HP Universal CMDB

Voor de besturingssystemen Windows en Red Hat Enterprise Linux

Softwareversie: 10.00

HP Universal CMDB en Configuration Manager beveiligen

Release-datum van document: Juni 2012

Release-datum van software: Juni 2012

Wettelijke kennisgevingen

Garantie

De enige garanties voor HP-producten en -services worden uiteengezet in de uitdrukkelijke garantieverklaringen die worden geleverd bij de betreffende producten en services. De inhoud van dit document kan op geen enkele wijze worden aangemerkt als een aanvullende garantie. HP is niet aansprakelijk voor technische of redactionele fouten in dit document.

De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd.

Legenda voor beperkte rechten

Vertrouwelijke computersoftware. Geldige licentie van HP vereist voor bezit, gebruik of kopieën. In overeenstemming met FAR 12.211 en 12.212 worden commerciële computersoftware, documentatie voor computersoftware en technische gegevens voor commerciële items in licentie gegeven aan de regering van de VS onder de commerciële standaardlicentie van de verkoper.

Copyright-kennisgeving

Handelsmerk-kennisgevingen

Adobe™ is een handelsmerk van Adobe Systems Incorporated.

Microsoft® en Windows® zijn gedeponeerde handelsmerken van Microsoft Corporation in de Verenigde Staten.

UNIX® is een geregistreerd handelsmerk van The Open Group.

Documentatie-updates

De titelpagina van dit document bevat de volgende identificatiegegevens:

- Versienummer van software, waarmee de softwareversie wordt aangegeven.
- Release-datum van document, die na elke update van het document wordt gewijzigd.
- Release-datum van software, waarmee de release-datum van deze versie van de software wordt aangegeven.

Als u wilt controleren of er recente updates beschikbaar zijn of wilt controleren of u de meest recente versie van een document gebruikt, gaat u naar:

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

Als u toegang wilt tot deze site, moet u zich aanmelden voor een HP Passport en zich aanmelden. Als u zich wilt aanmelden voor een HP Passport-ID, gaat u naar:

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

U kunt eventueel ook klikken op de koppeling **New users - please register** (Nieuwe gebruikers - Aanmelden) op de aanmeldingspagina voor HP Passport.

U ontvangt ook bijgewerkte of nieuwe versies als u zich abonneert op de ondersteuningsservice voor het desbetreffende product. Neem contact op met uw HP-vertegenwoordiger voor meer informatie.

Ondersteuning

Ga naar de website van HP Software Support Online op:

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

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

In de online ondersteuning van HP Software vindt u methoden waarmee klanten zelf problemen kunnen oplossen. Hiermee krijgt u snel en efficiënt toegang tot interactieve tools voor technische ondersteuning die u nodig hebt om uw bedrijf te kunnen beheren. Als gewaardeerde ondersteuningsklant kunt op de ondersteuningssite profiteren van de volgende mogelijkheden:

- Interessante kennisdocumenten zoeken
- Ondersteuningscases en verbeteringsaanvragen indienen en volgen
- Softwarepatches downloaden
- Ondersteuningscontracten beheren
- Contactpersonen van HP opzoeken voor ondersteuning
- Informatie over beschikbare services bekijken
- Discussies voeren met andere softwareklanten
- Softwaretrainingen bekijken en u hiervoor aanmelden

Voor de meeste ondersteuningssecties moet u zich registreren als HP Passport-gebruiker en u vervolgens aanmelden. Voor verschillende secties moet u verder beschikken over een ondersteuningscontract. Om u te registreren voor een HP Passport-ID, gaat u naar:

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

Als u meer informatie wilt over toegangsniveaus, gaat u naar:

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

Inhoud

Hoofdstuk 1

Inleiding tot beveiliging

In dit hoofdstuk vindt u de volgende informatie:

Beveiliging - overzicht

In dit gedeelte wordt het concept van een veilige HP Universal CMDB-applicatie geïntroduceerd en worden de benodigde planning en architectuur besproken voor het implementeren van beveiliging. U wordt ten zeerste aanbevolen dit gedeelte te lezen voordat u doorgaat naar de bespreking van de beveiliging in de volgende gedeelten.

HP Universal CMDB 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 HP Universal CMDB met meer beveiliging te implementeren.

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

Het wordt ten zeerste aangeraden om een reverse proxy te gebruiken in combinatie met HP Universal CMDB voor het bewerkstelligen van een veilige architectuur. Zie "Werken met een reverse proxy" op pagina 34 voor meer informatie over het configureren van een reverse proxy voor gebruik bij HP Universal CMDB.

Als u een ander type beveiligde architectuur bij HP Universal CMDB moet gebruiken dan in dit document wordt beschreven, moet u contact opnemen met HP Software Support om vast te stellen welke architectuur het beste is voor uw situatie.

Zie "Beveiliging Data Flow-probe" op pagina 63 voor meer informatie over beveiliging van de Data Flow-probe.

Opmerking:

- De beveiligingsprocedures zijn gebaseerd op de veronderstelling dat u enkel de instructies implementeert die in deze hoofdstukken worden verstrekt 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 vanuit gegaan dat de procedures in de volgende hoofdstukken worden uitgevoerd op machines die speciaal bedoeld zijn voor het werken met HP Universal CMDB. Het gebruik van deze machines voor andere doeleinden naast HP Universal CMDB, kan leiden tot problemen.
- De beveiligingsinformatie in dit gedeelte is niet bedoeld als leidraad tot beoordeling van de beveiligingsrisico's voor uw gecomputeriseerde systemen.

Voorbereidingen voor beveiliging

- Evalueer de beveiligingsrisico's en de beveiligingsstatus van uw algemene netwerk en gebruik de conclusies om te beslissen hoe u HP Universal CMDB best in uw netwerk integreert.
- Ontwikkel een goed begrip van het technische framework van HP Universal CMDB en de beveiligingsmogelijkheden van HP Universal CMDB.
- Lees alle richtlijnen rond beveiliging na.
- Controleer of HP Universal CMDB volledig werkt voordat u met de beveiligingsprocedures start.
- Volg de stappen voor de beveiligingsprocedure chronologisch in elk hoofdstuk. Als u bijvoorbeeld besluit om de HP Universal CMDB-server te configureren om SSL te ondersteunen, leest u"Secure Sockets Layer-communicatie (SSL) inschakelen" op pagina 18 en volgt u de instructies in chronologische volgorde.
- HP Universal CMDB ondersteunt geen basisverificatie met lege wachtwoorden. Gebruik geen leeg wachtwoord wanneer u verbindingsparameters voor basisverificatie instelt.

Tip: Druk de beveiligingsprocedures af en vink ze af terwijl u ze implementeert.

UCMDB implementeren in een beveiligde architectuur

Er worden verschillende maatregelen aanbevolen om uw HP Universal CMDB-servers veilig te implementeren:

- **DMZ-architectuur via een firewall**

  De beveiligde architectuur waarnaar in dit document wordt verwezen, is een typische DMZ-architectuur waarbij een apparaat wordt gebruikt als firewall. Het basisconcept van een dergelijke architectuur is om een volledige scheiding tot stand te brengen en rechtstreekse toegang tussen de HP Universal CMDB-clients en de HP Universal CMDB-server te vermijden.

- **Beveiligde browser**

  Internet Explorer en Firefox in een Windows-omgeving moeten worden geconfigureerd om Java-scripts, applets en cookies veilig te kunnen afhandelen.

- **SSL-communicatieprotocol**

  Secure Sockets Layer-protocol beveiligt de verbinding tussen de client en de server. URL's waarvoor een SSL-verbinding vereist is, gebruiken een veilige versie (HTTPS) van het Hypertext Transfer Protocol. Zie "Secure Sockets Layer-communicatie (SSL) inschakelen" op pagina 18 voor meer informatie over dit onderwerp.

- **Reverse proxy-architectuur**

  Een van de meest veilige en aanbevolen oplossingen is de implementatie van HP Universal CMDB met behulp van een reverse proxy. HP Universal CMDB biedt volledige ondersteuning van veilige reverse proxy-architectuur. Zie "Werken met een reverse proxy" op pagina 34 voor meer informatie over dit onderwerp.

Systeemtoegang

Toegangsbeveiliging voor Java JMX

Opmerking: De procedure die hier wordt beschreven, kan ook worden gebruikt voor JMX van de Data Flow-probe.

Om ervoor te zorgen dat de RMI-poort van JMX alleen toegankelijk is na het opgeven van gebruikersreferenties, voert u de volgende procedure uit:

1. Geef in het bestand **wrapper.conf**, dat op de server te vinden is in **C:\hp\UCMDB\UCMDBServer\bin**, de volgende instellingen op:

   wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

   Met deze instelling moet JMX om verificatie vragen.

   - **Voor JMX van de Data Flow-probe** voert u de volgende stappen uit:

     Geef in de bestanden **WrapperGateway.conf** en **WrapperManager.conf**, die te vinden zijn in **C:\hp\UCMDB\DataFlowProbe\bin**, de volgende instellingen op:

     wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. Wijzig de naam van het bestand **jmxremote.password.template** (dat te vinden is in: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) in **jmxremote.password**.

