deze tijdelijke plaatsaanduiding is een lege tekenreeks op Windows-systemen.
%DLLPRELOAD32%	De naam van de omgevingsvariabele LD_PRELOAD op 32-bits AIX-systemen.	Onder AIX: *LDR_PRELOAD*. Deze tijdelijke plaatsaanduiding is een lege tekenreeks op andere computers.
%DLLPRELOAD64%	De naam van de omgevingsvariabele LD_PRELOAD op 64-bits AIX-systemen.	Onder AIX: *LDR_PRELOAD64*. Deze tijdelijke plaatsaanduiding is een lege tekenreeks op andere computers.
%DP%	Het scheidingsteken voor het pad.	Onder Windows: ";". Onder UNIX: ":".
%DefaultAuditingDir%	De map waarnaar tijdelijke controlebestanden worden geschreven. Voor optimale prestaties moet deze locatie zich op de lokale schijf van de server bevinden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Auditing`. Onder UNIX, `<INSTALLDIR>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	De tijdelijke map die wordt gebruikt door de Job Server.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data`. Onder UNIX, `<INSTALLDIR>/sap_bobj/data/`.
%DefaultInputFRSDir%	De hoofdmap van de Input File Repository Server.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. Onder UNIX, `<INSTALLDIR>/sap_bobj/data/frsinput`.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%DefaultLoggingDir%	De opslaglocatie van de logboekbestanden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. Onder UNIX, `<INSTALLDIR>/sap_bobj/logging`.
%DefaultOutputFRSDir%	De hoofdmap van de Output File Repository Server.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. Onder UNIX, `<INSTALLDIR>/sap_bobj/data/frsoutput`.
%DefaultWorkingDir%	De werkmap voor 64-bits servers	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`.
%DefaultWorkingDir32%	De werkmap voor 32-bits servers	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`.
%EPM_LD_PRELOAD_ONCE%	De naam van de omgevingsvariabele LD_PRELOAD_ONCE voor het platform.	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	De naam van het uitvoerbare bestand voor de Event Server.	Onder Windows: `EventServer.exe`. Onder UNIX: `boe_eventsd`.
%EXEEXT%	De standaardextensie van uitvoerbare bestanden.	Onder Windows: `.exe`. Deze tijdelijke plaatsaanduiding is niet beschikbaar op UNIX.
%EXEPATH%	De naam van de omgevingsvariable die aangeeft in welke mappen wordt gezocht naar uitvoerbare bestanden op de computer waarop SAP BusinessObjects Business Intelligence-platform is geïnstalleerd.	Onder Windows: “Path”. Onder UNIX: “PATH”.
%EnterpriseDir%	De locatie waar de 64-bits versie van SAP BusinessObjects Business Intelligence-platform geïnstalleerd is.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%EnterpriseDir32%	De locatie waar de 32-bits versie van SAP BusinessObjects Business Intelligence platform is geïnstalleerd.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`.
%ExternalJavaLibDir%	De map met externe Java-bibliotheken van derden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/external`.
%FILESERVER_EXE%	De naam van het uitvoerbare bestand voor de bestandsserver.	Onder Windows: `fileserver.exe`. Onder UNIX: `boe_filesd`.
%HOARD_PATH%	De locatie van het geheugenbeheer.	Deze is standaard leeg.
%HOARD_PRELOAD%	Hiermee wordt aangegeven of het geheugenbeheer van tevoren moet worden geladen.	Deze is standaard leeg.
%INSTALLROOTDIR%	De map waarin de 64-bits versie van SAP BusinessObjects Business Intelligence-platform geïnstalleerd is.	Deze waarde wordt opgegeven tijdens de installatie.
%INSTALLROOTDIR32%	De map waar de 32-bits versie van SAP BusinessObjects Business Intelligence platform is geïnstalleerd.	Deze waarde wordt opgegeven tijdens de installatie.
%IntroscopeAgentEnableInstrumentation%	Hier wordt aangegeven of instrumentatie voor Java-servers met Introscope Agent Enterprise Manager actief is.	Mogelijke waarden zijn WAAR of ONWAAR, afhankelijk van of de Introscope Agent Enterprise Manager was ingeschakeld tijdens de installatie van SAP BusinessObjects Business Intelligence-platform.
%IntroscopeAgentEnterpriseManagerHost%	De Introscope Agent Enterprise Manager-hostnaam waarnaar instrumentatiegegevens worden verzonden.	Deze waarde wordt opgegeven tijdens de installatie.
%IntroscopeAgentEnterpriseManagerPort%	De Introscope Agent Enterprise Manager-poort waarnaar instrumentatiegegevens worden verzonden.	Deze waarde wordt opgegeven tijdens de installatie.
%IntroscopeAgentEnterpriseManagerTransport%	Het transport dat wordt gebruikt voor verzending van instrumentatiegegevens naar de Introscope Agent Enterprise Manager. De volgende waarden zijn toegestaan: • TCP • HTTP • HTTPS • SSL	TCP

