HP Universal CMDB 9.10 Configuration Manager

voor het Windows-besturingssysteem

Implementatiegids

Publicatiedatum document: november 2010
Uitgavedatum software: november 2010

Juridische kennisgevingen

Garantie

De enige garanties voor producten en services van HP worden uiteengezet in de expliciete garantieverklaringen die bij die producten en services worden geleverd. Niets hierin mag worden opgevat als zijnde een extra garantie. HP is niet verantwoordelijk voor technische of redactionele fouten of vergetelheden in dit document.

De informatie die dit document omvat, kan worden gewijzigd zonder kennisgeving.

Legende van beperkte rechten

Vertrouwelijke computersoftware. Geldige licentie van HP vereist voor bezit, gebruik of kopiëren. Consistent met FAR 12.211 en 12.212 worden commerciële computersoftware, computersoftwaredocumentatie en technische gegevens voor commerciële items aan de overheid van de Verenigde Staten onder licentie gegeven volgens de commerciële standaardlicentie van de leverancier.

Copyrightvermeldingen

Bijgewerkte documentatie

De titelpagina van dit document bevat de volgende identificerende informatie:

- De publicatiedatum van het document, die wijzigt elke keer als het document wordt bijgewerkt.
- De uitgavedatum van de software, waarmee de uitgavedatum van deze versie van de software wordt aangeduid.

Om te controleren of er recente updates zijn of om te controleren of u de recentste versie van een document gebruikt, gaat u naar:

http://h20230.www2.hp.com/selfsolve/manuals

Op deze website moet u zich registreren voor een HP Passport en aanmeldingsgegevens. Om u te registreren voor een HP Passport ID gaat u naar:

http://h20229.www2.hp.com/passport-registration.html

Of klik op de koppeling **New users - please register** op de aanmeldingspagina van HP Passport.

U ontvangt ook bijgewerkte of nieuwe versies als u zich inschrijft op de relevantie productondersteuningsservice. Neem contact op met uw HP-vertegenwoordiger voor meer informatie.

Ondersteuning

Bezoek de website van HP Software Support op:

http://www.hp.com/go/hpsoftwaresupport

Op deze website vindt u contactgegevens en details over de producten, services en ondersteuning die HP Software aanbiedt.

De online-ondersteuning van HP Software helpt de klant om problemen zelf op te lossen. Het is een snelle en efficiënte manier om interactieve hulpprogramma's voor technische ondersteuning te gebruiken die u nodig hebt voor uw zakelijke activiteiten. Als gewaardeerde ondersteuningsklant haalt u voordeel uit het gebruik van de ondersteuningswebsite om:

- interessante kennisdocumenten te zoeken
- verzoeken tot ondersteuning en verzoeken tot verbetering/uitbreiding in te dienen en op te volgen
- softwarepatches te downloaden
- ondersteuningscontracten te beheren
- contactpersonen van HP voor ondersteuning op te zoeken
- informatie over beschikbare services te lezen
- zaken te bespreken met andere softwareklanten
- softwareopleidingen op te zoeken en u ervoor in te schrijven

Voor de meeste pagina's op deze website moet u zich registreren als HP Passport-gebruiker en u aanmelden. Ook is voor veel pagina's een supportcontract nodig. Om u te registreren voor een HP Passport-ID gaat u naar:

http://h20229.www2.hp.com/passport-registration.html

Ga voor meer informatie over toegangsniveau's naar

http://h20230.www2.hp.com/new_access_levels.jsp

Inhoudsopgave

1

Installatie en configuratie

In dit hoofdstuk vindt u:

Configuration Manager-overzicht

Met de HP Universal CMDB Configuration Manager (Configuration Manager) kunt u de gegevens in uw CMS analyseren en beheren. Hij vormt ook een omgeving om de CMS-infrastructuur te beheren, die veel verschillende gegevensbronnen omvat en die wordt gebruikt voor allerlei verschillende producten en toepassingen.

De implementatie van Configuration Manager in een bedrijfsnetwerkomgeving is een procedure waarvoor middelenplanning en systeemarchitectuurontwerp vereist is. Voordat u Configuration Manager installeert, moet u de informatie in dit gedeelte lezen, met inbegrip van de systeemvereisten.

Systeemvereisten Configuration Manager

Systeemvereisten server

In de volgende tabel worden de systeemvereisten voor de Configuration Manager-server beschreven:

CPU	Intel Pentium 4, Minimum 4 core
Geheugen (RAM)	Minimaal 4 GB
Platform	x64
Besturingssysteem	De volgende 64-bits-besturingssystemen van Windows worden ondersteund: ➤ Windows 2003 Enterprise SP2 en R2 SP2 ➤ Windows 2008 Enterprise SP2 en R2

Database	➤ Microsoft SQL Server 2005 SP2; 2005 Compatibility Mode 80; (telkens Enterprise Edition) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB versie 9.03 (typische CMDB-installatie) Raadpleeg de HP Universal CMDB-documentatie voor een volledige lijst van systeemvereisten voor deze versie.

Clientvereisten

In de volgende tabel worden de clientvereisten voor het bekijken van Configuration Manager beschreven:

Browser	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Invoegtoepassing Flash Player voor browser	Flash Player 9 of hoger
Schermresolutie	➤ Minimaal 1024 x 768 ➤ Aanbevolen 1280 x 1024
Kleurenkwaliteit	Minimaal 16 bits

Aanbevolen installatierichtlijnen

In de volgende tabel staan richtlijnen voor de installatieopties van Configuration Manager.

LDAP	De volgende LDAP-omgevingen worden ondersteund: ➤ Active Directory ➤ SunONE 6.x
Minimaal aanbevolen databaseschemagrootte	2 GB

Configuration Manager Capaciteitsbeperkingen

In de volgende tabel staan de capaciteitslimieten voor Configuration Manager opgesomd:

Aanbevolen maximumaantal weergaven	100
Aanbevolen maximumaantal beleidslijnen	300
Aanbevolen maximumaantal samengestelde CI's per weergave	5000
Aanbevolen maximumaantal gelijktijdige gebruikers	50

Het database- of gebruikersschema configureren

Om met Configuration Manager te werken, moet u een databaseschema opgeven. Configuration Manager ondersteunt Microsoft SQL Server en Oracle Database Server. In deze taak wordt beschreven hoe de verbindingseigenschappen voor de Configuration Manager-database of -gebruikersschema moeten worden geconfigureerd met de installatiewizard.

Let op: Raadpleeg "Systeemvereisten server" op pagina 8 voor vereisten voor Microsoft SQL Server en Oracle Server.

Om uw database te configureren:

1 Wijs een gebruikersschema van Microsoft SQL Server database of Oracle Server toe.

- Voor **Microsoft SQL Server 2005**: activeer de snapshotisolatie.

  Voer de volgende opdracht eenmaal uit na het creëren van de database:

  ```
  alter database <ccm_database_name> set read_committed_snapshot on
  ```

  Raadpleeg http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx voor meer informatie over de snapshotisolatiefunctie van SQL Server.

- Voor **Oracle**: geef de Oracle-gebruiker enkel de functies **Connect** en **Resource**.
  (Indien u hem de machtiging **Select any table** toewijst, zal de schemapopulatieprocedure mislukken.)

2 Controleer de volgende informatie, die u nodig hebt tijdens deze configuratieprocedure:

✔	**Vereiste informatie**
	DB-hostnaam en poort
	DB-gebruikersnaam en wachtwoord
	Voor MS SQL: databasenaam
	Voor Oracle: SID

3 Voer de installatiewizard van Configuration Manager uit. Raadpleeg "Installeren Configuration Manager" op pagina 12 voor meer informatie.

Installeren Configuration Manager

In deze taak wordt beschreven hoe u Configuration Manager op uw server installeert en hoe u de databaseverbinding en de UCMDB-configuratie configureert. U kunt op elke wizardpagina op **Help** klikken voor hulp met de installatie. Zie "Configuratiewizard voor voltooiing van de installatie van Configuration Manager" op pagina 23 voor gedetailleerde beschrijvingen van de wizardpagina's.

Om Configuration Manager te installeren:

1 In de hoofdmap van de Configuration Manager-DVD zoekt u het bestand **install.bat**.

2 Dubbelklik op het bestand om de installatiewizard van de Configuration Manager uit te voeren.

3 Klik op **Volgende** om de pagina van de licentieovereenkomst voor de eindgebruiker te openen.

4 Accepteer de voorwaarden van de licentie en klik op **Volgende** om de pagina voor de productinstallatie te openen.

5. Selecteer de te installeren producten (UCMDB en Configuration Manager) en geef de plaats van installatie op. Indien u een aangepaste UCMDB-licentie hebt, selecteert u het selectievakje. Klik op **Volgende** om met de installatie van UCMDB te starten. Voor meer informatie over de installatie van UCMDB raadpleegt u the *HP Universal CMDB Deployment Guide* PDF.
6. Wanneer de installatie en de voltooiing van de installatie van UCMDB voltooid zijn, start de configuratiewizard voor de voltooiing van de installatie van Configuration Manager automatisch.
7. Klik op **Volgende** op de Welkomstpagina om de configuratiepagina voor de databaseverbinding te openen.
8. Selecteer het databasetype (Oracle of Microsoft SQL Server) en voer de gebruikersnaam en het wachtwoord in. Het is aanbevolen om de verbinding te testen door op de knop **Testen** te klikken. Indien de test van de verbinding slaagt, klikt u op **Volgende** om de configuratiepagina van de toepassingsserver te openen.

Let op: U kunt meer geavanceerde databaseverbindingsopties configureren nadat de wizard gereed is. Raadpleeg "Geavanceerde opties voor databaseverbindingen configureren" op pagina 15 voor meer informatie.

---

9. Voer de hostnaam in en klik op **Volgende** om de configuratiepagina van de Windows-service te openen.
10. Indien u Configuration Manager als Windows-service wilt installeren, kruist u het selectievakje aan. Klik op **Volgende** om de pagina met de aanmeldingsgegevens van de gebruiker te openen.
11. Voer de gebruikersnaam en het wachtwoord in voor zowel de administratieve gebruiker als voor de integratiegebruiker. Klik op **Volgende** op de configuratiepagina voor de HP UCMDB-verbinding te openen.

12 Indien UCMDB al geïnstalleerd is op deze machine of op een andere machine, moet u ervoor zorgen dat de UCMDB-server actief is voor u doorgaat.

Indien u UCMDB op een andere machine installeert, zorgt u ervoor dat het selectievakje geïnstalleerd is en moet u de vereiste parameters invoeren. Er wordt aanbevolen om de verbinding te testen door op de knop **Testen** te klikken. Indien de verbindingstest slaagt, klikt u op **Volgende** om de overzichtspagina met acties voor de voltooiing van de installatie te openen.

13 Lees de informatie op de overzichtspagina met acties voor de voltooiing van de installatie. Als die juist is, klikt u op **Volgende** om door te gaan met de voltooiing van de installatie.

14 Klik op **Voltooien** op de Voltooiingspagina om de installatie te voltooien.

15 Als dit niet de eerste opstart van UCMDB is, moet u de kolomgrootte in UCMDB als volgt wijzigen:

a Ga naar **Beheer** > **Beheer infrastructuurinstellingen**. Zoek de instelling **Objectbeginpunt** en wijzig die in **data**. Meld u af uit UCMDB en meld u opnieuw aan. Pas dan zal de wijziging actief worden.

b Ga naar **Modellering** > **CI-typebeheer**. Selecteer het CI-type **gegevens** in de boomstructuur en selecteer het tabblad Attributen. Bewerk het attribuut **Gebruikerslabel** door de **waardegrootte** op 900 in te stellen.

c Ga terug naar de **Infrastructuurinstellingenbeheer** en wijzig de instelling **Objecthoofdmap** terug in zijn oorspronkelijke waarde. Meld u af en meld u opnieuw aan. Pas dan zal de wijziging actief worden.

16 Indien Gegevensstroombeheer al op UCMDB werd uitgevoerd, is het mogelijk dat de geschiedenisgegevens beschadigd zijn. Om dit probleem op te lossen, voert u de volgende procedure uit:

a Start een webbrowser en voer het volgende adres in: http://<UCMDB-serveradres>.<domeinnaam>:8080/jmx-console.

Voer de aanmeldingsgegevens voor de verificatie in de JMX-console in. De standaardaanmeldingsgegevens zijn:

- Aanmeldingsnaam = **sysadmin**
- Wachtwoord = **sysadmin**

b Onder **UCMDB** selecteert u **History DB Services**.

c Selecteer de methode **Fix902EndTimeRecords**.

d Voor de klant met werkelijke status voert u **1** in als klant-ID-waarde en klikt u op **Invoke**.

e Indien de bewerking geslaagd is, verschijnt het bericht "History DB is updated successfully".

f Voor de klant met geautoriseerde status voert u **100001** in als klant-ID-waarde en klikt u op **Invoke**.

g Indien de bewerking geslaagd is, verschijnt het bericht "History DB is updated successfully".

Geavanceerde opties voor databaseverbindingen configureren

Indien u meer geavanceerde eigenschappen nodig hebt om de implementatie van uw database te ondersteunen, kunt u dat doen nadat de wizard voor voltooiing van de installatie klaar is met de uitvoering. Configuration Manager ondersteunt alle opties voor databaseverbindingen die door het JDBC-stuurprogramma van de leverancier worden ondersteund en kan worden geconfigureerd met de URL van de databaseverbinding. Om meer geavanceerde verbindingen te configureren, bewerkt u de eigenschap **jdbc.url** in het bestand <**Configuration Manager-installatiemap**>**conf****database.properties**.