> **Opmerking:** Voor JMX van de Data Flow-probe is dit bestand te vinden in: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. Voeg in **jmxremote.password** wachtwoorden toe voor de rollen **monitorRole** en **controlRole**.

   Bijvoorbeeld:

   monitorRole QED

   controlRole R&D

   zorgt ervoor dat het wachtwoord **QED** wordt toegewezen aan **monitorRole**, en het wachtwoord **R&D** aan **controlRole**.

   > **Opmerking:** Zorg dat alleen de eigenaar lees- en schrijfrechten heeft voor **jmxremote.password**, aangezien dit bestand de wachtwoorden in duidelijk herkenbare tekst bevat. De eigenaar van het bestand moet dezelfde gebruiker zijn waaronder de UCMDB-server wordt uitgevoerd.

4. In het bestand **jmxremote.access** (dat te vinden is in **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) wijst u toegang toe aan **monitorRole** en **controlRole**.

   Bijvoorbeeld:

   monitorRole readonly

   controlRole readwrite

   zorgt ervoor dat **monitorRole** alleen-lezen-toegang krijgt en **controlRole** lees- en schrijftoegang.

   > **Opmerking:** Voor JMX van de Data Flow-probe is dit bestand te vinden in: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Beveilig bestanden als volgt:

   - **Alleen voor Windows:** Voer vanaf de opdrachtregel de volgende opdrachten uit om bestanden te beveiligen:

     cacls jmxremote.password /P <gebruikersnaam>:F

     cacls jmxremote.access /P <gebruikersnaam>:R

     waarbij **<gebruikersnaam>** de bestandseigenaar is die zichtbaar is in de eigenschappen van beide bestanden. Open de eigenschappen van deze bestanden en controleer of ze correct zijn en slechts één eigenaar hebben.

   - **Voor de besturingssystemen Solaris en Linux:** Stel de bestandsrechten voor het wachtwoordbestand in door het volgende uit te voeren:

     chmod 600 jmxremote.password

6. **Voor upgrades van service packs, servermigraties en noodherstel:** Wijzig het eigendom

van het bestand **jmxremote.access** (dat te vinden is in **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) in de gebruiker van het besturingssysteem die de upgrade of migratie-installatie uitvoer.

Opmerking: Voor JMX van de Data Flow-probe is dit bestand te vinden in: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

Naam of wachtwoord systeemgebruiker voor de JMX-console wijzigen

De JMX-console gebruikt systeemgebruikers, dat wil zeggen, gebruikers bij verschillende klanten in een omgeving met meerdere klanten. U kunt u bij de JMX-console aanmelden met een willekeurige systeemgebruikersnaam. De standaardgebruikersnaam en het standaardwachtwoord zijn **sysadmin/sysadmin**.

U kunt het wachtwoord wijzigen via de JMX-console of via de tool Serverbeheer.

De standaardsysteemgebruikersnaam en het standaardwachtwoord wijzigen via de JMX-console:

1. Open een webbrowser en voer het volgende adres in: **http://localhost.<domeinnaam>:8080/jmx-console**.
2. Voer de aanmeldingsgegevens voor de verificatie in de JMX-console in. De standaardaanmeldingsgegevens zijn:
   - Aanmeldingsnaam = **sysadmin**
   - Wachtwoord = **sysadmin**
3. Zoek de **UCMDB:service=Authorization Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
4. Zoek naar de bewerking **resetPassword**.
   - Typ **sysadmin** in het veld **userName**.
   - Geef een nieuw wachtwoord op in het veld **password**.
5. Klik op **Aanroepen** om uw wijzigingen op te slaan.

De standaardsysteemgebruikersnaam en het standaardwachtwoord wijzigen via de tool Serverbeheer:

1. **Voor Windows:** voer het volgende bestand uit: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   Voor Linux: voer **server_management.sh** in de volgende map uit: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Meld u bij de tool aan met de referenties voor verificatie: **sysadmin/sysadmin**.
3. Klik op de koppeling Users.
4. Selecteer de systeemgebruiker en klik op **Wachtwoord wijzigen voor aangemelde**

gebruiker.

5. Voer het oude en het nieuwe wachtwoord in en klik op **OK**.

De gebruiker van de HP Universal CMDB-serverservice wijzigen

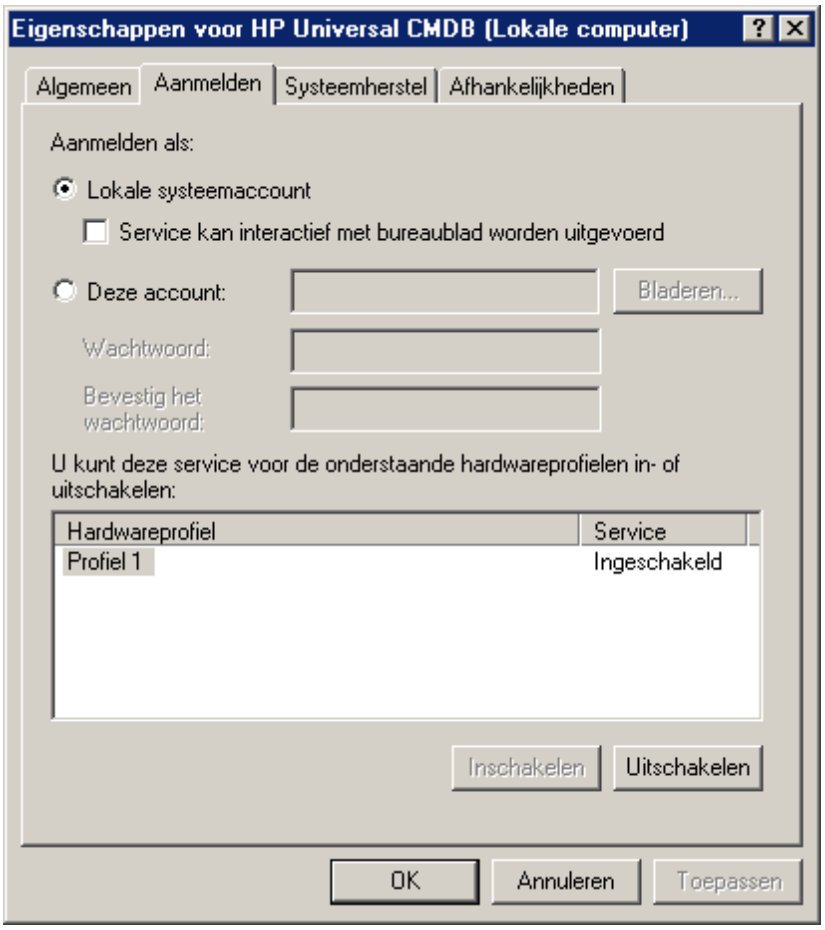
Op een Windows-platform wordt de HP Universal CMDB-service, die alle HP Universal CMDB-services en -processen uitvoert, geïnstalleerd wanneer u het hulpprogramma voor instelling en databaseconfiguratie uitvoert. Standaard wordt deze service uitgevoerd onder de local system-gebruiker. U moet echter mogelijk een andere gebruiker toewijzen om de service uit te voeren (bijvoorbeeld als u NTLM-verificatie gebruikt).

De gebruiker die u toewijst om de service uit te voeren, moet beschikken over de volgende rechten:

- Voldoende rechten voor de database (zoals gedefinieerd door de databasebeheerder).
- Voldoende rechten voor het netwerk.
- Beheerdersrechten op de lokale server.

De servicegebruiker wijzigen:

1. Schakel HP Universal CMDB uit via het menu Start (**Start > Alle programma's > HP UCMDB > HP Universal CMDB-server stoppen**) of door de HP Universal CMDB-serverservice te stoppen. Zie "De service HP Universal CMDB-server starten en stoppen" op pagina 1 voor meer informatie over dit onderwerp.
2. Dubbelklik in het venster **Services** van Windows op **UCMDB_Server**. Het dialoogvenster **Eigenschappen van UCMDB_Server (lokaal)** wordt geopend.
3. Klik op het tabblad Aanmelden.



4. Selecteer **Deze account** en kies een andere gebruiker in de lijst met geldige gebruikers op de machine.
5. Geef het Windows-wachtwoord van de geselecteerde gebruiker op en bevestig dit wachtwoord.
6. Klik op **Toepassen** om uw instellingen op te slaan en klik op **OK** om het dialoogvenster te sluiten.
7. Schakel HP Universal CMDB in via het menu Start (**Start > Alle programma's > HP UCMDB > HP Universal CMDB-server starten**) of door de HP Universal CMDB-serverservice te starten. Zie "De service HP Universal CMDB-server starten en stoppen" op pagina 1 voor meer informatie over dit onderwerp.

Het databasewachtwoord coderen voor Configuration Manager

Het CM-databasewachtwoord wordt opgeslagen in het bestand **<Configuration Manager-installatiemap>\conf\database.properties**. Als u het wachtwoord wilt coderen, voldoet ons standaard coderingsalgoritme aan de normen van FIPS 140-2.