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%IntroscopeAgentEnterpriseManagerTransportHTTP%	De klasse die wordt gebruikt voor verzending van instrumentatiegegevens naar de Introscope Agent Enterprise Manager via HTTP.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	De klasse die wordt gebruikt voor verzending van instrumentatiegegevens naar de Introscope Agent Enterprise Manager via HTTPS.	com.wily.isengard.postoffice-hub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	De klasse die wordt gebruikt voor verzending van instrumentatiegegevens naar de Introscope Agent Enterprise Manager via SSL.	com.wily.isengard.postoffice-hub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	De klasse die wordt gebruikt voor verzending van instrumentatiegegevens naar de Introscope Agent Enterprise Manager via TCP.	com.wily.isengard.postoffice-hub.link.net.DefaultSocketFactory
%IntroscopeDir%	De map waar Introscope Agent Enterprise Manager is geïnstalleerd.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily`.
%JAVAW_EXE%	De naam van het uitvoerbare bestand voor Java Virtual Machine zonder consolevenster.	Onder Windows: `javaw.exe`. Onder UNIX: `java`.
%JAVA_EXE%	De naam van het uitvoerbare bestand voor Java Virtual Machine.	Onder Windows: `java.exe`. Onder UNIX: `java`.
%JOBSERVERCHILD_EXE%	De naam van het uitvoerbare bestand voor de onderliggende Adaptive Job Server.	Onder Windows: `JobServerChild.exe`. Onder UNIX: `boe_jobcd`.
%JOBSERVER_EXE%	De naam van het uitvoerbare bestand voor de Adaptive Job Server.	Onder Windows: `JobServer.exe`. Onder UNIX: `boe_jobsd`.
%JdkBinDir%	De map met de binaire JDK-bestanden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. Onder UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin`.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%JreBinDir%	De map met de binaire JRE-bestanden.	Ondere Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. Onder UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/jre/bin`.
%JVM_ARCH_ENVIRONMENT%	Hiermee wordt aangegeven of de computer wordt uitgevoerd op een 32-bits of 64-bits versie van JVM.	Voor computers met een 32-bits versie van UNIX is de standaardwaarde "-d32". Voor computers met een 64-bits versie van UNIX is de standaardwaarde "-d64". Op Windows-systemen is deze tekenreeks leeg.
%JVM_HEADLESS_MODE%	Het opdrachtregelargument waarmee wordt aangegeven of de JVM wordt uitgevoerd in de headless-modus.	Onder Windows: -Djava.awt.headless=false. Onder UNIX: -Djava.awt.headless=true
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	De opdrachtregelparameters waarmee wordt opgegeven wat de JVM doet wanneer er fouten opgetreden vanwege onvoldoende geheugen.	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	De opdrachtregelparameters waarmee JVM-extensies worden ingeschakeld en het exemplaarnummer van de JVM wordt ingesteld.	Standaard is deze tijdelijke aanduiding leeg.
%LANGUAGEPACKSDIR%	De map waarin de taalpakketten van de implementatie zijn geïnstalleerd.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.
%LANGUAGEPACKSDIR32%	De map waar de taalpakketten van de implementatie worden geïnstalleerd op 32-bits systemen.	. Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`.
%LSTDir%	De map waar LST-configuratiebestanden worden opgeslagen.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst`.
%MDAS_JVM_OS_STACK_SIZE%	Hiermee wordt de JVM-stackgrootte voor de Multidimensional Analysis-service opgegeven.	Standaard is deze tijdelijke aanduiding leeg.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%NCSInstrumentLevelThreshold%	Het drempelniveau voor het traceringslogboek van de NCS-bibliotheek.	Standaard is deze waarde ingesteld op 0.
%PAGESERVER_EXE%	De naam van het uitvoerbare bestand voor de Crystal Reports 2020-verwerkingsserver.	Onder Windows: `crproc.exe`. Onder UNIX: `boe_crprocd.bin`.
%PJSContainerDir%	De map waarin de JARS van de APS-container zich bevinden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container`.
%PJSServicesDir%	De map waarin de JARS van de APS-service zich bevinden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services`.
%Platform%	Het besturingssysteem van de computer waarop SAP BI platform wordt uitgevoerd.	Het besturingssysteem van de computer waarop SAP BI platform wordt uitgevoerd.
%Platform32%	Het besturingssysteem van de computer waarop de 32-bitsversie van SAP BI platform wordt uitgevoerd.	Het besturingssysteem van de computer waarop SAP BI platform wordt uitgevoerd.
%RasBinDir%	De hoofdmap van de Report Application Server.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras`.
%SERVER_FRIENDLY_NAME%	De volledige naam van de server.	De volledige naam van de server.
%SERVER_NAME%	De volledige naam van de server.	De volledige naam van de server.
%SMDAgentHost%	De SMD Agent -hostnaam waarnaar instrumentatiegegevens worden verzonden.	Deze waarde wordt opgegeven tijdens de installatie.
%SMDAgentPort%	De SMD Agent-poort waarnaar instrumentatiegegevens worden verzonden.	Deze waarde wordt opgegeven tijdens de installatie.
%TRACE_CONFIGFILE_INI%	Het pad naar de map met het bestand `BO_Trace.ini`.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/BO-trace.ini`.