Hieronder vindt u voorbeelden van meer geavanceerde opties voor Microsoft SQL Server:

➤ **Windows (NTLM)-verificatie.** Om Windows-verificatie toe te passen, voegt u de domeineigenschap toe aan de verbindings-URL van JTDS in het bestand met database-eigenschappen. Geef het te verifiëren Windows-domein op.

Bijvoorbeeld:

```
jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
```

- **SSL.** Raadpleeg http://jtds.sourceforge.net/faq.html voor informatie over het verzekeren van de MS SQL-serververbinding met behulp van SSL.

Hieronder vindt u voorbeelden van meer geavanceerde opties voor Oracle Database Server:

- **Oracle URL.** Geef de verbindings-URL op van het systeemeigen stuurprogramma van Oracle. Vermeld een geldige Oracle-servernaam en SID. Indien u **Oracle RAC** gebruikt, geeft u de configuratiegegevens van Oracle RAC op.

Let op: Raadpleeg http://www.orafaq.com/wiki/JDBC#Thin_driver voor meer informatie over de configuratie van het systeemeigen URL-formaat van Oracle. Raadpleeg http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm voor meer informatie over de configuratie van de URL voor Oracle RAC.

- **SSL.** Hier vindt u de uitleg over het verzekeren van de Oracle-verbinding met behulp van SSL:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Databaseconfiguratie - MLU (Multi-Lingual Unit)-ondersteuning

In dit gedeelte worden de database-instellingen beschreven die vereist zijn om lokalisatie te ondersteunen.

Oracle-serverinstellingen

In deze tabel worden de vereiste instellingen voor Oracle Server opgesomd:

Optie	Ondersteund	Aanbevolen	Opmerkingen
Tekenset	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Microsoft SQL Server-instellingen

In deze tabel worden de vereiste instellingen voor Microsoft SQL Server opgesomd:

Optie	Ondersteund	Aanbevolen	Opmerkingen
Sortering	Niet hoofdlettergevoelig. Binaire sorteervolgorde en hoofdlettergevoeligheid worden niet ondersteund. Enkel de niet-hoofdlettergevoelige volgorde met een combinatie van accent-, kana- of breedte-instellingen wordt ondersteund.	Gebruik het dialoogvenster voor de sorteringsinstellingen om de sortering te selecteren. Selecteer het binaire selectievakje niet. Accent-, kana- en breedtegevoeligheid moeten worden geselecteerd volgens de relevante vereisten voor de taal. De geselecteerde taal moet dezelfde zijn als de taal in de regionale instellingen van het Windows-besturingssysteem.	Beperkt tot de landinstellingen voor sortering en de Engelse standaarddefinities.
Sorteringsdatabase-eigenschap	Standaardinstelling server		

Let op:

Voor alle talen is **<Taal>_CI_AS** de minimaal vereiste optie.
In het Japans, bijvoorbeeld, als u de Kana-gevoelige en breedtegevoelige opties wilt selecteren, is de aanbevolen optie **Japanese_CI_AS_KS_WS** of **Japanese_90_CI_AS_KS_WS**. Hiermee geeft u aan dat de Japanse tekens accentgevoelig, Kana-gevoelig en breedtegevoelig zijn.

- **Accentgevoelig (Accent-sensitive (_AS)).** Hiermee wordt een onderscheid gemaakt tussen tekens met en tekens zonder accent. **a** is bijvoorbeeld niet hetzelfde als **á**. Indien deze optie niet geselecteerd is, beschouwt Microsoft SQL Server de versie met accent en de versie zonder accent van letters als identiek met het oog op sortering.
- **Kana-gevoelig (Kana-sensitive (_KS)).** Hiermee wordt een onderscheid gemaakt tussen de twee soorten Japanse kana-tekens: Hiragana en Katakana. Indien deze optie niet geselecteerd is, beschouwt Microsoft SQL Server de Hiragana- en Katakana-tekens als identiek met het oog op sortering.
- **Breedtegevoelig (Width-sensitive (_WS)).** Hiermee wordt een onderscheid gemaakt tussen een teken van één byte en hetzelfde teken als dat als teken met twee bytes wordt weergegeven. Indien deze optie niet geselecteerd is, beschouwt Microsoft SQL Server weergave in één byte en de weergave in twee bytes van hetzelfde teken als identiek met het oog op sortering.

Lightweight Single Sign-On inschakelen

Sommige Configuration Manager-gebruikers hebben machtiging om zich bij UCMDB aan te melden. Voor het gemak biedt Configuration Manager een rechtstreekse koppeling met de gebruikersinterface van UCMDB (selecteer **Beheer** > **UCMDB openen**). Om single sign-on te gebruiken (zodat u zich niet langer bij UCMDB moet aanmelden na de aanmelding bij Configuration Manager) moet u LW-SSO inschakelen voor zowel Configuration Manager als UCMDB en moet u ervoor zorgen dat ze beide met dezelfde initString werken. In deze opdracht wordt beschreven hoe u LW-SSO inschakelt in Configuration Manager en in UCMDB.

Om LW-SSO in te schakelen:

1 Open het volgende bestand in de installatiemap van Configuration Manager: **\servers\server-0\webapps\cnc\WEB-INF\classes\ cnclwssofmconf.xml**.

Let op: Dit bestand bestaat niet voordat u Configuration Manager start.

---

2 Zoek het volgende gedeelte:

```
enableLWSSO enableLWSSOFramework="true"
```

en controleer of de waarde **true** is.

3 Zoek het volgende gedeelte:

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

en voer het Configuration Manager-serverdomein in na <**domain**>.

4. Zoek het volgende gedeelte:

   ```
   <initString="This string should be replaced"></crypto>
   ```

   en vervang "This string should be replaced" door een gedeelde tekenreeks die door alle vertrouwde toepassingen wordt gebruikt die met LW-SSO worden geïntegreerd.

5. Zoek het volgende gedeelte:

   ```
   <!--multiDomain>
   <trustedHosts>
   <DNSDomain>This value should be replaced by your application
   domain</DNSDomain>
   <DNSDomain>This value should be replaced by domain of other
   application</DNSDomain>
   </trustedHosts>
   </multiDomain-->
   ```

   Verwijder het opmerkingenteken aan het begin en voer de Configuration Manager-serverdomeinen in in de DNSDomain-elementen (in plaats van This value should be replaced by your application domain). De lijst moet het serverdomein bevatten dat werd ingevoerd bij 3 op pagina 20.

6. Sla het bestand met uw wijzigingen op en start de server opnieuw op.

7. Start een webbrowser en voer het volgende adres in: http://<UCMDB-serveradres>.<domeinnaam>:8080/jmx-console.

   Voer de aanmeldingsgegevens voor de verificatie in de JMX-console in. De standaardaanmeldingsgegevens zijn:

   - Aanmeldingsnaam = **sysadmin**
   - Wachtwoord = **sysadmin**

8. Onder **UCMDB-UI** selecteert u **LW-SSO-configuratie** om de weergavepagina van JMX MBEAN te openen.

9. Selecteer de methode **setEnabledForUI**, stel de waarde in op **true** en klik op **Invoke**.

10. Selecteer de methode **setDomain**. Voer de domeinnaam van de UCMDB-server in en klik op **Invoke**.

11 Selecteer de methode **setInitString**. Voer dezelfde initString in die u voor Configuration Manager hebt ingevoerd in stap 4 op pagina 21 en klik op **Invoke**.

12 Indien Configuration Manager en UCMDB zich elk in een ander domein bevinden, selecteert u de methode **addTrustedDomains** en voert u de domeinnaam van de UCMDB- en van deConfiguration Manager-server in. Klik op **Invoke**.

13 Om de LW-SSO-configuratie te zien zoals die in het instellingenmechanisme is opgeslagen, selecteert u de methode **retrieveConfigurationFromSettings** en klikt u op **Invoke**.

14 Om de werkelijk geladen LW-SSO-configuratie te zien, selecteert u de methode **retrieveConfiguration** en klikt u op **Invoke**.

IPv6-ondersteuning

Configuration Manager ondersteunt alleen IPv6-URL's voor URL's die klanten kunnen gebruiken.

Om met Configuration Manager te werken met behulp van een IPv6-adres:

1 Zorg ervoor dat uw besturingssysteem IPv6 ondersteunt. Raadpleeg de documentatie van het besturingssysteem voor meer informatie.

2 Open het bestand **client-config.properties** dat zich in de map **conf** van de <**Configuration Manager Install Directory**> bevindt. Wijzig de waarde van de parameter **bsf.server.url** in het IPv6-adres dat tussen vierkante haken staat. Bijvoorbeeld:

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

2

Configuratiewizard voor voltooiing van de installatie van Configuration Manager

In dit hoofdstuk vindt u:

Configuratieoverzicht voor voltooiing van de installatie van Configuration Manager

In dit hoofdstuk vindt u gedetailleerde beschrijvingen van de pagina's voor de wizard voor voltooiing van de installatie van Configuration Manager en de bijbehorende configuratietaken. Dit is de inhoud die wordt geopend wanneer u op een van de pagina's in de wizard op **Help** klikt.

Pagina Databaseverbinding

Dit gedeelte omvat:

Algemeen

Er moet een databaseverbinding opgezet worden die wordt geassocieerd met een standaard-URL-verbinding. Indien meer geavanceerde eigenschappen nodig zijn, zoals Oracle Real Application Cluster, stelt u een standaardverbinding op en bewerkt u vervolgens het bestand **database.properties** handmatig om de geavanceerde functies te configureren.

Configuration Manager maakt gebruik van systeemeigen stuurprogramma's voor zowel Oracle als voor Microsoft SQLServer. Dat betekent dat over het algemeen alle functies van de systeemeigen stuurprogramma's worden ondersteund, op voorwaarde dat die functies kunnen worden geconfigureerd met behulp van de database-URL. De URL bevindt zich in het bestand **database.properties**.

Let op: De configuratie van geavanceerde functies moet gebeuren na de procedure van de voltooiing van de installatie en nadat een werkende configuratie werd opgezet.

Parameters

Om de databaseverbinding in te stellen, moeten de volgende parameters gedefinieerd worden:

Parameter	Aanbevolen waarde	Beschrijving
Leverancier	<gedefinieerd door gebruiker>	Databaseleverancier Mogelijke waarden: **Oracle** of **Microsoft** HP Universal CMDB kan worden geïnstalleerd met hetzelfde installatieprogramma als Configuration Manager, of afzonderlijk. Indien Configuration Manager en UCMDB op dezelfde machine worden geïnstalleerd met behulp van hetzelfde installatieprogramma, is de standaardwaarde voor deze parameter de databaseleverancier die al geselecteerd is in de wizard voor voltooiing van de installatie van UCMDB. Enkel wanneer beide installaties worden geïnstalleerd met behulp van dezelfde installatieprogramma's, worden de standaardwaarden ingesteld. Indien u ze installeert met behulp van afzonderlijke installatiepakketten zullen de standaardwaarden NIET verschijnen in deze wizard voor voltooiing van de installatie, zelfs wanneer UCMDB op dezelfde machine als Configuration Manager is geïnstalleerd.

Parameter	Aanbevolen waarde	Beschrijving
Hostnaam	<gedefinieerd door gebruiker>	Hostnaam van de databaseserver Indien Configuration Manager en UCMDB op dezelfde machine worden geïnstalleerd, is de standaardwaarde voor deze parameter de databaseserver die al geselecteerd is in de wizard voor voltooiing van de installatie van UCMDB. **Deze waarde is vereist.**
Poort	<gedefinieerd door gebruiker>	Poort van de database-listener Indien Configuration Manager en UCMDB op dezelfde machine worden geïnstalleerd, is de standaardwaarde voor deze parameter de databasepoort die al geselecteerd is in de wizard voor voltooiing van de installatie van UCMDB. Voor Oracle is de standaardwaarde **1521**. Voor Microsoft SQL Server is de standaardwaarde **1433**. **Deze waarde is vereist.**
SID/DB	<gedefinieerd door gebruiker>	Naam van de Oracle SID of de naam van de Microsoft SQL Server-database. Indien Configuration Manager en UCMDB op dezelfde machine worden geïnstalleerd, is de standaardwaarde voor deze parameter de dis/db die al geselecteerd is in de wizard voor voltooiing van de installatie van UCMDB. **Deze waarde is vereist.**

Parameter	Aanbevolen waarde	Beschrijving
Gebruikersnaam	<gedefinieerd door gebruiker>	Gebruikersnaam die wordt gebruikt om zich aan te melden bij de database. **Deze waarde is vereist.**
Wachtwoord	<gedefinieerd door gebruiker>	Wachtwoord dat wordt gebruikt om zich aan te melden bij de database.

Opties

De volgende opties zijn ook beschikbaar:

Parameter	Aanbevolen waarde	Beschrijving
Wachtwoord coderen	<gedefinieerd door gebruiker>	Indien deze optie geselecteerd is, wordt het wachtwoord in het bestand **database.properties** gecodeerd. Om beveiligingsredenen is het aan te bevelen om wachtwoorden die in tekstbestanden zijn opgeslagen, te coderen.
Schema-objecten maken	<gedefinieerd door gebruiker>	Indien deze optie geselecteerd is, worden de schema-objecten gemaakt die vereist zijn om Configuration Manager uit te voeren. U mag deze optie enkel uitschakelen indien bij de installatie een bestaand schema wordt gebruikt dat al eerder werd gemaakt en ingevuld met Configuration Manager-objecten.