De codering wordt uitgevoerd 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. Raadpleeg "Parameters voor codering van het databasewachtwoord voor Configuration Manager" beneden voor meer informatie over de parameters die voor het coderen worden gebruikt.

Let op: Als u het coderingsalgoritme wijzigt, kunnen alle eerder gecodeerde wachtwoorden niet meer worden gebruikt.

De codering van uw databasewachtwoord 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 voor het geselecteerde algoritme in.
2. Voer het script **generate-keys.bat** uit. Dit script maakt het volgende bestand: **<Configuration Manager-installatiemap>\security\encrypt_repository** en genereert de coderingssleutel.
3. Voer het hulpprogramma **bin\encrypt-password.bat** uit om het wachtwoord te coderen. Stel de vlag **-h** in om alle beschikbare opties te zien.
4. Kopieer het resultaat van het hulpprogramma voor wachtwoordcodering naar het bestand **conf\database.properties**.

Parameters voor codering van het databasewachtwoord voor Configuration Manager

In de onderstaande tabel vindt u de parameters die zijn opgenomen in het bestand **encryption.properties** dat voor de codering van het CM-databasewachtwoord wordt gebruikt. Zie "Het databasewachtwoord coderen voor Configuration Manager" op vorige pagina voor meer informatie over het coderen van het databasewachtwoord.

Parameter	Beschrijving
cryptoSource	De infrastructuur die het coderingsalgoritme implementeert. De beschikbare opties zijn: • **lw.** Maakt gebruik van de Bouncy Castle-Lightweight-implementatie (standaardoptie) • **jce.** Java Cryptography Enhancement (standaard Java-cryptografie-infrastructuur)
storageType	Het type sleutelopslag. Momenteel wordt uitsluitend **binair bestand** ondersteund.
binaryFileStorageName	De plaats in het bestand waar de hoofdsleutel is opgeslagen.
cipherType	Het type coderingsmethode. Momenteel wordt uitsluitend **symmetricBlockCipher** ondersteund.

Parameter	Beschrijving
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
keySize	De grootte van de hoofdsleutel. Deze grootte 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:** Alleen relevant indien crytpSource jce is. Voor lw wordt engineName gebruikt

Hoofdstuk 2

Secure Sockets Layer-communicatie (SSL) inschakelen

In dit hoofdstuk vindt u de volgende informatie:

SSL inschakelen op de servermachine met een zelfondertekend certificaat - UCMDB

In deze gedeelten wordt uitgelegd hoe u HP Universal CMDB configureert om communicatie met behulp van het Secure Sockets Layer (SSL)-kanaal te ondersteunen.

HP Universal CMDB gebruikt Jetty 6.1 als de standaardwebserver.

1. **Vereisten**

   a. Voordat u de volgende procedure start, verwijdert u eerst de oude keystore **server.keystore** in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

b. Plaats de HP Universal CMDB-keystore (JKS-type) in de map **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Genereer een server-keystore**

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

- Voer de volgende opdracht uit vanuit **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**:

  ```
  keytool -genkey -alias hpcert -keystore
  C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
  ```

  Het dialoogvenster van de console wordt geopend.

- Voer het keystore-wachtwoord in. Als het wachtwoord is gewijzigd, voert u de JMX-bewerking **changeKeystorePassword** uit in **UCMDB:service=Security Services**. Als het wachtwoord niet is gewijzigd, gebruikt u het standaardwachtwoord **hppass**.
- Beantwoord de vraag naar uw **voornaam en achternaam**. Voer de naam van de HP Universal CMDB-webserver in. Voer de overige parameters in op basis van uw organisatie.
- Voer een sleutelwachtwoord in. Het sleutelwachtwoord MOET hetzelfde zijn als het keystore-wachtwoord.

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

b. Exporteer het zelfondertekende certificaat naar een bestand.

Voer de volgende opdracht uit vanuit **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**:

```
keytool -export -alias hpcert -keystore
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass
<uw wachtwoord> -file hpcert
```

3. **Plaats het certificaat in de vertrouwde gegevensopslag van de client**

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

> **Opmerking:** Er kan slechts één servercertificaat in **server.keystore** staan.

4. **Schakel HTTP-poort 8080 uit**

Zie "HTTP/HTTPS-poort inschakelen of uitschakelen" op pagina 29 voor meer informatie over dit onderwerp.

> **Opmerking:** controleer of HTTPS-communicatie werkt voordat u de HTTP-poort sluit.

5. **Start de server opnieuw op**

6. **HP Universal CMDB weergeven**

Typ de volgende URL in de webbrowser om te controleren of de UCMDB-server beveiligd is: **https://<naam of IP-adres van UCMDB-server>:8443/ucmdb-ui**.

SSL inschakelen op de servermachine met een zelfondertekend certificaat - Configuration Manager

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

Configuration Manager gebruikt Tomcat 7.0.19 als applicatieserver.

Opmerking: De locaties van alle mappen en bestanden zijn afhankelijk van uw specifieke platform, besturingssysteem en installatie-instellingen.

1. ## Vereisten

   Voordat u de volgende procedure start, verwijdert u het oude bestand **tomcat.keystore** uit de map **<installatiemap Configuration Manager>\java\windows\x86_64\lib\security** of de map **<installatiemap Configuration Manager>\java\linux\x86_64\lib\security** (afhankelijk van welke map relevant is), als dit bestaat.

2. ## Genereer een server-keystore

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

   - Voer de volgende opdracht uit in de bin-map van de Java-installatie in de installatiemap van Configuration Manager:

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

     Het dialoogvenster van de console wordt geopend.

   - Voer het keystore-wachtwoord in. Indien het wachtwoord gewijzigd is, moet u het handmatig in het bestand wijzigen.

   - Beantwoord de vraag naar uw **voornaam en achternaam**. Voer de naam van de Configuration Manager-webserver in. Voer de overige parameters in op basis van 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. ## Het certificaat in de vertrouwde gegevensopslag van de client plaatsen

   Voeg het certificaat toe aan de vertrouwde gegevensopslag van de client in Internet Explorer op uw computer (**Extra > Internetopties > Inhoud > Certificaten**). Als u dit niet doet, wordt u gevraagd dit te doen als u de eerste keer Configuration Manager wilt gaan gebruiken.

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

4. **Het bestand server.xml wijzigen**

   Open het bestand **server.xml**. Dit bestand bevindt zich in de **<installatiemap van Configuration Manager>\servers\server-0\conf**. Zoek het gedeelte dat begint met

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

   dat in de opmerkingen vermeld staat. Activeer het script door het opmerkingenteken te verwijderen en de volgende attributen toe te voegen aan de HTTPS-connector:

   ```
   keystoreFile="<bestandslocatie tomcat.keystore>" (zie stap 2)
   keystorePass="<wachtwoord>"
   ```

   Maak de volgende regel tot commentaarregel:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   Opmerking: U mag de HTTP-verbindingspoort niet blokkeren. Als u HTTP-communicatie wilt blokkeren, kunt u voor dit doel een firewall gebruiken.

5. **Start de server opnieuw op**

   Start de Configuration Manager-server opnieuw op.

6. **Controleer de beveiliging van de server**

   Om te controleren of de Configuration Manager-server veilig is, voert u de volgende URL in de webbrowser in: **https://<servernaam of IP-adres van Configuration Manager>:8143/cnc**.

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

SSL op de servermachine inschakelen met een certificaat van een certificeringsinstantie - UCMDB

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

1. **Vereisten**

   Voordat u de volgende procedure start, verwijdert u eerst de oude keystore **server.keystore** in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. **Genereer een server-keystore**

a. Genereer een certificaat ondertekend door een certificeringsinstantie en installeer het onder Windows.

b. Exporteer het certificaat 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 wordt naar dit wachtwoord gevraagd wanneer u het keystore-type converteert naar een JAVA-keystore.) Het **.pfx**-bestand bevat nu een openbaar certificaat en een persoonlijke sleutel en is beveiligd met een wachtwoord.

c. Kopieer het **PFX**-bestand dat u hebt gemaakt naar de volgende map: **C:\hp\UCMDB\UCMDBServer\conf\security**.

d. Open de opdrachtregel en wijzig de map in **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**.

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

```
keytool -importkeystore -srckeystore
c:\hp\UCMDB\UCMDBServer\conf\security\<PFX-bestandsnaam> -
srcstoretype PKCS12 -destkeystore server.keystore
```

U wordt gevraagd naar het keystore-wachtwoord (**.pfx**) van de bron. Dit is het wachtwoord dat u hebt opgegeven toen u het **PFX**-bestand maakte in stap b.)

e. Voer het doel-keystore-wachtwoord in. Dit wachtwoord moet hetzelfde zijn als het wachtwoord dat u eerder hebt gedefinieerd in de JMX-methode **changeKeystorePassword**, in Security Services. Als het wachtwoord niet is gewijzigd, gebruikt u het standaardwachtwoord **hppass**.

f. Na het genereren van het certificaat schakelt u HTTP-poort 8080 uit. Zie "HTTP/HTTPS-poort inschakelen of uitschakelen" op pagina 29 voor meer informatie.

g. Als u een ander wachtwoord hebt gebruikt dan **hppass** of het wachtwoord voor het **PFX**-bestand, voert u de JMX-methode **changeKeystorePassword** uit en zorgt u ervoor dat de sleutel hetzelfde wachtwoord heeft.