Tijdelijke aanduiding	Beschrijving	Standaardwaarden
%WarFilesDir%	De locatie van de webtoepassingsbestanden.	Onder Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`. Onder UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/warfiles/webapps`.
%WEBI_LD_PRELOAD%	De naam van de omgevingsvariabele LD_PRELOAD voor het platform.	$LD_PRELOAD$
%WEBISERVER_EXE%	De naam van het uitvoerbare bestand voor de Web Intelligence-verwerkingsserver.	Onder Windows: `wireportserver.exe`. Onder UNIX: `WIReportServer`.
%WEBI_LD_PRELOAD_ONCE%	De naam van de omgevingsvariabele LD_PRELOAD_ONCE voor het platform.	$LD_PRELOAD_ONCE$

Verwante informatie

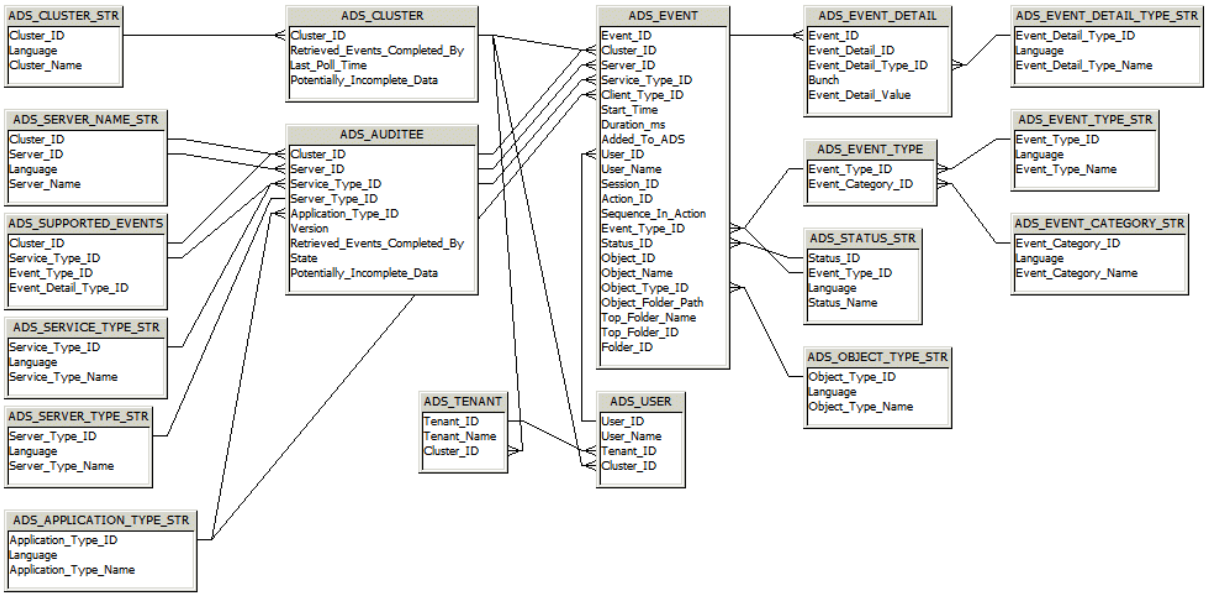
De tijdelijke plaatsaanduidingen voor een knooppunt bekijken en bewerken [pagina 498]