Test

Let op: Het is ten sterkste aan te bevelen om de verbindingseigenschappen te testen voordat u doorgaat.

Om de verbindingseigenschappen te testen, klikt u op **Testen**. De wizard probeert om toegang te krijgen tot de database en om de verbinding te controleren. De testresultaten verschijnen rechts van de knop **Testen**.

De database genereert verschillende foutmeldingen. Die wijzen zichzelf uit. Ze hebben meestal te maken met de invoer van een foutieve gebruikersnaam of een foutief wachtwoord. De fout moet worden rechtgezet en dat moet worden gevolgd door een geslaagd testresultaat voordat u doorgaat.

Pagina toepassingsserver

Dit gedeelte omvat:

➤ "Algemeen" op pagina 30

➤ "Parameters" op pagina 30

Algemeen

Stel de Configuration Manager-toepassingsserver in met de standaardpoortnummers die hieronder staan.

Parameters

Om de Configuration Manager-toepassingsserver in te stellen, moeten de volgende parameters gedefinieerd worden:

Parameter	Aanbevolen waarde	Beschrijving
Hostnaam	<gedefinieerd door gebruiker>	Externe naam van de toepassingsserver Standaard is deze waarde de geldige hostnaam van de machine waarop de wizard (en Configuration Manager) wordt uitgevoerd. In sommige implementeringen moet deze naam anders zijn, bijvoorbeeld wanneer een webserver wordt geïmplementeerd vóór de Configuration Manager-toepassingsserver.
Poorten aanpassen	<gedefinieerd door gebruiker>	Standaard is deze optie niet geselecteerd. Wanneer ze wel geselecteerd is, kunt u de standaardpoortnummers van de toepassingsserver aanpassen.
HTTP-poort	<gedefinieerd door gebruiker>	HTTP-poort van de Configuration Manager-toepassingsserver Standaardwaarde: **8080** Standaardwaarde wanneer geïnstalleerd op dezelfde machine als HP Universal CMDB: **8180**

Parameter	Aanbevolen waarde	Beschrijving
HTTPS-poort	<gedefinieerd door gebruiker>	HTTPS-poort van de Configuration Manager-toepassingsserver Standaardwaarde: **8443** Standaardwaarde wanneer geïnstalleerd op dezelfde machine als UCMDB: **8143**
Tomcat-poort	<gedefinieerd door gebruiker>	Poort voor het beheer van Configuration Manager-toepassingsserver Standaardwaarde: **8005**
AJP-poort	<gedefinieerd door gebruiker>	AJP-poort (Apache Java Protocol) Configuration Manager-toepassingsserver Standaardwaarde: **8009**
JMX HTTP-poort	<gedefinieerd door gebruiker>	JMX HTTP-poort Configuration Manager-toepassingsserver Standaardwaarde: **39900**
Externe poort JMX	<gedefinieerd door gebruiker>	JMX externe poort Configuration Manager-toepassingsserver Standaardwaarde: **39600**

Configuratiepagina Windows Service

Selecteer of Configuration Manager al dan niet als Windows-service moet worden geïnstalleerd. Deze optie is alleen beschikbaar bij installatie op een Windows-machine.

De Windows-service kan handmatig worden ingesteld met behulp van het hulpprogramma **create-windows-service.bat** in de map **cnc-home/bin**.

Pagina aanmeldingsgegevens gebruikers

Dit gedeelte omvat:

➤ "Algemeen" op pagina 32

Algemeen

Stel de volgende initiële gebruikers van Configuration Manager in:

Parameter	Aanbevolen waarde	Beschrijving
Admin-gebruiker	<gedefinieerd door gebruiker>	Administratieve gebruiker van Configuration Manager, de "super user"
Integratiegebruiker	<gedefinieerd door gebruiker>	Gebruiker die met het oog op integratie is aangemaakt door Configuration Manager in HP Universal CMDB

Let op: U moet gebruikersnaam en wachtwoord als aanmeldingsgegevens opgeven voor zowel de administratieve als voor de integratiegebruiker.

Pagina voor verbinding met HP Universal CMDB

Dit gedeelte omvat:

Algemeen

De verbinding met HP Universal CMDB instellen, is optioneel.

Wanneer Configuration Manager wordt geïnstalleerd op dezelfde machine als UCMDB in een gecombineerde installatie, hoeft u op deze pagina niets in te vullen.

Wanneer u UCMDB niet in een gecombineerde installatie installeert, of wanneer u UCMDB op een andere machine installeert (zelfs wanneer u UCMDB met de localhost verbindt) of wanneer u UCMDN installeert voordat u Configuration Manager installeert, moet UCMDB actief zijn en moet u deze verbindingseigenschappen opgeven.

Let op: Wanneer u installeert met behulp van een extern exemplaar van UCMDB, moet het exemplaar actief zijn. Wanneer u zowel Configuration Manager als UCMDB op dezelfde machine installeert, moet UCMDB inactief zijn terwijl deze wizard wordt uitgevoerd.

Parameters

Om de UCMDB-verbinding in te stellen, moeten de volgende parameters gedefinieerd worden:

Parameter	Aanbevolen waarde	Beschrijving
Gebruik HP UCMDB op een andere host	<gedefinieerd door gebruiker>	Selecteer deze optie om alle andere eigenschappen in te schakelen wanneer Configuration Manager en UCMDB op verschillende machines worden geïnstalleerd.
Hostnaam	<gedefinieerd door gebruiker>	Hostnaam waarop UCMDB geïnstalleerd is
Poort	<gedefinieerd door gebruiker>	Poort waarop UCMDB luistert
Protocol	<gedefinieerd door gebruiker>	HTTP of HTTPS
Klant	<gedefinieerd door gebruiker>	UCMDB-klant
Administratieve gebruikersnaam	<gedefinieerd door gebruiker>	UCMDB sysadmin-gebruikersnaam
Administratief wachtwoord	<gedefinieerd door gebruiker>	UCMDB sysadmin-wachtwoord

Test

Let op: Het is ten sterkste aan te bevelen om de verbindingseigenschappen te testen voordat u doorgaat.

Om de verbindingseigenschappen te testen, klikt u op **Testen**. De wizard probeert om toegang te krijgen tot UCMDB en om de verbinding te controleren. De testresultaten verschijnen rechts van de knop **Testen**.

UCMDB genereert verschillende foutmeldingen. Die wijzen zichzelf uit. Ze hebben meestal te maken met het invoer van een foutieve gebruikersnaam of een foutief wachtwoord. De fout moet worden rechtgezet en dat moet worden gevolgd door een geslaagd testresultaat voordat u doorgaat.

Overzichtspagina

Alle selecties die op de vorige pagina's van de wizard werden gemaakt, worden weergegeven. Ga na of alle selecties juist zijn en breng eventueel de nodige wijzigingen aan. Wanneer alle selecties correct zijn, klikt u op **Volgende** en de wizard voltooit de configuratieopdrachten.

Voltooiingspagina

Dit is de laatste pagina van de configuratiewizard voor voltooiing van de **installatie** van Configuration Manager. De configuratietaken van de voltooiing van de installatie zijn gereed. Klik op **Voltooien** om de wizard te sluiten.

Let op: Zelfs wanneer alle taken met succes voltooid zijn, is het aan te bevelen om de logboeken te controleren die u vindt in **cnc-home/tmp/chp/app.log**.

3

LDAP configureren

HP UCMDB Configuration Manager maakt gebruik van LDAP voor het beheer van gebruikers, rollen en machtigingen. In dit hoofdstuk worden de stappen beschreven voor de configuratie en de probleemoplossing van LDAP.

Dit hoofdstuk omvat:

LDAP-overzicht

Configuration Manager wordt geleverd met een LDAP-server (in de gebruikersinterface **Shared (Gedeeld)** genoemd) en kan ook verbinding maken met een LDAP-organisatieserver. Configuration Manager gebruikt die servers om gebruikers, groepen en rollen te zoeken, om personalisatiegegevens op te slaan en om gebruikers te verifiëren. U kunt zelf kiezen welke daarvan gebruik maken van de LDAP-organisatieserver en welke van de interne LDAP-server.

Bij een typische implementatie wordt de interne (gedeelde) LDAP-server gebruikt om rollen op te slaan en wordt de externe LDAP-server (organisatieserver) voor al de rest gebruikt.

Providers kiezen

1. Meld u aan bij **Configuration Manager** als beheerder.
2. Ga naar **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** en selecteer SHARED (GEDEELD) of EXTERNAL (EXTERN) voor elk van de volgende attributen, volgens uw eigen voorkeur voor de provider (SHARED is de standaardkeuze):
   - Verificatieprovider
   - Groepenprovider
   - Personaliseringsprovider
   - Rollenprovider
   - Rollenrelatieprovider
3. Sla de configuratieset op.

Verbinding maken met uw LDAP-organisatieserver

HP UCMDB Configuration Manager is initieel geconfigureerd met een interne (gedeelde) LDAP. In dit gedeelte worden de stappen beschreven om verbinding te maken met uw LDAP-organisatieserver.

Dit gedeelte omvat:

De LDAP-verbinding configureren

In dit gedeelte wordt uitgelegd hoe u Configuration Manager verbindt met een externe LDAP-server. De externe LDAP-server is de LDAP-organisatieserver. Hij bevat de organisatiegebruikers.

1 Meld u aan bij **Configuration Manager** als beheerder.

2 Ga naar **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats** en werk de volgende attributen bij volgens de eigenschappen van uw organisatie-LDAP:

Algemene LDAP-verbinding

ldapHost: <Hostnaam LDAP>

ldapPort: <Poortnummer LDAP>

enableSSL: <True/false—gebruik SSL-verbinding met LDAP>

useAdministrator: <True/false—gebruik gebruiker voor verbinding met LDAP>

ldapAdministrator: <LDAP-gebruikersnaam (moet worden opgegeven indien **useAdministrator=true)**>

ldapAdministratorPassword: <LDAP-gebruikerswachtwoord (moet worden opgegeven indien **useAdministrator=true**)>

3 Sla de configuratieset op.

Configureer de providers van groepen en gebruikers

Met deze procedure wordt de organisatie-LDAP (externe opslagplaats) ingesteld als provider voor groepen en gebruikers. De interne LDAP (gedeelde opslagplaats) wordt nog steeds gebruikt voor de verificatie, maar de gebruikers en groepen worden uit de externe LDAP opgehaald. Deze modus wordt gebruikt om de externe LDAP-configuratie te testen en om machtigingen toe te wijzen aan de organisatiegebruikers.

Om de providers van groepen en gebruikers in te stellen:

1. Als u nog niet op deze pagina staat, gaat u naar **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats**. Zorg dat u hetzelfde ontwerp van de configuratieset gebruikt als degene die u hebt opgeslagen in het gedeelte "De LDAP-verbinding configureren" op pagina 39.
2. Werk de volgende attributen bij volgens de eigenschappen van uw organisatie-LDAP:

   a **Zoekopdracht gebruikers**

   usersBase: <Basis-DN voor zoekopdracht gebruikers>

   usersScope: <Bereik voor zoekopdracht gebruikers>

   usersFilter: <Filter voor zoekopdracht gebruikers>

   b **Objectklasse gebruikers** (hangt af van LDAP-leverancier)

   usersObjectClass: <Objectklasse gebruikers LDAP>

   usersUniqueIDAttribute: <LDAP-attribuut unieke ID van gebruikers>

   De volgende attributen zijn optioneel:

   usersDisplayNameAttribute: <LDAP-attribuut weergavenaam van gebruikers>

   usersLoginNameAttribute: <LDAP-attribuut aanmeldingsnaam van gebruikers>

   usersLoginNameAttribute: <LDAP-attribuut aanmeldingsnaam van gebruikers>

   usersLastNameAttribute: <LDAP-attribuut achternaam van gebruikers>

   usersEmailAttribute: <LDAP-attribuut e-mail van gebruikers>

   usersPreferredLanguageAttribute: <LDAP-attribuut voorkeurtaal van gebruikers>

   usersPreferredLocationAttribute: <LDAP-attribuut voorkeurplaats van gebruikers>

   usersTimeZoneAttribute: <LDAP-attribuut tijdzone van gebruikers>

usersDateFormatAttribute: <LDAP-attribuut datumopmaak van gebruikers>

usersNumberFormatAttribute: <LDAP-attribuut datumopmaak van gebruikers>

usersWorkWeekAttribute: <LDAP-attribuut werkweek van gebruikers>

usersTenantIDAttribute: <LDAP-attribuut tenant-ID van gebruikers>

usersPasswordAttribute: <LDAP-attribuut wachtwoord van gebruikers>

c **Zoekopdracht groepen**

groupsBase: <Basis-DN voor zoekopdracht groepen>

groupsScope: <LDAP-bereik voor zoekopdracht groepen>

groupsFilter: <Filter voor zoekopdracht groepen>

rootGroupsBase: <Basis-DN voor zoekopdracht hoofdgroepen>

rootGroupsScope: <LDAP-bereik voor zoekopdracht hoofdgroepen>

rootGroupsFilter: <Filter voor zoekopdracht groepen>

d **Objectklasse groepen** (hangt af van LDAP-leverancier)