> **Opmerking:** controleer of HTTPS-communicatie werkt voordat u de HTTP-poort sluit.

3. **Start de server opnieuw op**

4. **Controleer de beveiliging van de server**

Typ de volgende URL in de webbrowser om te controleren of de UCMDB-server beveiligd is: **https://<naam of IP-adres van UCMDB-server>:8443/ucmdb-ui**.

> **Let op:** Er kan slechts één servercertificaat in **server.keystore** staan.

SSL inschakelen op de servermachine met een certificaat van een certificeringsinstantie - Configuration Manager

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

1. ## Vereisten

   Voordat u de volgende procedure start, verwijdert u het oude bestand **tomcat.keystore** uit de map **<installatiemap Configuration Manager>\java\windows\x86_64\lib\security** of de map **<installatiemap Configuration Manager>\java\linux\x86_64\lib\security** (afhankelijk van welke map relevant is), als dit bestaat.

2. ## Genereer een server-keystore

   a. Genereer een certificaat ondertekend door een certificeringsinstantie en installeer het onder Windows.

   b. Exporteer het certificaat 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 wordt naar dit wachtwoord gevraagd wanneer u het keystore-type converteert naar een JAVA-keystore.)
   Het **.pfx**-bestand bevat nu een openbaar certificaat en een persoonlijke sleutel en is beveiligd met een wachtwoord.

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

   c. Open de opdrachtprompt en wijzig de map in **<installatiemap van Configuration Manager>\java\bin**.

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

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

   U wordt gevraagd naar het keystore-wachtwoord (**.pfx**) van de bron. Dit is het wachtwoord dat u hebt opgegeven toen u het PFX-bestand maakte in stap b.

3. ## Het bestand server.xml wijzigen

   Open het bestand **server.xml**. Dit bestand bevindt zich in de **<installatiemap van Configuration Manager>\servers\server-0\conf**. 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" />
```

Maak de volgende regel tot commentaarregel:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

Opmerking: U mag de HTTP-verbindingspoort niet blokkeren. Als u HTTP-communicatie wilt blokkeren, kunt u voor dit doel een firewall gebruiken.

4. **Start de server opnieuw op**

   Start de Configuration Manager-server opnieuw op.

5. **Controleer de beveiliging van de server**

   Om te controleren of de Configuration Manager-server veilig is, voert u de volgende URL in de webbrowser in: **https://<servernaam of IP-adres van Configuration Manager>:8143/cnc**.

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

   Opmerking: De locaties van alle mappen en bestanden zijn afhankelijk van uw specifieke platform, besturingssysteem en installatievoorkeuren.

   Bijvoorbeeld: `java/{naam besturingssysteem}/lib`.

SSL inschakelen op de clientmachines - UCMDB

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

Als de certificeringsinstantie niet wordt vertrouwd door de webbrowser, moet u het volledige trust-pad van het certificaat importeren of het certificaat dat door HP Universal CMDB wordt gebruikt, expliciet importeren in de truststore van de browser.

In het volgende voorbeeld ziet u hoe u het zelfondertekende certificaat **hpcert** importeert in de Windows-truststore om te worden gebruikt door Internet Explorer.

Een certificaat importeren in de Windows-truststore:

1. Zoek het certificaat **hpcert** en wijzig de naam in **hpcert.cer**.

   In Windows Verkenner wordt met een pictogram aangegeven dat het bestand een veiligheidscertificaat is.

2. Dubbelklik op **hpcert.cer** om het dialoogvenster Certificaten van Internet Explorer te openen.
3. Volg de instructies voor het inschakelen van vertrouwen door het certificaat te installeren met de wizard Certificaat importeren.

Opmerking: een andere methode voor het importeren van het certificaat dat door de UCMDB-server aan de webbrowser wordt uitgegeven, is door u aan te melden bij UCMDB en het certificaat te installeren wanneer de waarschuwing met betrekking tot een niet-vertrouwd certificaat wordt weergegeven.

SSL inschakelen met een Client-certificaat - Configuration Manager

Als het certificaat dat door de Configuration Manager-webserver wordt gebruikt is uitgegeven door een bekende certificeringsinstantie (CA), is het zeer waarschijnlijk dat uw webbrowser het certificaat kan valideren zonder verdere acties.

Als de servertruststore de certificeringsinstantie niet vertrouwt, 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).

Een certificaat importeren in de vertrouwde gegevensopslag van de server:

1. Zoek op de clientmachine het **hpcert**-certificaat en verander de naam van dit certificaat in **hpcert.cer**.
2. Kopieer **hpcert.cer** naar de servermachine in de map **<installatiemap van Configuration Manager>\java\bin**.
3. Op de servermachine importeert u het certificaat van de certificeringsinstantie naar de vertrouwde gegevensopslag (cacerts), met behulp van het hulpprogramma voor sleutels. Gebruik hiervoor de volgende opdracht:

   ```
   <installatiemap van Configuration Manager>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Wijzig het bestand **server.xml** (in de map **<installatiemap van Configuration Manager>\servers\server-0\conf**) als volgt:
   a. Breng de wijzigingen aan die worden beschreven in "Het bestand server.xml wijzigen" op pagina 23.
   b. Zodra u deze wijzigingen hebt gemaakt, voegt u de volgende attributen toe aan de HTTPS-connector:

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

   c. Stel `clientAuth="true"` in.
5. Controleer de serverbeveiliging zoals beschreven in "Controleer de beveiliging van de server" op vorige pagina.

SSL inschakelen op de client-SDK

U kunt HTTPS-transport tussen de client-SDK en de server-SDK gebruiken:

1. Zoek op de clientmachine in het product waarin de client-SDK is opgenomen naar de transportinstelling en zorg ervoor dat deze is geconfigureerd voor HTTPS en niet HTTP.
2. Download het CA-certificaat/zelfondertekende openbare certificaat naar de clientmachine en importeer het naar de truststore **cacerts** op de JRE die verbinding zal maken met de server.

   Gebruik de volgende opdracht:

   ```
   Keytool -import -alias <naam CA> -trustcacerts -file <pad naar openbare certificaten server> -keystore <pad naar client jre trusted cacerts store (bijvoorbeeld x:\program files\java\jre\lib\security\cacerts)>
   ```

Wederzijdse certificaatverificatie voor SDK

Deze modus gebruikt SSL en maakt zowel serververificatie door de UCMDB-server als clientverificatie door de UCMDB-API-client mogelijk. Zowel de server als de UCMDB-API-client probeert een certificaat naar de andere entiteit te sturen ter verificatie.

Opmerking: De volgende methode voor het inschakelen van SSL met wederzijdse verificatie op de SDK, is de veiligste methode en derhalve de aanbevolen communicatiemodus.

1. De UCMDB-API-clientconnector beveiligen in UCMDB:
   a. Open de JMX-console van UCMDB. Open een webbrowser en voer het volgende adres in: **http://<naam of IP-adres UCMDB-server>:8080/jmx-console**. Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord (standaard is dit sysadmin/sysadmin).
   b. Zoek de **UCMDB:service=Ports Management Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
   c. Zoek naar de bewerking **PortsDetails** en klik op **Aanroepen**. Let op het nummer van de HTTPS-poort met clientverificatie. De standaard is 8444 en deze poort moet zijn ingeschakeld.
   d. Ga terug naar de pagina Bewerkingen.
   e. Als u de ucmdb-api-connector wilt toewijzen aan de modus voor wederzijdse verificatie, roept u de methode **mapComponentToConnectors** aan met de volgende parameters:
      - **componentName**: ucmdb-api
      - **isHTTPSWithClientAuth**: true
      - Alle andere vlaggen: false

      Het volgende bericht wordt weergegeven:

```
Bewerking geslaagd. Component ucmdb-api is nu toegewezen aan:
HTTPS_CLIENT_AUTH-poorten.
```

f. Ga terug naar de pagina Bewerkingen.