38 Appendix met schema voor controle van gegevensopslag

38.1 Overzicht

Deze appendix dient als referentie voor rapportontwerpers die de tabellen Gegevensopslag controleren zullen openen en voor rapportage zullen gebruiken. De volgende diagram- en tabelbeschrijving toont de tabellen waarin de controlegegevens worden vastgelegd en hoe deze tabellen zich tot elkaar verhouden.

38.2 Schemadiagram



38.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example `<EN>`, or `<DE>`.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (long-text)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example `<EN>`, or `<DE>`.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example `<EN>`, or `<DE>`.
Object_Type_Name	Character (255)	Name of the object type.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example `<EN>`, or `<DE>`.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example `<EN>`, or `<DE>`.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example `<EN>`, or `<DE>`.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

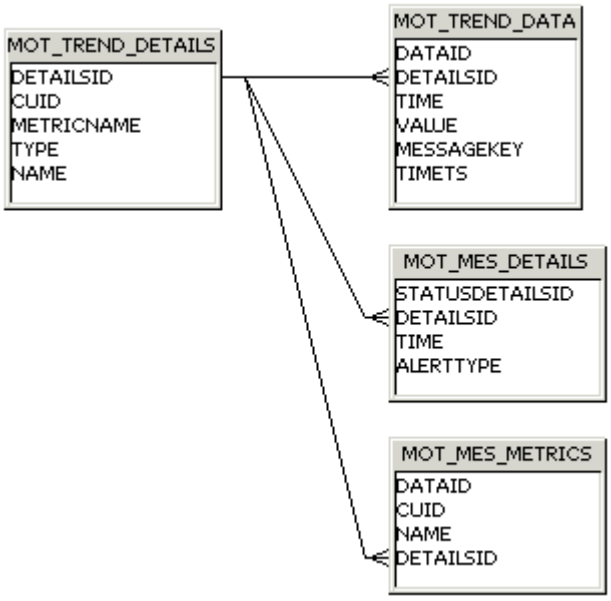
This table records the relationship between users and tenants.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

39 Appendix met schema voor controle van database

39.1 Schema van trending-database

De volgende beschrijving van het diagram en de tabel van de Trending-database geeft de tabellen weer waarin de waarde-, test- en controlegegevens worden vastgelegd en hoe deze tabellen zich tot elkaar verhouden.



MOT_TREND_DETAILS

In deze tabel wordt informatie over beheerde entiteiten, tests en controles vastgelegd. Bijvoorbeeld namen van CUID's en gegevens.

Kolomnaam	Type	Toets	Beschrijving
DetailsId	INTEGER	Primaire sleutel Automatisch gegenereerd	
CUID	VARCHAR(64)	N.v.t.	CUID van het InfoObject dat het gegeven weergeeft of is gerelateerd aan het gegeven
MetricName	VARCHAR(255)	N.v.t.	Naam van het gegeven

Kolomnaam	Type	Toets	Beschrijving
Type	VARCHAR(32)	N.v.t.	Een van "Subscription", "ManagedEntityStatus" of "Probe"
Naam	VARCHAR(255)	N.v.t.	Naam van de controle wanneer het type "ManagedEntity-Status" is. Wordt anders standaard ingesteld op dezelfde tekenreeks als in Type, alleen volledig in hoofdletters, bij-voorbeeld "PROBE" of "SUBSCRIPTION".

MOT_TREND_DATA

In deze tabel worden de trending-gegevens van gegevens, controles en tests vastgelegd. Gegevens en tijd, bijvoorbeeld.