groupsObjectClass: <Objectklasse groepen LDAP>

groupsMembersAttribute: <LDAP-attribuut groepsleden>

De volgende attributen zijn optioneel:

groupsNameAttribute: <LDAP-attribuut unieke naam groepen>

groupsDisplayNameAttribute: <LDAP-attribuut weergavenaam groepen>

groupsDescriptionAttribute: <LDAP-attribuut groepsbeschrijving>

enableDynamicGroups: <Dynamische groepen inschakelen>

dynamicGroupsClass: <Objectklasse dynamische groepen LDAP>

dynamicGroupsMemberAttribute: <LDAP-attribuut leden dynamische groepen>

dynamicGroupsNameAttribute: <LDAP-attribuut unieke naam dynamische groepen>

dynamicGroupsDisplayNameAttribute: <LDAP-attribuut weergavenaam dynamische groepen>

dynamicGroupsDescriptionAttribute: <LDAP-attribuut beschrijving dynamische groepen>

e **Groepshiërarchie** (indien uw organisatie-LDAP groepshiërarchie gebruikt)

enableNestedGroups: <Ondersteuning van geneste groepen inschakelen>

maximalAllowedGroupsHierarchyDepth: <Maximale toegestane diepte van groepshiërarchie>

f **Geavanceerde configuratie**

ldapVersion: <LDAP-versie>

baseDistinguishNameDelimiter: <Scheidingsteken basis-DN>

scopeDelimiter: <Scheidingsteken bereik>

attributeValuesDelimiter: <Scheidingsteken waarden LDAP-attribuut>

3 Sla het ontwerp van de configuratieset op.

Activeer de configuratieset

1 Ga naar **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** en werk het volgende bij:

Externe UUM-bron: True

Groepenprovider: EXTERNAL

Gebruikersprovider: EXTERNAL

2 Sla de configuratieset op en activeer hem.

3 Meld u af en start de **Configuration Manager**-server opnieuw op.

Wijzigingen aan gebruikers toewijzen

Met deze procedure wordt de rol van **Systeembeheerder** toegewezen aan de organisatiegebruiker(s). Een gebruiker met de rol van **Systeembeheerder** heeft machtigingen om de relevante rollen aan de rest van de organisatiegebruikers toe te wijzen.

1. Meld u aan bij **Configuration Manager** als beheerder.
2. Opn de module **Gebruikersbeheer** (**Beheer** > **Gebruikersbeheer**).
3. Controleer of u de groepen en gebruikers van uw organisatie-LDAP ziet.
4. Ga naar **Gebruikersbeheer** > **Deelvenster gebruikers zoeken** en zoek de gebruiker(s) die als beheerder(s) zal/zullen fungeren. Bijvoorbeeld: Voornaam = j*, Achternaam = Smith.
5. Voeg de rol van **System administrator (Systeembeheerder)** toe aan de gebruiker(s).

Stel de verificatieprovider in op de externe LDAP

Met deze procedure wordt de externe organisatie-LDAP ingesteld op de Verificatieprovider, zodat de organisatiegebruikers voor verificatie worden gebruikt.

1. Ga naar **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** en werk het volgende bij:

   Verificatieprovider: EXTERNAL
2. Sla de configuratieset op en activeer hem.
3. Meld u af en start de **Configuration Manager**-server opnieuw op.
4. Meld u aan met een van de organisatiegebruikers die de rol van **Systeembeheerder** hebben gekregen.

Het LDAP-certificaat importeren

Indien een certificaat vereist is om verbinding te maken met uw organisatie-LDAP, voert u de volgende stappen uit:

1. Exporteer het certificaat naar een bestand.
2. Stop de Windows-service van Configuration Manager.

3 Voer de volgende opdracht uit:

<Configuration Manager-installatie>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <certificaatalias> -keystore <Configuration Manager-installatie>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <bestandspad certificaat>

4 Start de Windows-service van Configuration Manager.

Interne (gedeelde) LDAP configureren

Het wachtwoord van de interne (gedeelde) LDAP-server wijzigen (optioneel)

U kunt het wachtwoord van de interne (gedeelde) LDAP-server wijzigen uit veiligheidsoverwegingen.

1 Meld u aan bij **HP Universal CMDB Configuration Manager**.

2 Open een opdrachtregel en navigeer naar de map **<Configuration Manager-installatie>\ldap\serverRoot\bat**.

3 Voer **ldappasswordmodify -h localhost -p <ldap port> -D "cn=Directory Manager" -w <ldap admin-wachtwoord> -c <ldap admin-wachtwoord> -n <nieuw ldap admin-wachtwoord>** uit.

   a Het standaardwachtwoord van de admin voor ldap is **ldapadmin**.

   b De standaardpoort is **2389**.

   c Ga na of de uitvoering van de opdracht geslaagd is en ga dan pas verder met de volgende stappen.

4 In **UCMDB Configuration Manager** selecteert u **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Gedeelde gebruikersopslagplaats**.

5 Werk het wachtwoord bij in het attribuut **ldapAdministratorPassword**.

6 Sla de configuratieset op en activeer hem.

7 Meld u af bij **UCMDB Configuration Manager**.

8 Start de **UCMDB Configuration Manager**-server opnieuw op.

De interne (gedeelde) LDAP-poort configureren

De standaardpoort, 2389, wordt misschien al door een andere toepassing gebruikt. Om deze standaardpoort te wijzigen, gebruikt u de volgende procedure.

Om de interne LDAP-poort te configureren:

1. Open een opdrachtregel en navigeer naar de map <**Configuration Manager-installatie**>**ldap****serverRoot****bat**.
2. Voer de volgende opdracht uit:
   dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <ldap admin-wachtwoord> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<nieuwe poort>

   Het standaard<admin-wachtwoord voor ldap> is **ldapadmin**.
3. Ga na of er geen foutmelding wordt weergegeven en ga dan pas verder met de volgende stappen.
4. Meld u aan bij HP Universal CMDB Configuration Manager.
5. In UCMDB Configuration Manager selecteert u B**eheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Gedeelde gebruikersopslagplaats** en werkt u het poortnummer bij in het attribuut **ldapPort**.
6. Sla de configuratieset op en activeer hem.
7. Meld u af bij UCMDB Configuration Manager.
8. Start de UCMDB Configuration Manager-server opnieuw op.

Probleemoplossing LDAP

Probleem: communicatie met LDAP-server kan niet worden uitgevoerd. Communicatie-uitzondering verschijnt in logboeken.

Oplossing: controleer de LDAP-host, de poort en de SSL-modusinstellingen:

a Controleer of de LDAP-host en de poort juist geconfigureerd zijn: Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats** en controleer de instellingen **ldapHost, ldapPort**.

b Controleer of de SSL-modus juist geconfigureerd is. Vraag bij uw organisatie-LDAP-beheerder of de beheerder vereist is voor een LDAP-verbinding. Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats** en controleer de instelling **enableSSL**.

c Controleer of het juiste servercertificaat geïnstalleerd is. Voer de volgende opdracht uit:

<Configuration Manager-installatie>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <certificaatalias>] -keystore <Configuration Manager-installatie>\java\windows\x86_64\lib\security\cacerts -storepass changeit

d Vraag bij uw organisatie-LDAP-beheerder of de beheerder vereist is voor een LDAP-verbinding. Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats** en controleer de volgende instellingen: **useAdministrator, ldapAdministrator, ldapAdministratorPassword**

Probleem: er verschijnen geen groepn in het beheerscherm voor gebruikers of groepen. Er verschijnt geen uitzondering in de logboeken.

Oplossing: controleer het volgende:

a Controleer of de zoekfilters voor gebruikers en groepen juist geconfigureerd zijn: Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats** en pas de volgende eigenschappen aan: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

b Open de LDAP-clientbrowser en zoek de gebruikers onder de basis-DNS.

Probleem: gebruikersinterface is te langzaam.

Oplossing: gewoonlijk komt dit omdat er te veel groepen of gebruikers in uw LDAP geconfigureerd zijn. Configureer de basis-DNS en de filters zo, dat het aantal groepen van de relevante subset als volgt wordt beperkt:

a Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats**

b Pas de volgende instellingen aan: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

Probleem: sommige gekende gebruikers verschijnen niet op het scherm voor groepen- of gebruikersbeheer.

Oplossing: in het scherm voor groepen- of gebruikersbeheer verschijnen alleen gebruikers die tot een groep behoren. Plaats de gebruikers in LDAP in de juiste groepen om ze op het hoofdscherm te kunnen zien.

Probleem: aanmelden duurt lang.

Oplossing: het is mogelijk dat de gebruiker lid is van te veel groepen. U kunt de opstarttijd optimaliseren door de zoekfilter van de groepen te wijzigen, zodat er minder groepen worden gevonden. Dat doet u zo:

a Selecteer **Beheer** > **Serverbeheer** > **Gebruikersbeheer** > **Configuratie gebruikersbeheer** > **Externe gebruikersopslagplaats**

b Pas de instelling **groupsFilter** aan.

4

Verificatie bij Lightweight via eenmalige aanmelding (Single Sign-On (LW-SSO)) - Algemene leidraad

In dit hoofdstuk vindt u:

Overzicht LW-SSO-verificatie

LW-SSO is een toegangscontrolemethode waarmee de gebruiker zich één keer kan aanmelden en toegang krijgt tot de bronnen van meerdere softwaresystemen zonder dat hem wordt gevraagd om zich opnieuw aan te melden. De toepassingen binnen de geconfigureerde groep softwaresystemen vertrouwen de verificatie en een verdere verificatie is niet nodig wanneer van de ene toepassing naar de andere wordt gegaan.

De informatie in dit gedeelte is van toepassing op LW-SSO-versie 2.2 en 2.3.

In dit gedeelte vindt u de volgende onderwerpen:

➤ "SecurityToken ophalen voor URL-functionaliteit" op pagina 50

Verloop van het LW-SSO-token

De verloopwaarde van het LW-SSO-token bepaalt de geldigheid van de sessie van de toepassing. Daarom moet de verloopwaarden ten minste dezelfde waarde hebben als die van de verlooptijd van de sessie van de toepassing.

Aanbevolen configuratie van de verlooptijd van de LW-SSO

Voor elke toepassing die gebruikmaakt van LW-SSO moet tokenverloop geconfigureerd zijn. De aanbevolen waarde is 60 minuten. Voor een toepassing waarvoor geen hoog beveiligingsniveau vereist is, is het mogelijk om een waarde van 300 minuten te configureren.

GMT-tijd

Alle toepassingen die deel uitmaken van een LW-SSO-integratie moeten dezelfde GMT-tijd gebruiken, met een maximumverschil van 15 minuten.

Functionaliteit voor meerdere domeinen

Voor de functionaliteit voor meerdere domeinen moeten voor alle toepassingen die deel uitmaken van LW-SSO-integratie de instellingen van de trustedHost geconfigureerd zijn (of de instellingen voor **protectedDomains**), indien ze moeten kunnen integreren met toepassingen van andere DNS-domeinen. Bovendien moeten ze het juiste domein toevoegen in het element **lwsso** van de configuratie.

SecurityToken ophalen voor URL-functionaliteit

Om van andere toepassingen informatie te ontvangen die als **SecurityToken voor URL** werd verzonden, moet de hosttoepassing het juiste domein configureren in het element **lwsso** van de configuratie.

Beveiligingswaarschuwingen LW-SSO

In dit gedeelte worden beveiligingswaarschuwingen beschreven die relevant zijn voor de LW-SSO-configuratie.

- **Vertrouwelijke InitString-parameter in LW-SSO.** LW-SSO maakt gebruik van symmetrische codering om een LW-SSO-token te valideren en te maken. De parameter **initString** binnen de configuratie wordt gebruikt voor initialisatie van de geheime sleutel. Een toepassing maakt een token aan en elke toepassing die dezelfde initString-parameter gebruikt, valideert het token.

Caution:

- Het is niet mogelijk om LW-SSO te gebruiken zonder de parameter **initString** in te stellen.
- De parameter **initString** is vertrouwelijke informatie en moet ook zo worden behandeld bij het publiceren, transporteren en bij de handhaving ervan.
- De parameter **initString** mag enkel worden gedeeld tussen toepassingen die met elkaar integreren met behulp van LW-SSO.
- De parameter **initString** moet minimaal 12 tekens lang zijn.

- **LW-SSO alleen inschakelen indien vereist.** LW-SSO moet uitgeschakeld zijn, behalve indien specifiek vereist.
- **Niveau van verificatiebeveiliging.** De toepassing die het zwakste verificatieframework gebruikt en die een LW-SSO-token uitgeeft dat door andere geïntegreerde toepassingen wordt vertrouwd, bepaalt het niveau van beveiligingsinformatie voor alle toepassingen.

  Het is aanbevolen dat enkel toepassingen met sterke en beveiligde verificatieframeworks een LW-SSO-token uitgeven.

- **Implicaties van symmetrische codering.** LW-SSO maakt gebruik van symmetrische cryptografie voor het uitgeven en valideren van LW-SSO-tokens. Daarom kan elke toepassing die een LW-SSO gebruikt, een token uitgeven dat door alle andere toepassingen wordt vertrouwd die dezelfde parameter **initString** delen. Dit risico is relevant wanneer een toepassing die een initString deelt, zich bevindt op, of kan worden geopend vanaf, een niet-vertrouwde locatie.