2. Zorg ervoor dat de JRE die de UCMDB-API-client uitvoert, een keystore met een clientcertificaat heeft.
3. Exporteer het UCMDB-API-clientcertificaat uit de betreffende keystore.
4. Importeer het geëxporteerde UCMDB-API-clientcertificaat in de UCMDB-server-truststore.
   a. Op de UCMDB-machine kopieert u het UCMDB-API-clientcertificaatbestand dat werd gemaakt, naar de volgende map op de UCMDB-server:

      C:\HP\UCMDB\UCMDBServer\conf\security

   b. Voer de volgende opdracht uit:

      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <geëxporteerd UCMDB-api-clientcertificaat> - alias ucmdb-api

   c. Voer het wachtwoord van de UCMDB-server-truststore in (standaard **hppass**).
   d. Wanneer wordt gevraagd of het certificaat moet worden vertrouwd, drukt u op **j** en drukt u vervolgens op **Enter**.
   e. De uitvoer moet zijn: **Certificaat** is toegevoegd aan keystore.
5. Exporteer het UCMDB-servercertificaat uit de betreffende keystore.
   a. Voer de volgende opdracht uit op de UCMDB-machine:

      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file C:\HP\UCMDB\conf\security\server.cert

   b. Voer het wachtwoord van de UCMDB-server-truststore in (standaard **hppass**).
   c. Controleer of het certificaat is gemaakt in de volgende map:

      C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
6. Importeer het geëxporteerde UCMDB-certificaat naar de JRE van de UCMDB-API-client-truststore.
7. Start de UCMDB-server en de UCMDB-API-client opnieuw op.
8. Gebruik de volgende code om de UCMDB-API-client te verbinden met de UCMDB-API-server:

```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https", <SOME_HOST_NAME>,
<HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER (default:8444)>));
UcmdbService ucmdbService = provider.connect
(provider.createCertificateCredentials(<TheClientKeystore,
bijvoorbeeld: "c:\\client.keystore">, <KeystorePassword>),
provider.createClientContext(<ClientIdentification>));
```

De wachtwoorden voor de server-keystore wijzigen

Na installatie van de server is de HTTPS-poort geopend en is de store beveiligd met een zwak wachtwoord (het standaardwachtwoord **hppass**). Als u van plan bent om met alleen SSL te werken, moet u het wachtwoord wijzigen.

De volgende procedure laat zien hoe u alleen het **server.keystore**-wachtwoord kunt wijzigen. U moet echter dezelfde procedure uitvoeren om het **server.truststore**-wachtwoord te wijzigen.

Opmerking: U moet alle stappen van deze procedure uitvoeren.

1. Start de UCMDB-server.
2. Voer de wachtwoordwijziging door in de JMX-console.
   a. Start de webbrowser en voer het adres van de server in: **http://<hostnaam of IP-adres UCMDB-server>:8080/jmx-console**.

      Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

   b. Klik onder UCMDB op **UCMDB:service=Security Services** om de pagina Bewerkingen te openen.

   c. Zoek de bewerking **changeKeystorePassword** en voer deze uit.

      Dit veld mag niet leeg zijn en moet uit ten minste zes tekens bestaan. Het wachtwoord wordt alleen in de database gewijzigd.
3. Stop de UCMDB-server.
4. Voer opdrachten uit.

   Voer de volgende opdrachten uit vanuit **C:\hp\UCMDB\UCMBServer\bin\jre\bin**:

   a. Wijzig het store-wachtwoord:

      keytool -storepasswd -new <nieuw_keystore-wachtwoord> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <huidig_ keystore-wachtwoord>

   b. De volgende opdracht geeft de interne sleutel van de keystore weer. De eerste parameter is de alias. Sla deze parameter op voor de volgende opdracht:

      keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   c. Wijzig het sleutelwachtwoord (als de store niet leeg is):

      keytool -keypasswd -alias <alias> -keypass <huidigWachtwoord> -new <nieuwWachtwoord> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   d. Voer het nieuwe wachtwoord in.
5. Start de UCMDB-server.
6. Herhaal de procedure voor de server-truststore.

HTTP/HTTPS-poort inschakelen of uitschakelen

U kunt de HTTP- en HTTPS-poorten inschakelen of uitschakelen vanuit de gebruikersinterface of vanuit de JMX-console.

De HTTP/HTTPS-poort inschakelen of uitschakelen vanuit de gebruikersinterface:

1. Meld u aan bij HP Universal CMDB.
2. Selecteer **Beheer > Infrastructuurinstellingen**.
3. Geef **http** of **https** op in het vak **Filteren** (op naam) om de HTTP-instellingen weer te geven.
   - **HTTP(S)-verbindingen inschakelen**. **True**: de poort wordt ingeschakeld. **False**: de poort wordt uitgeschakeld.
4. Start de server opnieuw op om de wijziging toe te passen.

> **Let op:** de HTTPS-poort is standaard open. Als u de poort sluit, wordt de werking van **Server_Management.bat** verhinderd.

De HTTP/HTTPS-poort inschakelen of uitschakelen vanuit de JMX-console:

1. Open een webbrowser en voer het volgende adres in: http://localhost.<domeinnaam>:8080/jmx-console.
2. Voer de aanmeldingsgegevens voor de verificatie in de JMX-console in. De standaardaanmeldingsgegevens zijn:
   - Aanmeldingsnaam = **sysadmin**
   - Wachtwoord = **sysadmin**
3. Zoek de **UCMDB:service=Ports Management Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
4. Zoek naar de bewerking **HTTPSetEnable** en stel de juiste waarde in om de HTTP-poort in of uit te schakelen.
   - **True:** de poort wordt ingeschakeld.
   - **False:** de poort wordt uitgeschakeld.
5. Zoek naar de bewerking **HTTPSSetEnable** en stel de juiste waarde in om de HTTPS-poort in of uit te schakelen.
   - **True:** de poort wordt ingeschakeld.
   - **False:** de poort wordt uitgeschakeld.
6. Zoek naar de bewerking **HTTPSClientAuthSetEnable** en stel de juiste waarde in om de HTTPS-poort met clientverificatie in of uit te schakelen.
   - **True:** de poort wordt ingeschakeld.
   - **False:** de poort wordt uitgeschakeld.

De UCMDB-webcomponenten toewijzen aan poorten

U kunt de toewijzing van elke UCMDB-component aan de beschikbare poorten configureren vanuit de JMX-console.

De huidige componentconfiguraties weergeven:

1. Open een webbrowser en voer het volgende adres in: **http://localhost.<domeinnaam>:8080/jmx-console**.
2. Voer de aanmeldingsgegevens voor de verificatie in de JMX-console in. De standaardaanmeldingsgegevens zijn:

   Aanmeldingsnaam = **sysadmin**

   Wachtwoord = **sysadmin**
3. Zoek de **UCMDB:service=Ports Management Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
4. Zoek naar de methode **ComponentsConfigurations** en klik op **Aanroepen**.
5. Voor elke component worden de geldige poorten en momenteel toegewezen poorten weergegeven.

De componenten toewijzen:

1. Zoek de **UCMDB:service=Ports Management Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
2. Zoek naar de methode **mapComponentToConnectors**.
3. Geef een componentnaam op in het vak Waarde. Selecteer **True** of **False** voor elke poort die overeenkomt met uw selectie. Klik op **Aanroepen**. De geselecteerde component wordt toegewezen aan de geselecteerde poorten. U kunt de componentnamen zoeken door de methode **serverComponentsNames** aan te roepen.
4. Herhaal het proces voor elke relevante component.

Opmerking:

- elke component moet aan ten minste één poort zijn toegewezen. Als u een component aan geen enkele poort toewijst, wordt deze standaard aan de HTTP-poort toegewezen.
- als u een component toewijst aan zowel de HTTPS-poort als de HTTPS-poort met clientverificatie, wordt alleen de optie voor clientverificatie toegewezen (de andere optie is in dit geval redundant).

U kunt ook de waarde wijzigen die aan elke poort is toegewezen.

Waarden voor de poorten instellen:

1. Zoek de **UCMDB:service=Ports Management Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.

2. Als u een waarde wilt instellen voor de HTTP-poort, zoekt u naar de methode **HTTPSetPort** en geeft u een waarde op in het vak **Waarde**. Klik op **Aanroepen**.
3. Als u een waarde wilt instellen voor de HTTPS-poort, zoekt u naar de methode **HTTPSSetPort** en geeft u een waarde op in het vak **Waarde**. Klik op **Aanroepen**.
4. Als u een waarde wilt instellen voor de HTTPS-poort met clientverificatie, zoekt u naar de methode **HTTPSSetPort** en geeft u een waarde op in het vak **Waarde**. Klik op **Aanroepen**.

Configuration Manager configureren voor een SSL-verbinding met UCMDB

U kunt Configuration Manager configureren om met UCMDB te werken via SSL (Secure Sockets Layer). De SSL-connector op poort 8443 is in UCMDB standaard ingeschakeld.

1. Ga naar **<installatiemap van UCMDB>\bin\jre\bin** en voer de volgende opdracht uit:

   ```
   keytool -export -alias hpcert -keystore <map UCMDB-server>
   \conf\security\server.keystore -storepass hppass -file
   <certificaatbestand>
   ```

2. Kopieer het certificaatbestand naar een tijdelijke locatie op de lokale Configuration Manager-machine.
3. Voer een nieuwe installatie uit of configureer een bestaande installatie van Configuration Manager opnieuw. Zie de betreffende secties in de interactieve *HP Universal CMDB – Implementatiehandleiding* voor instructies.

   Stel in het UCMDB-configuratiescherm het protocol in op HTTPS, en kies het certificaatbestand dat u in stap 2 hebt gekopieerd.