Kolomnaam	Type	Toets	Beschrijving
DataId	INTEGER	Primaire sleutel Automatisch gegene-reerd	
DetailsId	INTEGER	Externe sleutel (van MOT_TREND_DE-TAILS)	
Time of TimeT	BIGINT of NUMBER of FIXED Unix Epoch-datum	N.v.t.	Tijd waarop gegevens zijn verzameld
Waarde	FLOAT of DOUBLE of NUMBER	N.v.t.	Waarde van het gegeven/abonnement
MessageKey	VARCHAR(32)	N.v.t.	Foutberichtsleutel of null indien geslaagd. Voor Controle kan dit ook "watchEnabled" of "watchDisabled" zijn. Het is een "key" omdat het uiteindelijk wordt gebruikt om ge-lokaliseerde berichten op te halen voordat de gebruikers-interface wordt opgehaald.
Ts	DATETIME of TI-MESTAMP	N.v.t.	Tijd waarop gegevens naar de database worden geschre-ven.

MOT_MES_DETAILS

In deze tabel wordt informatie over abonnemtsoverschrijding en de levering van meldingen vastgelegd. Bijvoorbeeld de overschrijdingstijd en de tijd waarop melding is geleverd.

Kolomnaam	Type	Toets	Beschrijving
StatusDetailsId	INTEGER	Primaire sleutel Automatisch gegenereerd	
DetailsId	INTEGER	Externe sleutel (van MOT_TREND_DETAILS)	
Tijd	BIGINT of NUMBER Unix Epoch-datum	N.v.t.	Tijd waarop gegevens zijn verzameld
AlertType	SMALLINT of NUMBER	N.v.t.	Verzendingstype van abonnementsbericht (bijvoorbeeld per e-mail)

MOT_MES_METRICS

In deze tabel wordt informatie vastgelegd over controles en over de gegevens die bij de controlevergelijkingen horen. Voor elk gegeven van de controle is één vermelding in deze tabel aanwezig.

Kolomnaam	Type	Toets	Beschrijving
DataId	INTEGER	Primaire sleutel Automatisch gegenereerd	
DetailsId	INTEGER	Externe sleutel (van MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	N.v.t.	CUID van de controle
Naam	VARCHAR(255)	N.v.t.	Naam van de controle

40 Bijlage met werkblad Systeemkopie

40.1 Werkblad Systeemkopie

Eigenschap	Waarde
Clustersleutel.	
Namen van de knooppunten.	
De computernaam en installatiemap van het BI-platform voor elke computer in de implementatie.	
Het beheerderswachtwoord voor het BI-platform.	
CMS-databaseverbindingen en de gebruikersnamen en wachtwoorden voor deze verbindingen op elke computer in de implementatie.	
Controledatabaseverbindingen en de gebruikersnamen en wachtwoorden voor deze verbindingen op elke computer in de implementatie.	
Voor elke computer in de implementatie: details van eventuele andere databaseclientverbindingen voor elke computer in het bronsysteem die door universes en rapporten worden gebruikt.	
Voor elke computer in de implementatie: databaseclienttypen en -versies.	
De versie, het ondersteuningspakket en het patchniveau.	
De locatie van de bestandsopslag voor elke invoer-FRS en uitvoer-FRS in de implementatie.	
Als u van plan bent Promotiebeheer, de locatie van de Promotiebeheer-databasemap en Subversion-mappen te kopieren.	
Als u van plan bent de controledatabase te kopiëren: de controledatabasemap.	
Het pad naar de map van de semantische laag.	

Belangrijke disclaimers en juridische informatie

Hyperlinks

Sommige links zijn voorzien van een pictogram en/of een muistekst. Deze links bieden aanvullende informatie.
Informatie over de pictogrammen:

- Links met het pictogram : u gaat naar een website die niet wordt gehost door SAP. Door uw gebruik van dergelijke links stemt u (tenzij uitdrukkelijk anders vermeld in uw overeenkomsten met SAP) in met het volgende:
  - De gelinkte site bevat geen SAP-documentatie. U kunt op basis van deze informatie geen productclaims neerleggen bij SAP.
  - SAP kan de inhoud van de gelinkte site niet bevestigen of ontkennen, noch de beschikbaarheid en juistheid garanderen. SAP is niet aansprakelijk voor schade die wordt veroorzaakt door het gebruik van dergelijke inhoud, tenzij deze schade is ontstaan door bewuste roekeloosheid of opzet van SAP.
- Links met het pictogram : u verlaat de documentatie voor dat bepaalde SAP-product (of die SAP-service) en u gaat naar een website die door SAP wordt gehost. Door het gebruik van dergelijke links stemt u ermee in (tenzij uitdrukkelijk anders vermeld in uw overeenkomsten met SAP) dat u geen productclaims kunt neerleggen bij SAP op basis van deze informatie.