- **Gebruikerstoewijzing (synchronisatie).** Het LW-SSO-framework stelt de gebruikerstoewijzing tussen de geïntegreerde toepassingen niet zeker. Daarom moet de geïntegreerde toepassing gebruikerstoewijzing controleren. We raden u aan om hetzelfde gebruikersregister (als LDAP/AP) te delen tussen alle geïntegreerde toepassingen.

  Indien gebruikers niet worden toegewezen, kan dat leiden tot veiligheidsinbreuken en negatief gedrag van de toepassing. Zo kan dezelfde gebruikersnaam bijvoorbeeld worden toegewezen aan verschillende echte gebruikers in de verschillende toepassingen.

  Bovendien: wanneer een gebruiker zich aanmeldt bij een toepassing (ToepA) en vervolgens toegang krijgt tot een tweede toepassing (ToepB) die een container- of toepassingverificatie gebruikt, en de gebruiker kan niet worden toegewezen, dan is de gebruiker verplicht om zich handmatig aan te melden bij ToepB en een gebruikersnaam in te voeren. Indien de gebruiker een andere gebruikersnaam invoert dan de gebruikersnaam die werd ingevoerd om zich bij ToepA aan te melden, dan kan het volgende gedrag ontstaan: indien de gebruiker zich daarna toegang verschaft tot een derde toepassing (ToepC) van ToepA of ToepB, dan zal hij zich toegang verschaffen met behulp van de gebruikersnamen die werden gebruikt om zich aan te melden bij respectievelijk ToepA of ToepB.

- **Identity Manager**. Indien gebruikt ter verificatie, moeten alle onbeschermde bronnen in de Identity Manager worden geconfigureerd met de instelling **nonsecureURLs** in het configuratiebestand LW-SSO.

Probleemoplossing en beperkingen

Bekende problemen

In dit gedeelte worden de bekende problemen voor LW-SSO-verificatie beschreven.

- **Beveiligingscontext.** De LW-SSO-beveiligingscontext ondersteunt slechts één attribuutwaarde per attribuutnaam.

  Daarom wordt slechts één waarde geaccepteerd door het LW-SSO-framework wanneer het SAML2-token meer dan één waarde voor dezelfde attribuutnaam verzendt.

  Op dezelfde manier wordt slechts één waarde geaccepteerd door het LW-SSO-framework wanneer het idM-token meer dan één waarde voor dezelfde attribuutnaam verzendt.

- **Afmeldingsfunctionaliteit voor meerdere domeinen bij gebruik van Internet Explorer 7**. Afmeldingsfunctionaliteit voor meerdere domeinen kan onder de volgende voorwaarden vallen:

  - De gebruikte browser is Internet Explorer 7 en de toepassing roept meer dan drie opeenvolgende HTPP 302-omleidingsbewerkingen aan in de afmeldingsprocedure.

  In dat geval is het mogelijk dat Internet Explorer de HTTP 302-omleidingsreactie verkeerd verwerkt en dat in de plaats daarvan een foutpagina **De webpagina kan niet worden weergegeven** verschijnt.

  Om dat op te lossen, wordt aanbevolen om indien mogelijk het aantal omleidingsopdrachten van de toepassing in de afmeldingsprocedure te verlagen.

Beperkingen

Let op de volgende beperkingen bij het werken met LW-SSO-verificatie:

- **Clienttoegang tot de toepassing**.

  Indien een domein wordt opgegeven in de LW-SSO-configuratie:

  - De toepassingsclients moeten zich toegang tot de toepassing verschaffen met een Fully Qualified Domain Name (FQDN) in de aanmeldings-URL, bijvoorbeeld: http://myserver.**bedrijfsdomein**.com/WebApp.
  - LW-SSO ondersteunt geen URL's met een IP-adres, bijvoorbeeld: http://192.168.12.13/WebApp.
  - LW-SSO ondersteunt geen URL's zonder een domein, bijvoorbeeld: http://myserver/WebApp.

  Indien geen domein wordt opgegeven in de LW-SSO-configuratie: de client krijgt toegang tot de toepassing zonder een FQDN in de aanmeldings-URL. In dit geval wordt specifiek voor één machine zonder domeininformatie een LW-SSO-sessiecookie gemaakt. Daarom wordt de cookie niet van de ene browser aan de andere overgedragen en wordt hij niet doorgegeven aan andere computers in hetzelfde DNS-domein. Dat betekent dat LW-SSO niet in hetzelfde domein werkt.

- **LW-SSO-frameworkintegratie.** De toepassingen kunnen alleen gebruik maken van LW-SSO-functies indien ze vooraf in het LW-SSO-framework werden geïntegreerd.

- **Ondersteuning van meerdere domeinen**.
  - Ondersteuning van meerdere domeinen is gebaseerd op de HTTP-referrer. Daarom ondersteunt LW-SSO koppelingen van één toepassing naar de andere en wordt het intikken van een URL in een browservenster niet ondersteund, tenzij beide toepassingen zich in hetzelfde domein bevinden.
  - De eerste koppeling over domeinen heen die **HTTP-POST** gebruikt, wordt niet ondersteund.

    De functionaliteit voor meerdere domeinen ondersteunt het eerste **HTTP POST**-verzoek aan een tweede toepassing niet (enkel het verzoek **HTTP GET** wordt ondersteund). Indien uw toepassing bijvoorbeeld een HTTP-koppeling met een tweede toepassing heeft, wordt een **HTTP GET**-verzoek ondersteund, maar wordt een **HTTP FORM**-verzoek niet ondersteund. Alle verzoeken na de eerste kunnen ofwel **HTTP POST** ofwel **HTTP GET** zijn.
  - Grootte van het LW-SSO-token

    De grootte van de informatie die LW-SSO kan doorgeven van een toepassing in één bepaald domein naar een andere toepassing in een ander domein, is beperkt tot 15 groepen/rollen/attributen (let op, elk item kan gemiddeld 15 tekens lang zijn).
  - Koppelingen van beveiligd (HTTPS) naar niet-beveiligd (HTTP) in een scenario met meerdere domeinen:

    Functionaliteit van meerdere domeinen werkt niet wanneer u koppelt van een beveiligde (HTTPS) naar een niet-beveiligde (HTTP) pagina. Dit is een browserbeperking waarbij de koptekst van de verwijzende site niet wordt verzonden wanneer wordt gekoppeld van een beveiligde naar een niet-beveiligde bron. Raadpleeg http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP voor een voorbeeld.

- **SAML2-token.**
  - De afmeldingsfunctionaliteit wordt niet ondersteund wanneer het SAML2-token wordt gebruikt.

    Indien het SAML2-token dus wordt gebruikt om toegang te krijgen tot een tweede toepassing, wordt een gebruiker die zichzelf uit de eerste toepassing afmeldt, niet uit de tweede toepassing afgemeld.
  - De verlooptijd van het SAML2-token wordt niet weergegeven in het sessiebeheer van de toepassing.

    Als het SAML2-token gebruikt wordt om toegang te krijgen tot een tweede toepassing, wordt het sessiebeheer van elke toepassing dus onafhankelijk verwerkt.
- **JAAS Realm.** De JAAS Realm in Tomcat wordt niet ondersteund.
- **Gebruik van spaties in Tomcat-mappen.** Het gebruik van spaties in Tomcat-mappen wordt niet ondersteund.

  Het is niet mogelijk om LW-SSO te gebruiken wanneer een Tomcat-installatiepad (mappen) spaties bevat (bv. Program Files) en het LW-SSO-configuratiebestand zich in de Tomcat-map **common\classes** bevindt.
- **Configuratie van de netwerktaakverdeling.** De netwerktaakverdeling gebruikt bij LW-SSO moet zo zijn geconfigureerd, dat "sticky sessions" kunnen worden gebruikt.

5

Verificatie van de Identity Manager

In dit hoofdstuk vindt u:

Verificatie van de Identity Manager accepteren

Indien u een Identity Manager gebruikt en u bent van plan om HP Universal CMDB Configuration Manager toe te voegen, dan moet u deze taak uitvoeren.

In deze taak wordt beschreven hoe u HP Universal CMDB Configuration Manager zo configureert, dat hij de Identity Manager-verificatie accepteert.

Deze taak omvat de onderstaande stappen:

Vereisten

De Configuration Manager Tomcat-server moet een verbinding hebben met uw webserver (IIS of Apache), beschermd door uw Identity manager via een Tomcat Java (AJP13)-connector.

Voor instructies voor het gebruik van een Tomcat Java (AJP13)-connector raadpleegt u de documentatie van Tomcat Java (AJP13).

HP Universal CMDB Configuration Manager zo configureren dat Identity Manager wordt geaccepteerd

Om Tomcat Java (AJP13) met IIS6 te accepteren:

1. Configureer Identity Manager zo, dat een gepersonaliseerde koptekst / terugbeloproep wordt verzonden die de gebruikersnaam bevat, en vraag de naam van de koptekst.
2. Open het bestand <**Configuration Manager-installatiemap**>**conf****lwssofmconf.xml** en zoek het gedeelte dat begint met **in-ui-identity-management**.

   Bijvoorbeeld:

   ```
   <in-ui-identity-management enabled="false">
       <identity-management>
         <userNameHeaderName>sm-user</userNameHeaderName>
       </identity-management>
   </in-ui-identity-management>
   ```

   a. Activeer de functie door het opmerkingenteken te verwijderen.

   b. Vervang **enabled**="**false**" door **enabled**="**true**".

   c. Vervang **sm-user** door de koptekst die u hebt aangevraagd in stap 1.
3. Open het bestand <**Configuration Manager-installatiemap**>**conf****client-config.properties** en bewerk de volgende eigenschappen:

   a. Wijzig **bsf.server.url** in de URL van de Identity Manager en wijzig de poort in de poort van de Identity Manager:

   ```
   bsf.server.url=http://< URL van Identity Manager>:< poort van Identity Manager >/bsf
   ```

   b. Wijzig **bsf.server.services.url** in het HTTP-protocol en wijzig de poort in de oorspronkelijke Configuration Manager-poort:

   ```
   bsf.server.services.url=http://<Configuration Manager-URL>:< Configuration Manager-poort>/bsf
   ```

Voorbeeld van het gebruik van Java Connector om Identity Management voor Configuration Manager te configureren met IIS6 op het besturingssysteem Windows 2003

In deze voorbeeldtaak wordt beschreven hoe Java Connector zo kan worden geïnstalleerd en geconfigureerd, dat Identity Management kan worden geconfigureerd voor gebruik met Configuration Manager met IIS6 uitgevoerd op het besturingssysteem Windows 2003.

Om Java Connector te installeren en het te configureren voor IIS6 op een Windows 2003:

1. Download de recentste versie van Java Connector (bijvoorbeeld **djk-1.2.21**) van de Apache-website.
   a. Klik **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.
   b. Selecteer de recentste versie.
   c. Download het bestand **isapi_redirect.dll** uit de map **amd64**.
2. Sla dit bestand op onder <**Configuration Manager-installatiemap**>**tomcat****bin****win32**.
3. Maak een nieuw tekstbestand met de naam **isapi_redirect.properties** in dezelfde map met isapi_redirect.dll.

   De inhoud van dit bestand is:

   ```
   # Configuration file for the Jakarta ISAPI Redirector

   # The path to the ISAPI Redirector Extension, relative to the website

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

   log_file=<Configuration Manager Install Directory>\servers\server-0\logs\isapi.log

   # Log level (debug, info, warn, error or trace)

   log_level=info
   ```

```
# Full path to the workers.properties file

worker_file==<Configuration Manager Install
Directory>\tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager Install
Directory>\tomcat\conf\uriworkermap.properties
```

4 Maak een nieuw tekstbestand met de naam **workers.properties.minimal** in <**Configuration Manager-installatiemap**>**tomcat****conf**.

De inhoud van dit bestand is:

```
# workers.properties.minimal -

#

# This file provides minimal jk configuration

# properties needed to

# connect to Tomcat.

#

# Defining a worker named ajp13w and of type ajp13

# Note that the name and the type do not have to

# match.

        worker.list=ajp13w

        worker.ajp13w.type=ajp13

        worker.ajp13w.host=localhost

        worker.ajp13w.port=8009

#END
```

5 Maak een nieuw tekstbestand met de naam **uriworkermap.properties** in <**Configuration Manager-installatiemap**>**tomcat****conf**.