Als u Configuration Manager wilt configureren om via SSL met andere producten te werken (zoals netwerktaakverdelingen), importeert u het beveiligingscertificaat van het product in de truststore van Configuration Manager (standaard JRE-truststore) door de volgende opdracht uit te voeren:

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias>
-keystore <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit
-file <certificaatbestand>
```

De UCMDB KPI-adapter voor gebruik met SSL inschakelen

U kunt de informatie voor de UCMDB KPI-adapter configureren die moet worden verzonden met SSL (Secure Sockets Layer).

1. Exporteer het Configuration Manager-certificaat:

   ```
   <CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
   <CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
   <wachtwoord keystore> -file <naam certificaatbestand>
   ```

2. Importeer het certificaat dat u uit Configuration Manager hebt geëxporteerd als volgt in de

UCMDB-truststore:

```
<map UCMDB-server>\bin\jre\bin keytool -import -trustcacerts
-alias tomcat -keystore <map UCMDB-server>\bin\jre\lib
\security\cacerts -storepass changeit -file <certificaatbestand>
```

3. Importeer het certificaat dat u uit Configuration Manager hebt geëxporteerd als volgt in de truststore van de probe:

   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   <map DataFlowProbe>\bin\jre\bin\keytool.exe -import -v -keystore
   <map DataFlowProbe>\conf\security\MAMTrustStoreExp.jks -file
   <certificaatbestand> -alias tomcat
   ```

   b. Voer het keystore-wachtwoord in: logomania

   c. Wanneer wordtgevraagd of het certificaat moet worden vertrouwd, drukt u op **j** en vervolgens op **Enter**.

   Het volgende bericht wordt weergegeven:

   Certificaat is toegevoegd aan keystore.

   Zie "Beveiliging Data Flow-probe" op pagina 63 voor aanvullende informatie over beveiliging van de Data Flow-probe

4. Start UCMDB, de Data Flow-probe en Configuration Manager opnieuw op.

SSL-ondersteuning voor de UCMDB-browser configureren

Opmerking: De instructies die hier worden beschreven, zijn relevant voor UCMDB-browser versie 1.7. Als u een latere versie van de UCMDB-browser gebruikt die afzonderlijk van de rest van de UCMDB-productsuite is bijgewerkt, raadpleegt u de sectie over het configureren van SSL-ondersteuning in de *UCMDB Browser Installation and Configuration Guide* voor die versie.

SSL-ondersteuning voor Tomcat installeren en configureren:

1. Maak een Keystore-bestand om de persoonlijke sleutel en het zelfondertekende certificaat van de server op te slaan door een van de volgende opdrachten uit te voeren:

   - Voor Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - Voor Unix: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   Voor beide opdrachten gebruikt u de wachtwoordwaarde **changeit** (voor alle overige velden in het dialoogvenster van de console dat wordt geopend, kunt u elke gewenste waarde gebruiken).

2. Verwijder opmerkingen uit de de vermelding **SSL HTTP/1.1 Connector** in **$CATALINA_BASE/conf/server.xml**, waarbij **$CATALINA_BASE** de map is waarin u Tomcat hebt

geïnstalleerd.

> **Opmerking:** Voor een volledige beschrijving van de configuratie van **server.xml** om SSL te kunnen gebruiken, raadpleegt u de officiële site van Apache Tomcat: http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. Start de Tomcat-server opnieuw op.

Het HTTPS-protocol gebruiken om verbinding te maken met de UCMDB-server:

1. Wijs in **ucmdb_browser_config.xml** de waarde **https** toe aan de tag **<protocol>** en wijs de HTTPS-poortwaarde voor de UCMDB-server (standaard 8443) toe aan de tag **<poort>.**
2. Download het openbare certificaat voor de UCMDB-server naar de machine met de UCMDB-browser (als u SSL gebruikt op de UCMDB-server, kan de UCMDB-beheerder dit certificaat aan u verstrekken), en importeer het in de truststore **cacerts** op de JRE die verbinding zal maken met de server door de volgende opdracht uit te voeren:

   "%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB-Server-certificate-file> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"

   waarbij **<UCMDB-Server-certificate-file>** het volledige pad is naar het openbare certificaatbestand van de UCMDB-server.
3. Start de Tomcat-server opnieuw op.

Hoofdstuk 3

Werken met een reverse proxy

In deze sectie worden de afsplitsingen in de beveiliging van reverse proxy's beschreven en worden instructies geven voor het gebruik van een reverse proxy met HP Universal CMDB. Beveiligingsaspecten van een reverse proxy worden besproken, maar geen andere aspecten, zoals caching en netwerktaakverdeling.

In dit hoofdstuk vindt u de volgende informatie:

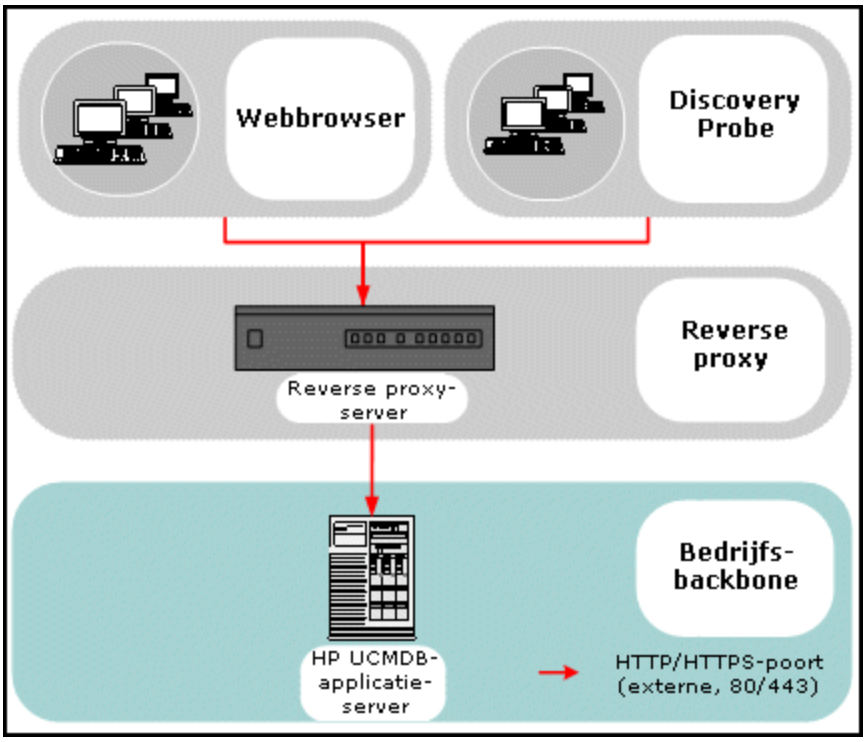
Reverse proxy - overzicht

Een reverse proxy is een tussenliggende server tussen de clientmachine en de webservers. Voor de clientmachine lijkt de reverse proxy een standaardwebserver die de HTTP-protocolverzoeken van de clientmachine afhandelt.

De clientmachine verzendt gewone verzoeken voor webcontent en gebruikt daarvoor de naam van de reverse proxy in plaats van de naam van de webserver. De reverse proxy verzendt het verzoek naar een van de webservers. Hoewel de respons via de reverse proxy naar de clientmachine wordt teruggestuurd, lijkt het voor de clientmachine alsof de respons wordt verzonden door de webserver.

Het is mogelijk om meerdere reverse proxy's te hebben (met verschillende URL's) die hetzelfde UCMDB/CM-exemplaar voorstellen. U kunt daarnaast ook een enkele reverse proxy-server gebruiken om toegang te krijgen tot meerdere UCMDB/CM-servers door verschillende hoofdcontexten in te stellen voor elke UCMDB/CM-server.

HP Universal CMDB en Configuration Manager ondersteunen een reverse proxy in een DMZ-architectuur. De reverse proxy is een HTTP-mediator tussen de Data Flow-probe en de webclient en de HP Universal CMDB/CM-server.



Opmerking:

- Verschillende typen reverse proxy vereisen een verschillende configuratiesyntaxis. Zie bijvoorbeeld " Voorbeeld: Configuratie van Apache 2.0.x " op pagina 37 voor de reverse proxy-configuratie voor Apache 2.0.x.
- Het is alleen nodig om de instelling URL Front-end te configureren wanneer u een directe koppeling naar een rapport maakt met Planner.

Beveiligingsaspecten van het gebruik van een reverse proxy-server

Een reverse proxy-server werkt als een bastion-host. De proxy wordt geconfigureerd om de enige machine te zijn die rechtstreeks door externe clients wordt aangesproken. De proxy schermt dus de rest van het interne netwerk af. Door het gebruik van een reverse proxy kan de applicatieserver op een afzonderlijke machine in het interne netwerk worden geplaatst.

In deze sectie wordt het gebruik van een DMZ en reverse proxy in een back-to-back topologie besproken.

Hieronder vindt u de belangrijkste voordelen van het gebruik van een reverse proxy voor de veiligheid in een omgeving van dit type:

- Er vindt geen DMZ-protocolvertaling plaats. Het inkomende en uitgaande protocol zijn hetzelfde (alleen de koptekst verandert).
- Alleen HTTP-toegang tot de reverse proxy is toegestaan. Dit betekent dat firewalls voor stateful packet inspection de communicatie beter kunnen beschermen.