Video's die worden gehost op externe platforms

Sommige video's verwijzen mogelijk naar externe videohostingplatforms. SAP kan niet garanderen dat de video's die op deze platforms zijn opgeslagen, in de toekomst beschikbaar blijven. Verder vallen de advertenties en andere inhoud die op deze platforms worden gehost (bijvoorbeeld: voorgestelde video's of andere video's waarnaar wordt genavigeerd en die worden gehost op dezelfde site) niet onder het beheer of de verantwoordelijkheid van SAP.

Bèta en andere experimentele functies

Experimentele functies vormen geen onderdeel van de officiële leveringsscope die SAP garandeert voor toekomstige releases. Dit betekent dat experimentele functies op elk moment, op elke grond en zonder kennisgeving kunnen worden gewijzigd door SAP. Experimentele functies zijn niet bedoeld voor gebruik in de dagelijkse productie. U mag de experimentele functies niet demonstreren, testen, onderzoeken, evalueren of anderszins gebruiken in een live gebruiksomgeving of met gegevens waarvan u geen goede back-up hebt.
Het doel van experimentele functies is om vroegtijdig feedback te krijgen, zodat klanten en partners het toekomstige product zo nodig kunnen bijsturen. Door uw feedback te verstrekken (bijv. in de SAP Community), gaat u ermee akkoord dat de intellectuele eigendomsrechten van de bijdragen of daarvan afgeleide items het exclusieve eigendom van SAP blijven.

Voorbeeldcode

Alle softwarecode en/of codefragmenten zijn voorbeelden. Ze zijn niet bedoeld voor gebruik in de dagelijkse productie. De voorbeeldcode is alleen bedoeld om de syntaxis- en fraseringsregels uit te leggen en te visualiseren. SAP kan de juistheid en volledigheid van de voorbeeldcode niet garanderen. SAP is niet aansprakelijk voor fouten of schade als gevolg van het gebruik van voorbeeldcode, tenzij deze schade is ontstaan door bewuste roekeloosheid of opzet van SAP.

Inclusief taalgebruik

SAP omarmt een cultuur van diversiteit en inclusie. Waar mogelijk maken we gebruik van inclusief taalgebruik in onze documentatie om te verwijzen naar mensen. Hierbij wordt uitgegaan van de positieve kwaliteiten van iedereen, los van culturele of etnische achtergrond, geslacht of seksuele gerichtheid en een eventuele handicap of beperking.

www.sap.com/contactsap

© 2024 SAP SE of een aan SAP gelieerde onderneming. Alle rechten voorbehouden.

Niets uit deze publicatie mag in welke vorm of voor welk doel dan ook worden vermenigvuldigd of overgedragen zonder de uitdrukkelijke toestemming van SAP SE of een aan SAP gelieerde onderneming. De informatie in deze publicatie kan zonder voorafgaande kennisgeving worden gewijzigd.

Sommige softwareproducten die door SAP SE en haar distributeurs op de markt worden gebracht, bevatten merkspecifieke softwareonderdelen van andere softwareleveranciers. Productspecificaties kunnen per land verschillen.

Deze materialen worden uitsluitend ter informatie geleverd door SAP SE of een aan SAP gelieerde onderneming, zonder dat hier enige rechten aan kunnen worden ontleend en zonder garantie van enige aard, en SAP en de aan haar gelieerde ondernemingen zijn niet aansprakelijk voor fouten of omissies met betrekking tot de materialen. De enige garanties voor producten en diensten van SAP of een aan SAP gelieerde onderneming zijn de garanties in de uitdrukkelijke garantieverklaringen die bij dergelijke producten en diensten worden geleverd, indien van toepassing. Niets hierin mag worden opgevat als een aanvullende garantie.

SAP en andere SAP-producten en -diensten die hierin worden genoemd, evenals de respectieve logo's, zijn handelsmerken of gedeponeerde handelsmerken van SAP SE (of een aan SAP gelieerde onderneming) in Duitsland en andere landen. Alle andere genoemde namen van producten en diensten zijn handelsmerken van de desbetreffende ondernemingen.

Zie https://www.sap.com/netherlands/about/legal/trademark.html voor aanvullende informatie en kennisgevingen over handelsmerken.

THE BEST RUN SAP