De inhoud van dit bestand is:

```
# uriworkermap.properties - IIS

#
```

```
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Belangrijk: Let op, Configuration Manager moet twee regels bevatten. Met de nieuwe syntaxis kunnen die worden verenigd in één regel, zoals:

/cnc|/*=ajp13w

---

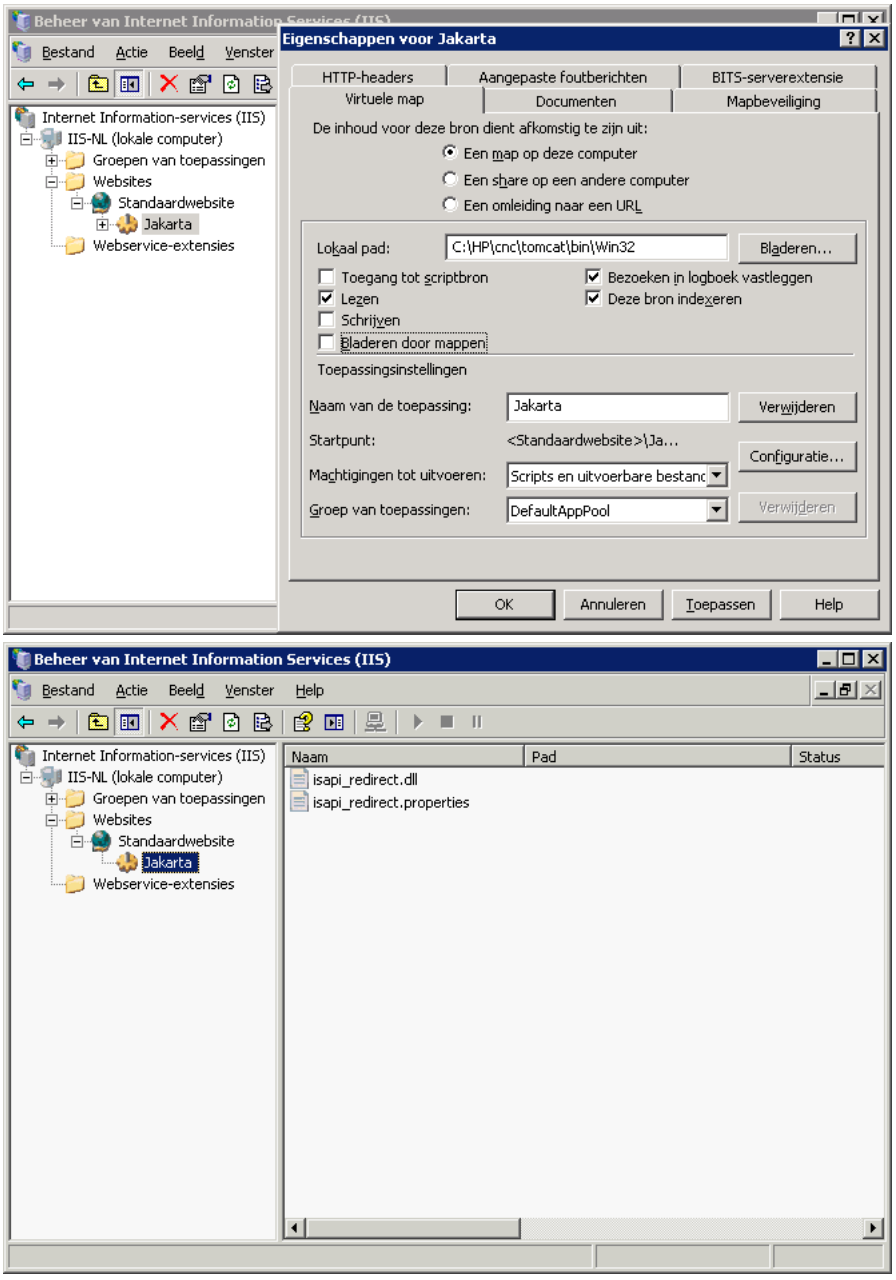
6 Maak de virtuele map in het overeenkomstige websiteobject in de IIS-configuratie.

a In het Start-menu van Windows opent u **Instellingen****Configuratiescherm****Systeembeheer****Internet Information Services (IIS)-beheermodule**.

b In het rechterdeelvenster klikt u met de rechtermuisknop op **<Plaatselijke computernaam>****Websites****<Naam van uw website>** en selecteert u **Nieuwe****Virtuele map**.

c Geef de map de aliasnaam **Jakarta** en stel het plaatselijke pad in op de map die isapi_redirect.dll bevat.

Het venster van de beheerder ziet er ongeveer zo uit:



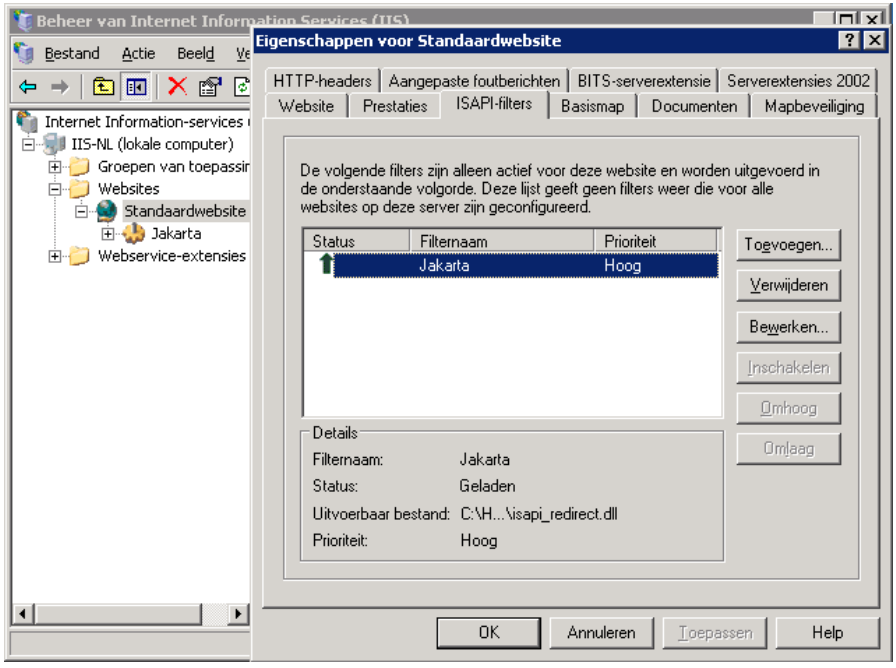
7 **Isapi_redirect.dll** toeveoegen als ISAPI-filter.

a Klik met de rechtermuisknop op **<Naam van uw website>** en selecteer **Eigenschappen**.

b Selecteer het tabblad **ISAPI-filters** en klik op de knop **Toevoegen…**.

c Selecteer de filternaam **Jakarta** en ga naar **isapi_redirect.dll**.
De filter wordt toegevoegd, maar is nog niet actief.

Het configuratievenster ziet er ongeveer zo uit:



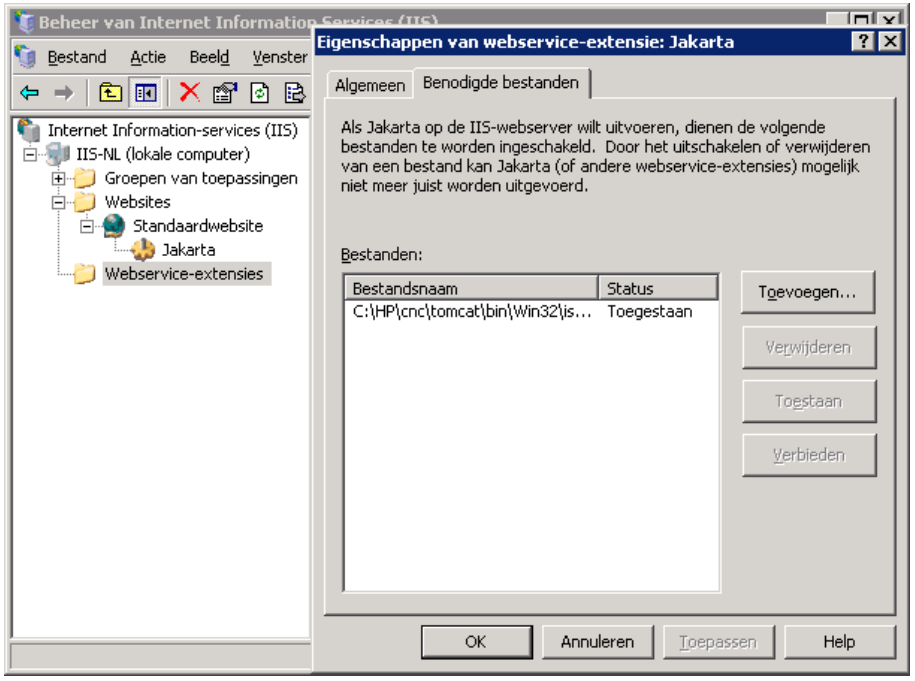
d Klik op de knop **Toepassen**.

8 Bepaal de webservice-extensie en sta die toe.

a Klik met de rechtermuisknop op **<Naam van de plaatselijke machine>\ Webservice-extensies** en selecteer het menu-item **Nieuwe webservice-extensie toevoegen…**.

b Noem de nieuwe webservice-extensie **Jakarta** en ga naar het bestand **isapi_redirect.dll**.

Let op: Voordat u op de knop **OK** klikt, moet u het selectievakje **Extensiestatus op toegestaan instellen** selecteren.



9 Start de IIS-webserver opnieuw op en ga naar de toepassing via de webservice.

6

Zich aanmelden bij Configuration Manager

Dit hoofdstuk omvat:

Configuration Manager openen

U opent Configuration Manager met behulp van een ondersteunde webbrowser, vanaf om het even welke computer met een netwerkverbinding (intranet of internet) met de Configuration Manager-server. Het toegangsniveau hangt af van de gebruikersmachtigingen. Voor meer informatie over het toestaan van gebruikersmachtigingen raadpleegt u "Gebruikersbeheer" in de *Configuration Manager-gebruikershandleiding* van *HP Universal CMDB*.

Raadpleeg "Systeemvereisten Configuration Manager" op pagina 8 voor meer informatie over de vereisten voor de browser en de minimumvereisten om Configuration Manager goed te kunnen bekijken.

Raadpleeg "Beveiliging" op pagina 75 voor meer informatie over het openen van Configuration Manager.

Toegang tot Configuration Manager

In de webbrowser voert u de URL in van de Configuration Manager-server, bijvoorbeeld: **http://<servernaam of IP-adres>.<domeinnaam>:<poort>** waarbij**<servernaam of IP-adres>.<domeinnaam>** staat voor de geldige domeinnaam (FQDN) van de Configuration Manager-server en **<poort>** voor de poort die tijdens de installatie wordt geselecteerd.

Zich aanmelden bij Configuration Manager

1. Voer de gebruikersnaam en het wachtwoord in dat u in de wizard voor voltooiing van de installatie van Configuration Manager hebt ingevoerd.
2. Klik op **Login**. Na het aanmelden verschijnt de gebruikersnaam in de rechterbovenhoek van het scherm.
3. (Aanbevolen) Maak verbinding met de LDAP-organisatieserver en wijs administratieve rollen toe aan LDAP-gebruikers om het voor Configuration Manager-beheerder mogelijk te maken om toegang te krijgen tot het systeem. Voor meer informatie over de toewijzing van rollen in het Configuration Manager-systeem raadpleegt u "Gebruikersbeheer" in de *Configuration Manager-gebruikershandleiding* van *HP Universal CMDB*.

Zich afmelden

Wanneer u uw sessie hebt voltooid, is het aan te bevelen dat u zich bij de website afmeldt, om toegang door onbevoegden te voorkomen.

Om u af te melden:

Klik op **Afmelden** bovenaan op de pagina.

Let op: De standaardtijd voordat de sessie verstrijkt, is 30 minuten.

Toegang tot de JMX-console voor Configuration Manager

Het is mogelijk dat u de JMX-console moet gebruiken om problemen op te lossen of om bepaalde configuraties aan te passen.

Om toegang te krijgen tot de JMX-console:

1. Open de JMX-console op http://<servernaam of IP-adres>:<poort>/cnc/jmx-console. De poort is de poort die werd geconfigureerd tijdens de installatie van Configuration Manager.
2. Voer de standaardaanmeldingsgegevens in. Die zijn dezelfde als de gebruikersgegevens om u aan te melden bij Configuration Manager.

Probleemoplossing en beperkingen

Probleem. Na het wijzigen van de configuratieset in Serverbeheer start de server niet op.

Oplossing. Keer terug naar de vorige configuratieset. Ga als volgt te werk:

1. Voer de volgende opdracht uit om de ID van de laatst geactiveerde configuratieset te zoeken:

   ```
   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <database-eigenschappen> --history
   ```

   waarbij <**database-eigenschappen**> kan worden bepaald door te verwijzen naar de plaats van het bestand <**Configuration Manager-installatiemap**>**\conf\database.properties** of door iedere database-eigenschap op te geven. Bijvoorbeeld:

   ```
   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p
   ..\conf\database.properties --history
   ```

2 Voer de volgende opdracht uit om de laatste configuratieset te exporteren:

```
< HP Universal CMDB Configuration Manager>\bin\export-cs.bat
<database-eigenschappen > <configuratie-set-ID> <naam dumpbestand>
```

waarbij <**configuratie-set-ID**> de configuratie-set-ID uit de vorige stap is en <**dumpbestand**> de naam is van een tijdelijk bestand dat wordt gebruikt om de configuratieset op te slaan. Om bijvoorbeeld een configuratieset met ID **491520** te exporteren naar het bestand **mydump.zip**, voert u het volgende in:

```
cd <Plaats van HP Universal CMDB Configuration-installatie>\bin export-
cs.bat -p ..\conf\database.properties --history
```

3 Zet de HP Universal CMDB Configuration Manager-service stil.

4 Voer de volgende opdracht uit om de vorige configuratieset te importeren en te activeren:

```
< HP Universal CMDB Configuration Manager>\bin\export-cs.bat
<database-eigenschappen > <naam dumpbestand> --activate
```

Probleem. Er is een fout in de UCMDB-verbinding.

Oplossing. Een van de volgende is mogelijk de oorzaak:

- De UCMDB-server is uitgevallen. Start Configuration Manager opnieuw op nadat UCMDB weer helemaal herstel is (controleer of de status van de UCMDB-server wel degelijk **Up** is).
- De UCMDB-server is actief, maar de aanmeldingsgegevens voor de verbinding met Configuration Manager of de URL is verkeerd. Start Configuration Manager op. Ga naar Serverbeheer, wijzig de instellingen van de verbinding met UCMDB en sla de nieuwe configuratieset op. Activeer de configuratieset en start de server opnieuw op.

Probleem. De instellingen van de LDAP-verbinding zijn fout.

Oplossing. Keer terug naar de vorige configuratieset. Stel de juiste instellingen voor de LDAP-verbinding in en activeer de nieuwe configuratieset.

Probleem. Wijzigingen aan het UCMDB-klassemodel worden niet gedetecteerd in Configuration Manager.

Oplossing. Start de Configuration Manager-server opnieuw op.

Probleem. Het Configuration Manager-logboek bevat een fout **UCMDB Er heeft zich een time-out voorgedaan bij de uitvoering**.

Oplossing. Dit gebeurt wanneer de UCMDB-database overbelast is. Om dit te corrigeren, kunt u de time-out van de verbinding als volgt verhogen:

1. Maak een bestand jdbc.properties aan binnen de map **UCMDBServer\conf**.
2. Voer de volgende tekst in: QueryTimeout=<aantal in seconden>.
3. Start de UCMDB-server opnieuw op.

Probleem. In Configuration Manager kunt u geen weergave toevoegen om te beheren.

Oplossing. Wanneer een weergave wordt toegevoegd om te beheren, wordt een nieuwe TQL aangemaakt in UCMDB. Indien de maximumlimiet actieve TQL's bereikt is, kan de weergave niet worden weergegeven. Verhoog de limiet van actieve TQL's in UCMDB door de volgende instellingen te wijzigen in Infrastructuurinstellingenbeheer.

- Maximumaantal actieve TQL's in server
- Maximumaantal actieve TQL's klant

Probleem. Het HTTPS-servercertificaat is niet geldig.

Oplossing. Een van de volgende is mogelijk de oorzaak:

- De geldigheidsdatum van het certificaat is verstreken. U moet een nieuw certificaat hebben.
- De certificeringsinstantie op het certificaat is geen vertrouwde instantie. Voeg de certificeringsinstantie toe aan uw lijst van vertrouwde basiscertificeringsinstanties.

Probleem. Wanneer u zich aanmeldt vanaf de aanmeldingspagina van Configuration Manager, krijgt u een aanmeldingsfout of wordt u de toegang ontzegd.

Oplossing. Een van de volgende is mogelijk de oorzaak:

- De gebruikersnaam is misschien niet bepaald in de verificatieprovider (externe/gedeelde LDAP). Voeg de gebruiker toe in het systeem van verificatieproviders.
- De gebruiker is gedefinieerd, maar heeft geen aanmeldingsmachtiging voor Configuration Manager. Geef de gebruiker een aanmeldingsmachtiging. Het is aangewezen om een aanmeldingsmachtiging te geven aan de basisgroep van alle Configuration Manager-gebruikers.
- Deze oplossingen zijn ook van toepassing wanneer de aanmelding mislukt wanneer u zich aanmeldt via een IDM-systeem.

Probleem. De Configuration Manager-server start niet, omdat foutieve databaseaanmeldingsgegevens werden ingevoerd.

Oplossing. Indien u de databaseaanmeldingsgegevens hebt gewijzigd en de server start niet, is het mogelijk dat de aanmeldingsgegevens fout zijn. (**Opmerking**: de wizard voor voltooiing van de installatie test de ingevoerde aanmeldingsgegevens niet automatisch. U moet op de knop **Testen** in de wizard klikken.) U moet het databasewachtwoord opnieuw coderen en nieuwe aanmeldingsgegevens invoeren in het configuratiebestand.

1. Vanaf een opdrachtregel voert u de volgende opdracht uit om het bijgewerkte databasewachtwoord te coderen:

   <Configuration Manager (CnC)-installatiemap>\bin\encrypt-password.bat –p <wachtwoord>

   waarbij het resultaat een gecodeerd wachtwoord is.

2. Kopieer het gecodeerde wachtwoord (met inbegrip van het voorvoegsel {ENCRYPTED} in de parameter **db.password** in <**CnC-installatiemap**>**conf****database.properties**.

Probleem. Indien de DNS niet juist is geconfigureerd, is het mogelijk dat u zich met het server-IP-adres moet aanmelden. Wanneer u het IP-adres invoert, doet zich een tweede DNS-fout voor.

Oplossing. Vervang de machinenaam opnieuw door het IP-adres. Bijvoorbeeld:

Indien u zich aanmeldt met het volgende IP-adres:
http://16.55.245.240:8180/cnc/

en u krijgt een adres met de machinenaam waarbij een DNS-fout wordt aangegeven, zoals:
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

kunt u dit vervangen door:
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

en kunt u de toepassing opnieuw opstarten in de browser.

Probleem. De Configuration Manager tomcat-server start niet.

Oplossing. Probeer een van de volgende mogelijkheden:

- Voer de wizard voor voltooiing van de installatie uit en vervang de serverpoorten van Configuration Manager
- Breek het andere proces af dat de Configuration Manager-poorten bezet.
- Wijzig de poorten in de configuratiebestanden van Configuration Manager handmatig door het volgende bestand te bewerken: **<CnC-installatiemap>\servers\server-0\conf\server.xml** en de relevante poorten bij te werken:
  - HTTP (8080): regel 69
  - HTTPS (8443): regels 71, 90

Probleem. Er heeft zich een geheugenprobleem voorgedaan in het logboekbestand van Configuration Manager.

Oplossing. Verhoog het maximale Java-geheugen naar behoefte.

Om de grootte van het geheugen in de Configuration Manager-service te wijzigen:

1. Ga naar de map <**CnC-installatiemap**>**cnc****bin** en voer de volgende opdracht uit: edit-server-0.bat.
2. Selecteer het tabblad **Java**.
3. Werk de parameters **Initiële geheugengroep** en **Maximale geheugengroep** bij.

Om de grootte van het geheugen in het batchbestand te wijzigen:

1. Ga naar de map <**CnC-installatiemap**>**cnc** en open het bestand **start-server-0.bat** om het te bewerken.
2. Zoek de regel die begint met **SET JAVA_OPTS=-Dcnc.home**.
3. Zoek de opdrachten **-Xms** and **-Xmx** en wijzig ze volgens uw behoeften.

   -Xms<grootte initiële geheugengroep> -Xmx<maximale grootte geheugengroep>

   Bijvoorbeeld: om de initiële geheugengroep in te stellen op 100 MB en de maximale geheugengroep in te stellen als 800 MB, voert u het volgende in:

   -Xms100m -Xmx800m

Probleem. De wizard voor voltooiiing van de installaties doet er lang over nadat u op **Voltooien** hebt geklikt.

Oplossing. Voor een UCMDB-systeem dat niet vooraf werd geconfigureerd voor de geconsolideerde modus, is het mogelijk dat de bewerking voor consolidering van het schema lang duurt (afhankelijk van de hoeveelheid gegevens). Wacht een kwartier. Indien u geen vooruitgang ziet, breekt u de wizard voor voltooiing van de installatie af en start u het proces opnieuw op.

Probleem. Wijzigingen van CI's in UCMDB zijn niet zichtbaar in Configuration Manager.

Oplossing. Configuration Manager maakt gebruik van een offline, asynchroon analyseproces. Het proces heeft mogelijk nog niet de meest recente wijzigingen in UCMDB verwerkt. Om dit op te lossen, kunt u het volgende proberen:

- Wacht enkele minuten. Het standaardinterval tussen uitvoeringen van het analyseproces is 10 minuten; deze waarde kunt u instellen in de module Serverbeheer.
- Voer een JMX-aanroep uit om de offline analysebewerking op de betreffende weergave uit te voeren.
- Ga naar Beleidsregelbeheer en klik op de knop **Beleidsanalyse herberekenen**. Dit roept het offline analyseproces aan voor alle weergaven (dit kan enige tijd duren). Breng eventueel handmatig een wijziging aan in een beleidsregel en sla deze wijziging op.

Probleem. Als u klikt op **Beheer** > **UCMDB openen** wordt de aanmeldingspagina van UCMDB geopend.

Oplossing. Om opnieuw toegang te krijgen tot UCMDB zonder u opnieuw aan te melden, moet u single sign-on inschakelen. Raadpleeg "Lightweight Single Sign-On inschakelen" op pagina 20 voor meer informatie. Daarnaast moet u zeker zijn dat de aangemelde Configuration Manager-gebruiker vermeld wordt in het gebruikersbeheersysteem van UCMDB.

Probleem. Wanneer een UCMDB-verbinding in de wizard voor voltooiing van installatie wordt geconfigureerd voor een IPv6-adres, werkt het menu-item **Beheer** > **UCMDB openen** niet.

Oplossing. Ga als volgt te werk:

1. Ga naar **Beheer** > **Serverbeheer** > **Configuration Manager** > **UCMDB-verbinding**.
2. Voeg vierkante haken aan het IP-adres toe in de URL van UCMDB-toegang. De URL moet er ongeveer zo uitzien: http://[x:x:x:x:x:x:x:x]:8080/.
3. Sla de configuratieset op en activeer hem.
4. Start Configuration Manager opnieuw op.

Als u werkt met Configuration Manager, gelden de volgende beperkingen:

- Elke keer als de tijd wordt gewijzigd op de tomcat-server van Configuration Manager, moet de server opnieuw worden opgestart om de tijd op de server bij te werken.

7

Beveiliging

In dit hoofdstuk vindt u:

Beveiliging Configuration Manager

In dit gedeelte wordt het concept van een beveiligde Configuration Manager-toepassing uitgelegd en wordt besproken welke planning en architectuur nodig zijn om beveiliging te implementeren. Het is ten sterkste aanbevolen dat u dit gedeelte leest voordat u doorgaat naar de bespreking van de beveiliging in de volgende gedeelten.

Configuration Manager is zo ontworpen, dat het deel kan uitmaken van een beveiligde architectuur. Daarom is het geschikt om het hoofd te bieden aan de beveiligingsproblemen waaraan het kan worden blootgesteld.

In de beveiligingsrichtlijnen wordt de configuratie besproken die vereist is om een Configuration Manager met meer beveiliging te implementeren.

De opgegeven beveiligingsinformatie is vooral bedoeld voor Configuration Manager-beheerders die zich vertrouwd moeten maken met de beveiligingsinstellingen en de aanbevelingen voordat ze met de beveiligingsprocedures starten.

Dit zijn de aanbevolen voorbereidingen om uw systeem te beveiligen:

- Evalueer de beveiligingsrisico's en de beveiligingsstatus van uw algemene netwerk en gebruik de conclusies om te beslissen hoe u Configuration Manager best in uw netwerk integreert.
- Ontwikkel een goed begrip van het technische framework van Configuration Manager en de beveiligingsmogelijkheden van Configuration Manager.
- Lees alle richtlijnen rond beveiliging na.
- Controleer of Configuration Manager volledig werkt voordat u met de beveiligingsprocedures start.
- Volg de stappen voor de beveiligingsprocedure chronologisch in elk gedeelte.

Belangrijk:

- De beveiligingsprocedures zijn gebaseerd op de veronderstelling dat u enkel de instructies implementeert die in die gedeelten worden doorgegeven en dat u geen andere beveiligingsstappen uitvoert die u ergens anders vindt.
- Waar de beveiligingsprocedures gericht zijn op een bepaalde gedistribueerde architectuur, betekent dat niet dat dat de beste architectuur is voor de behoeften van uw organisatie.
- Er wordt verondersteld dat de procedures in de volgende gedeelten moeten worden uitgevoerd op machines die toegewezen zijn aan Configuration Manager. Als u de machines voor andere doeleinden gebruikt naast Configuration Manager, kan dat tot problematische resultaten leiden.
- De beveiligingsinformatie in dit gedeelte is niet bedoeld als leidraad tot beoordeling van de beveiligingsrisico's voor uw gecomputeriseerde systemen.

Codeer het wachtwoord van de database

Het databasewachtwoord wordt opgeslagen in het bestand **<Configuration Manager-installatiemap>\conf\database.properties**. Als u het wachtwoord wilt coderen, voldoet onze standaardcodering met de normen van FIPS 140-2. Om het databasewachtwoord te coderen, selecteert u het selectievakje **Wachtwoord coderen** op de pagina Databaseconfiguratie van de wizard bij voltooiing van installatie van Configuration Manager.

De codering wordt verwezenlijkt met behulp van een sleutel, waarmee het wachtwoord wordt gecodeerd. De sleutel zelf wordt vervolgens gecodeerd met een andere sleutel, de zogenaamde hoofdsleutel. Beide sleutels worden gecodeerd met hetzelfde algoritme. Meer informatie over de parameters die in het coderingsproces worden gebruikt, vindt u in "Coderingsparameters" op pagina 86.

Caution: Indien u het coderingsalgoritme wijzigt, worden alle eerder gecodeerde wachtwoorden niet langer bruikbaar.

Om de codering van uw databasewachtwoord te wijzigen:

1. Open het bestand <**Configuration Manager-installatiemap**>**conf****encryption.properties** en bewerk de volgende velden:
   - **engineName.** Voer de naam van het coderingsalgoritme in.
   - **keySize.** Voer de grootte van de hoofdsleutel in voor het geselecteerde algoritme.
2. Voer het script **generate-keys.bat** uit, waarmee u de volgende map aanmaakt: **cnc****security****encrypt_repository** en waarmee de coderingssleutel wordt aangemaakt.
3. Voer de wizard Na installatie opnieuw uit.

SSL op de servermachine inschakelen met een zelfondertekend certificaat

In deze gedeelten wordt uitgelegd hoe u Configuration Manager zo configureert, dat verificatie en codering worden ondersteund met behulp van het Secure Sockets Layer (SSL)-kanaal.

Configuration Manager gebruikt Tomcat 6.0 als toepassingsserver.

Let op: Alle plaatsen van mappen en bestanden hangen af van uw specifieke platform, uw besturingssysteem en uw installatievoorkeuren.

---

1 Vereisten

Voordat u met de volgende procedure start, verwijdert u het oude bestand **tomcat.keystore** in <**Configuration Manager-installatiemap**>**\java\lib\security\tomcat.keystore**.

2 Genereer een server-keystore

Maak een keystore (type JKS) met een zelfondertekend certificaat en een bijbehorende persoonlijke sleutel:

➤ Vanuit de bin-map van de Java-installatie in <**Configuration Manager-installatiemap**> voert u de volgende opdracht uit:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore
..\lib\security\tomcat.keystore
```

Het dialoogvenster van de console wordt geopend.