- Een statische, beperkte set omleidingsverzoeken kan worden gedefinieerd op de reverse proxy.
- De meeste webserverbeveiligingsfuncties zijn beschikbaar op de reverse proxy (verificatiemethoden, codering, enzovoort).
- De reverse proxy screent de IP-adressen van de real servers, alsmede de architectuur van het interne netwerk.
- De reverse proxy is de enige toegankelijke client van de webserver.
- Deze configuratie ondersteunt NAT-firewalls (in tegenstelling tot andere oplossingen).
- De reverse proxy vereist een minimaal aantal geopende poorten in de firewall.
- De reverse proxy levert goede prestaties in vergelijking met andere bastion-oplossingen.

Een reverse proxy configureren

In deze sectie wordt beschreven hoe u een reverse proxy configureert.

Een reverse proxy configureren met behulp van infrastructuurinstellingen

De volgende procedure laat zien hoe u infrastructuurinstellingen kunt gebruiken om een reverse proxy te configureren. Deze configuratie is alleen nodig wanneer u een directe koppeling maakt naar een rapport met Planner.

Zo configureert u een reverse proxy:

1. Selecteer **Beheer > Infrastructuurinstellingen > Algemene instellingen**.
2. Wijzig de instelling voor URL Front-end. Voer het adres in, bijvoorbeeld **https://mijn_proxyserver:443/**.

Opmerking: Nadat u deze wijziging hebt doorgevoerd, kunt u de HP Universal CMDB-server niet meer rechtstreeks via een client benaderen. Als u de reverse proxy-configuratie wilt wijzigen, gebruikt u de JMX-console op de servermachine. Zie Een reverse proxy configureren met behulp van de JMX-console hieronder voor meer informatie.

Een reverse proxy configureren met behulp van de JMX-console

U kunt wijzigingen in de reverse proxy-configuratie aanbrengen met behulp van de JMX-console op de HP Universal CMDB-servermachine. Deze configuratie is alleen nodig wanneer u een directe koppeling maakt naar een rapport met Planner.

Een reverse proxy-configuratie wijzigen:

1. Start de webbrowser op de HP Universal CMDB-servermachine en voer het volgende adres in:

   http://<machinenaam of IP-adres>.<domeinnaam>:8080/jmx-console

   waarbij **<machinenaam of IP-adres>** de machine is waarop HP Universal CMDB is geïnstalleerd. Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

2. Klik op de koppeling **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

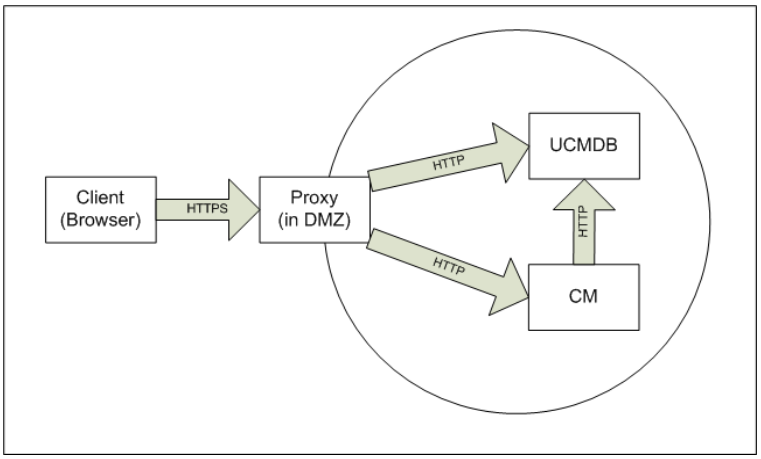
   Voer in het veld **setUseFrontendURLBySettings** de URL van de proxyserver in, bijvoorbeeld `https://mijn_proxyserver:443/`.

3. Klik op **Aanroepen**.
4. U kunt de waarde van deze instelling weergeven met de methode **showFrontendURLInSettings**.

Voorbeeld: Configuratie van Apache 2.0.x

In deze sectie wordt een voorbeeld beschreven van een configuratiebestand waarbij het gebruik van een Apache 2.0.x reverse proxy wordt ondersteund in een geval waarin zowel Data Flow-probes als applicatiegebruikers verbinding maken met HP Universal CMDB.

In het onderstaande diagram wordt het configuratieproces voor een reverse proxy voor Configuration Manager en de UCMDB geïllustreerd:



Opmerking:

- In dit voorbeeld zijn de DNS-naam en poort van de HP Universal CMDB-machine UCMDB_server.
- In dit voorbeeld zijn de DNS-naam en poort van HP Configuration Manager UCMDB_CM_server.
- Deze wijziging mag uitsluitend worden aangebracht door gebruikers met kennis van het beheer van Apache.

1. Open het bestand **<hoofdmap Apache-machine>\Webserver\conf\httpd.conf**.
2. Schakel de volgende modules in:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
   - **LoadModule headers_module modules/mod_headers.so**
3. Voeg de volgende regels toe aan het bestand httpd.conf:

```
ProxyRequests off

<Proxy *>

Order deny,allow

Deny from all
```

```
Allow from all
</Proxy>
ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
```

```
ProxyPassReverse /docs http://UCMDB_CM_server/docs

ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser

ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-
browser

ProxyPreserveHost On

RequestHeader set X-Reverse-Proxy "https://<SRP-host>:<SRP-poort>"
```

Opmerking: De regel `ProxyPreserveHost On` is alleen vereist als er sprake is van een virtuele host.

Let op: Het is van cruciaal belang dat u de regel `RequestHeader set X-Reverse-Proxy "https://<SRP host>:<SRP port>"` toevoegt. Zonder deze regel werkt de configuratie niet.

4. Sla de wijzigingen op.

De Data Flow-probe verbinden op basis van reverse proxy of load balancer middels wederzijdse verificatie

Voer de volgende procedure uit om de Data Flow-probe te verbinden via reverse proxy of load balancer middels wederzijdse verificatie. Deze procedure is van toepassing op de volgende configuratie:

- Wederzijdse SSL-verificatie tussen de probe en een reverse proxy of load balancer op basis van een clientcertificaat dat is verstrekt door de probe en vereist is voor de reverse proxy of load balancer.
- Een normale SSL-verbinding tussen de reverse proxy of load balancer en de UCMDB-server.

Opmerking: De volgende instructies gaan uit van het gebruik van de keystore **cKeyStoreFile** als de probe-keystore. Dit is een voorgedefinieerde client-keystore die deel uitmaakt van de installatie van de Data Flow-probe en een zelfondertekend certificaat bevat. Zie "Standaardkeystore en -truststore voor server en Data Flow-probe" op pagina 78 voor meer informatie over dit onderwerp.

Het is raadzaam om een nieuwe, unieke keystore te maken waarin een nieuwe gegenereerde persoonlijke sleutel is opgenomen. Zie "Een keystore maken voor de Data Flow-probe" op pagina 77 voor meer informatie over dit onderwerp.

Een certificaat verkrijgen van een certificeringsinstantie

Verkrijg het hoofdcertificaat van de certificeringsinstantie en importeer het naar de volgende locaties:

- de truststore van de Data Flow-probe
- de JVM-cacerts van de Data Flow-probe
- de truststore van de UCMDB-server
- de truststore van de reverse proxy

1. Importeer het hoofdcertificaat van de certificeringsinstantie in de truststore van de Data Flow-probe.
   a. Plaats het hoofdcertificaat van de certificeringsinstantie in de volgende map: <installatiemap Data Flow-probe>\conf\security\<naam certificaatbestand>.
   b. Importeer het hoofdcertificaat van de certificeringsinstantie in de Data Flow-truststore door het volgende script uit te voeren.

      ```
      <installatiemap Data Flow-probe>\bin\jre\bin\keytool.exe -import
      -trustcacerts -alias <UwAlias> -file
      C:\hp\UCMDB\DataFlowProbe\conf\security\<naam
      certificaatbestand> -keystore <installatiemap Data Flow-
      probe>\conf\security\MAMTrustStoreExp.jks
      ```

      Het standaardwachtwoord is: **logomania**.
2. Importeer het hoofdcertificaat van de certificeringsinstantie in de JVM-cacerts van de Data Flow-probe door het volgende script uit te voeren.

   ```
   <installatiemap Data Flow-probe>\bin\jre\bin\keytool.exe -import -
   trustcacerts -alias <UwAlias> -file <installatiemap Data Flow-
   probe>\conf\security\<naam certificaatbestand> -keystore
   <installatiemap Data Flow-probe>\bin\jre\lib\security\cacerts
   ```

   Het standaardwachtwoord is: **changeit**.
3. Importeer het hoofdcertificaat van de certificeringsinstantie in de UCMDB-truststore.
   a. Plaats het hoofdcertificaat van de certificeringsinstantie in de volgende map: <installatiemap UCMDB>\conf\security\<naam certificaatbestand>.
   b. Importeer het hoofdcertificaat van de certificeringsinstantie in de UCMDB-truststore door het volgende script uit te voeren.

      ```
      <installatiemap UCMDB>\bin\jre\bin\keytool.exe -import -
      trustcacerts -alias <UwAlias> -file <installatiemap
      UCMDB>\conf\security\<naam ceritificaatbestand> -keystore
      <installatiemap UCMDB>\conf\security\sever.truststore
      ```

      Het standaardwachtwoord is: **hppass**.
4. Importeer het hoofdcertificaat van de certificeringsinstantie in de truststore voor de reverse proxy. Deze stap is afhankelijk van de leverancier.