➤ Voer het wachtwoord van de keystore in. Indien het wachtwoord gewijzigd is, moet u het handmatig in het bestand wijzigen.

➤ Beantwoord de vraag **Wat is uw voor- en achternaam?** Voer de naam van de Configuration Manager-webserver in. Voer de andere parameters in volgens uw organisatie.

➤ Voer een sleutelwachtwoord in. Het sleutelwachtwoord MOET hetzelfde zijn als het keystore-wachtwoord.

Er wordt een JKS-keystore gemaakt met de naam **tomcat.keystore** met een servercertificaat met de naam **hpcert**.

3 Plaats het certificaat in de vertrouwde gegevensopslag van de client

Na het genereren van **tomcat.keystore** en het exporteren van het servercertificaat moet u dit certificaat voor elke client die via SLL met dit zelfondertekende certificaat met Configuration Manager moet kunnen communiceren in de vertrouwde gegevensopslag van die client plaatsen.

Beperking: er kan slechts één servercertificaat in **tomcat.keystore** staan.

---

4 Controleer de configuratie-instellingen van de client

Open het bestand **client-config.properties** dat zich in de map **conf** van de <**Configuration Manager-installatiemap**> bevindt. Stel het protocol in op **https** en de poort op **8443**.

5 Wijzig het bestand server.xml

Open het bestand **server.xml** in de map **conf** van de <**Configuration Manager-installatiemap**>.
Zoek het gedeelte dat begint met

Connector port="8443"

dat in de opmerkingen vermeld staat. Activeer het script door het opmerkingenteken te verwijderen en voeg de volgende twee regels toe:

keystoreFile="<bestandslocatie tomcat.keystore>" (zie stap 2 op pagina 79)

keystorePass="<password>"

6 Start de server opnieuw

7 Controleer de beveiliging van de server

Om te controleren of de Configuration Manager-server beveiligd is, voert u de volgende URL in in uw webbrowser:
https://<Configuration Manager Servernaam of IP-adres>:8443/cnc.

Tip: Indien u geen verbinding kunt maken, kunt u een andere browser gebruiken of naar een nieuwere versie van de browser upgraden.

SSL inschakelen op de servermachine met een certificaat van een certificeringsinstantie

Om een certificaat te gebruiken dat wordt uitgegeven door een certificeringsinstantie, moet de keystore in Java-formaat zijn. In het volgende voorbeeld wordt uitgelegd hoe u de keystore voor een Windows-machine kunt formatteren.

1 Vereisten

Voordat u met de volgende procedure start, verwijdert u het oude bestand **tomcat.keystore** in <**Configuration Manager-installatiemap**>**java****lib****security****tomcat.keystore**.

2 Genereer een server-keystore

a Genereer een certificaat getekend door een certificeringsinstantie en installeer het op Windows.

b Exporteer het exporteren naar een ***.pfc**-bestand (met inbegrip van persoonlijke sleutels) met behulp van Microsoft Management Console (**mmc.exe**).

➤ Voer een willekeurige tekenreeks in als wachtwoord voor het **pfx**-bestand. (U hebt dit wachtwoord gevraagd toen u het keystore-type converteerde naar een JAVA-keystore.)
Het **.pfx**-bestand bevat nu een publiek certificaat en een persoonlijke sleutel en is beveiligd met een wachtwoord.

c Kopieer het **.pfx**-bestand dat u hebt gemaakt naar de volgende map: <**Configuration Manager-installatiemap**>**java****lib****security**.

d Open de opdrachtregel en wijzig de map naar <**Configuration Manager-installatiemap**>**bin****jre****bin**.

➤ Wijzig het keystore-type van **PKCS12** in een **JAVA**-keystore door de volgende opdracht uit te voeren:

```
keytool -importkeystore -srckeystore <Configuration Manager-installatiemap>\conf\security\<pfx-bestandsnaam> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

U hebt het keystore-wachtwoord van de bron (.**pfx**) aangevraagd. Dit is het wachtwoord dat u hebt aangevraagd toen u het pfx-bestand hebt gemaakt in stap b.

3 Controleer de configuratie-instellingen van de client

Open het volgende bestand: <**Configuration Manager-installatiemap**>**cnc****conf****client-config.properties** en controleer of de eigenschap **bsf.server.url** is ingesteld op **https** en de poort **8443** is.

4 Wijzig het bestand server.xml

Open het volgende bestand: <**Configuration Manager-installatiemap**>**conf****server.xml**. Zoek het gedeelte dat begint met

```
Connector port="8443"
```

dat in de opmerkingen vermeld staat. Activeer het script door het opmerkingenteken te verwijderen en voeg de volgende twee regels toe:

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

5 Start de server opnieuw

6 Controleer de beveiliging van de server

Om te controleren of de Configuration Manager-server beveiligd is, voert u de volgende URL in in uw webbrowser:
https://<Configuration Manager-servernaam of IP-adres>:8443/cnc.

Beperking: er kan slechts één servercertificaat in **tomcat.keystore** staan.

SSL inschakelen met een Client-certificaat

Indien het certificaat gebruikt door de Configuration Manager-webserver werd uitgegeven door een bekende certificeringsinstantie, is het zeer waarschijnlijk dat uw webbrowser het certificaat kan valideren zonder verdere acties.

Indien de certificeringsinstantie niet wordt vertrouwd door de vertrouwde gegevensopslag van de server, moet u het certificaat in de vertrouwde gegevensopslag van de server importeren.

In het volgende voorbeeld wordt getoond hoe het zelfondertekende **hpcert**-certificaat kan worden geïmporteerd in de vertrouwde gegevensopslag van de server (cacerts).

Om een certificaat te importeren in de vertrouwde gegevensopslag van de server:

1. Op de clientmachine zoekt u het **hpcert**-certificaat en u verandert de naam ervan in **hpcert.cer**.

   In Windows Explorer geeft het pictogram aan dat het bestand een veiligheidscertificaat is.

2. Dubbelklik op **hpcert.cer** om het dialoogvenster van de Explorer-certificaten te openen en importeer het bestand.

3. Op de servermachine importeert u het certificaat van de certificeringsinstantie in de vertrouwde gegevensopslag (cacerts) met behulp van het hulpprogramma voor sleutels, via de volgende opdracht:

   ```
   keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
   ```

4. Wijzig het bestand server.xml als volgt:

   a. Voer de wijzigingen door zoals beschreven in stap 5 op pagina 80.

   b. Onmiddellijk na deze wijzigingen voegt u de volgende regels toe:

   ```
   truststoreFile="../../java/lib/security/cacerts"
   truststorePass="changeit" />
   ```

   c. Stel clientAuth="true" in.

5. Controleer de serverbeveiliging zoals beschreven in stap 7 op pagina 80.

SLL inschakelen voor verificatie alleen

In deze taak wordt beschreven hoe u Configuration Manager zo configureert, dat enkel verificatie wordt ondersteund. Dat is het minimale beveiligingsniveau dat vereist is om met Configuration Manager te werken.

Om SLL in te schakelen voor verificatie:

1. Volg een van de procedures om SLL in te schakelen op de servermachine zoals beschreven in "SSL op de servermachine inschakelen met een zelfondertekend certificaat" op pagina 78 tot en met stap 6 op pagina 80 of "SSL inschakelen op de servermachine met een certificaat van een certificeringsinstantie" op pagina 81 tot en met stap 5 op pagina 82.
2. Voer de volgende URL in in de webbrowsers: **http://<Configuration Manager Servernaam of IP-adres>:8080/cnc**.

Clientcertificaatverificatie inschakelen

In deze taak wordt beschreven hoe u Configuration Manager zo instelt, dat certificaatverificatie langs de client wordt geaccepteerd.

Om Clientcertificaatverificatie in te schakelen:

1. Volg de procedure om SSL in te schakelen op de servermachine zoals beschreven in "SSL op de servermachine inschakelen met een zelfondertekend certificaat" op pagina 78.
2. Open het volgende bestand: **<Configuration Manager-installatiemap>\conf\lwssofmconf.xml.** Zoek het gedeelte dat begint met in-client certificate. Bijvoorbeeld:

   ```
   <in-clientCertificate userIdentifierRetrieveField="SubjectDN"
   userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
   ```

   Activeer de functie van het clientcertificaat door het opmerkingenteken te verwijderen.

3 Haal de gebruikersnaam uit het certificaat volgens de volgende procedure:

a De parameter **userIdentifierRetrieveField** geeft aan welk certificaatveld de gebruikersnaam bevat. De opties zijn:

- **SubjectDN**
- **SubjectAlternativeName**

b De parameter **userIdentifierRetrieveMode** geeft aan of de gebruikersnaam bestaat uit de volledige inhoud van het relevante veld of enkel een gedeelte ervan. De opties zijn:

- **EntireField**
- **FieldPart**

c Indien de waarde van **userIdentifierRetrieveMode FieldPart**, is, duidt de parameter **userIdentifierRetrieveFieldPart** aan welk deel van het relevante veld de gebruikersnaam is. De waarde is een codeletter gebaseerd op een legende gedefinieerd in het certificaat zelf.

4 Open het volgende bestand **<Configuration Manager-installatiemap>\conf\client-config.properties** en bewerk de volgende eigenschappen:

- Wijzig **bsf.server.url** zo, dat het HTTPS-protocol wordt gebruikt en wijzig de HTTPS-poort in de poort beschreven in "SSL op de servermachine inschakelen met een zelfondertekend certificaat" op pagina 78.
- Wijzig **bsf.server.services.url** zo, dat het HTTP-protocol wordt gebruikt en wijzig de poort in de oorspronkelijke HTTP-poort.

Coderingsparameters

In de volgende tabel staan de parameters opgesomd die in het bestand **encryption.properties** omvat zitten dat wordt gebruikt voor de databasewachtwoordcodering. Zie "Codeer het wachtwoord van de database" op pagina 77 voor meer informatie over de codering van het databasewachtwoord.

Parameter	Beschrijving
cryptoSource	Duidt de infrastructuur aan die het coderingsalgoritme implementeert. De beschikbare opties zijn: ➤ **lw.** Maakt gebruik van de lichte implementatie Bouncy Castle (standaardoptie) ➤ **jce.** Java Cryptography Enhancement (gebruikelijke Java-cryptografie-infrastructuur)
storageType	Duidt het type sleutelopslag aan. Momenteel wordt enkel **binair bestand** ondersteund.
binaryFileStorageName	Duidt aan op welke plaats in het bestand de hoofdsleutel opgeslagen is.
cipherType	Het type van de coderingsmethode. Momenteel wordt enkel **symmetricBlockCipher** ondersteund.
engineName	De naam van het coderingsalgoritme. De volgende opties zijn beschikbaar: ➤ **AES.** American Encryption Standard. Deze codering voldoet aan FIPS 140-2. (standaardoptie) ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (voldoet aan FIPS 140-2) ➤ **Null**. Geen codering

Parameter	Beschrijving
keySize	Het formaat van de hoofdsleutel. Het formaat wordt bepaald door het algoritme: ➤ **AES.** 128, 192 of 256 (standaardoptie is 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156
encodingMode	De ASCII-codering van de binaire coderingsresultaten. De volgende opties zijn beschikbaar: ➤ **Base64** (standaardoptie) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	De modus van het algoritme. Momenteel wordt alleen **CBC** ondersteund.
algorithmPaddingName	Het opvullingsalgoritme dat wordt gebruikt. De volgende opties zijn beschikbaar: ➤ **PKCS7Padding** (standaardoptie) ➤ **PKCS5Padding**
jceProviderName	De naam van het JCE-coderingsalgoritme. **Opmerking:** enkel relevant wanneer crytpSource **jce** is. Voor **lw** wordt engineName gebruikt.