Converteer het certificaat naar een Java-keystore

Verkrijg het clientcertificaat (en de persoonlijke sleutel) voor de Data Flow-probe van uw certificeringsinstantie in de PFX/PKCS12-indeling en converteer het naar een Java-keystore door het volgende script uit te voeren:

```
<installatiemap Data Flow-probe>\bin\jre\bin\keytool.exe -
importkeystore -srckeystore <volledig pad PFX-keystore> -destkeystore
<volledig pad nieuwe doel-keystore> -srcstoretype PKCS12
```

U wordt gevraagd om de wachtwoorden voor de bron- en doel-keystore.

Voor het wachtwoord van de bron-keystore gebruikt u hetzelfde wachtwoord dat werd gebruikt tijdens het exporteren van de PFX-keystore.

Het standaardwachtwoord voor de doel-keystore voor de keystore van de Data Flow-probe is: **logomania**.

Opmerking: Als u voor de doel-keystore een ander wachtwoord hebt ingevoerd dat het standaardwachtwoord voor de keystore van de Data Flow-probe (logomania), moet u het nieuwe wachtwoord gecodeerd opgeven in het bestand **<installatiemap Data Flow-probe>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Zie "Wachtwoorden voor de probe-keystore en probe-truststore coderen" op pagina 77 voor meer informatie over dit onderwerp.

Plaats de nieuwe keystore in de volgende map: **<installatiemap Data Flow-probe>\conf\security**

Let op: Zorg dat u het bestand **MAMKeyStoreExp.jks** niet overschrijft.

Het SSL-eigenschappenbestand wijzigen zodat de nieuwe keystore wordt gebruikt

Stel in het bestand **<installatiemap Data Flow-probe>\conf\ssl.properties** de keystore die het clientcertificaat bevat, in op **javax.net.ssl.keyStore**.

Als het wachtwoord voor uw keystore niet het standaardwachtwoord voor de keystore van de Data Flow-probe is (logomania), werkt u het bestand **javax.net.ssl.keyStorePassword** bij nadat u het hebt gecodeerd. Zie "Wachtwoorden voor de probe-keystore en probe-truststore coderen" op pagina 77 voor meer informatie over het coderen van het wachtwoord.

De configuratie van de Data Flow-probe controleren

Bewerk het bestand **<installatiemap Data Flow-probe>\conf\DataFlowProbe.properties** als volgt:

```
appilog.agent.probe.protocol = HTTPS

serverName = <serveradres reverse proxy>

serverPortHttps = <de HTTPS-poort waarnaar de reverse proxy luistert
om verzoeken om te leiden naar de UCMDB>
```

UCMDB configureren om te werken met SSL

Zie "Secure Sockets Layer-communicatie (SSL) inschakelen" op pagina 18 voor meer informatie over dit onderwerp.

Als het certificaat van de UCMDB-server wordt gemaakt door dezelfde certificeringsinstantie die de rest van de certificaten in deze procedure heeft gemaakt, vertrouwt de reverse proxy of load balancer het UCMDB-certificaat.

Hoofdstuk 4

Beheer van Data Flow-referenties

In dit hoofdstuk vindt u de volgende informatie:

Beheer van Data Flow-referenties - overzicht

Voor het toepassen van discovery of het uitvoeren van integratie moet u de benodigde referenties instellen voor toegang tot het externe systeem. Referenties worden geconfigureerd in het venster Instellingen Data Flow-probe en opgeslagen op de UCMDB-server. Raadpleeg het gedeelte over de instellingen van de Data Flow-probe in de *HP Universal CMDB – Handleiding Data Flow Management* voor meer informatie.

De opslag van referenties wordt beheerd door de component Confidential Manager. Zie "Confidential Manager" op pagina 91 voor meer informatie over dit onderwerp.

De Data Flow-probe heeft toegang tot de referenties via de Confidential Manager-client. De Confidential Manager-client bevindt zich op de Data Flow-probe en communiceert met de Confidential Manager-server, die zich op de UCMDB-server bevindt. Communicatie tussen de Confidential Manager-client en de Confidential Manager-server is gecodeerd en verificatie van de Confidential Manager-client is vereist wanneer deze verbinding maakt met de Confidential Manager-server.

De verificatie van de Confidential Manager-client op de Confidential Manager-server is gebaseerd op een LW-SSO-component. Alvorens verbinding te maken met de Confidential Manager-server, stuurt de Confidential Manager-client eerst een LW-SSO-cookie. De Confidential Manager-server verifieert de cookie en als de verificatie slaagt, wordt de communicatie met de Confidential Manager-client gestart. Zie "LW-SSO-instellingen configureren" op pagina 47 voor meer informatie over LW-SSO.

De communicatie tussen de Confidential Manager-client en de Confidential Manager-server is gecodeerd. Zie "Confidential Manager-communicatiecodering configureren " op pagina 47 voor meer informatie over het bijwerken van de coderingsconfiguratie.

Let op: De Confidential Manager-verificatie maakt gebruik van de universele tijd die op de computer is gedefinieerd (UTC). Om de verificatie laten slagen, moet u ervoor zorgen dat de universele tijd op de Data Flow-probe en de UCMDB-server hetzelfde zijn. De server en probe kunnen zich in verschillende tijdzones bevinden, aangezien UTC onafhankelijk is van de tijdzone of het gebruik van zomertijd.

De Confidential Manager-client houdt een lokale cache van de referenties bij. De Confidential Manager-client is geconfigureerd om alle referenties te downloaden van de Confidential Manager-server en op te slaan in een cache. Wijzigingen in de referenties worden automatisch continu gesynchroniseerd vanaf de Confidential Manager-server. De cache kan een bestandssysteem- of

geheugencache zijn, afhankelijk van de vooraf geconfigureerde instellingen. Verder is de cache gecodeerd en kan deze niet extern worden benaderd. Zie "De cachemodus van de Confidential Manager-client configureren op de probe" op pagina 52 voor meer informatie over het bijwerken van de cache-instellingen. Zie "De instellingen voor cachecodering van de Confidential Manager-client configureren op de probe" op pagina 52 voor meer informatie over het bijwerken van de cachecodering.

Zie "Het niveau van logboekbestandberichten voor de Confidential Manager-client wijzigen" op pagina 55 voor meer informatie over het oplossen van problemen.

U kunt referenties kopiëren van de ene naar de andere UCMDB-server. Zie "Referentie- en bereikgegevens gecodeerd exporteren en importeren" op pagina 53 voor meer informatie over dit onderwerp.

Opmerking: Het **DomainScopeDocument** (DSD) dat werd gebruikt voor de opslag van referenties op de probe (in UCMDB versie 9.01 of eerder), bevat geen referentiegevoelige informatie meer. Het bestand bevat nu een lijst met probes en informatie over het netwerkbereik. Het bevat bovendien een lijst met referentievermeldingen voor elk domein, waarbij elke vermelding uitsluitend de referentie-ID en een netwerkbereik (gedefinieerd voor deze referentie) omvat.

In dit gedeelte vindt u de volgende onderwerpen:

Uitgangspunten voor beveiliging

Voor beveiliging wordt uitgegaan van het volgende:

U hebt de UCMDB-server en de JMX-console van de probe zodanig beveiligd dat alleen UCMDB-systeembeheerders toegang hebben, bij voorkeur alleen via localhost-toegang.

Data Flow-probe uitgevoerd in de afzonderlijke modus

Wanneer de probe-manager en probe-gateway als afzonderlijke processen worden uitgevoerd, wordt de Confidential Manager-clientcomponent onderdeel van het managerproces. Referentiegegevens worden alleen door de probe-manager gecached en gebruikt. Voor toegang tot de Confidential Manager-server op het UCMDB-systeem wordt het Confidential Manager-clientverzoek afgehandeld door het gateway-proces. Van daaruit wordt het doorgestuurd naar het UCMDB-systeem.

Deze configuratie wordt automatisch uitgevoerd wanneer de probe in de afzonderlijke modus is geconfigureerd.

De cache met referenties up-to-date houden

Na de eerste geslaagde verbinding met de Confidential Manager-server downloadt de Confidential Manager-client alle relevante referenties (alle referenties die in het domein van de probe zijn geconfigureerd). Na de eerste geslaagde communicatie behoudt de Confidential Manager-client een doorlopende synchronisatie met de Confidential Manager-server. Differentiële synchronisatie wordt uitgevoerd met een interval van één minuut. Gedurende deze intervallen worden alleen de verschillen tussen de Confidential Manager-server en de Confidential Manager-client gesynchroniseerd. Als de referenties worden gewijzigd op de UCMDB-server (bijvoorbeeld doordat nieuwe referenties worden toegevoegd of bestaande referenties worden bijgewerkt of verwijderd), ontvangt de Confidential Manager-client direct een bericht van de UCMDB-server en wordt een extra synchronisatie uitgevoerd.

Alle probes synchroniseren met configuratiewijzigingen

Voor succesvolle communicatie moet de Confidential Manager-client worden bijgewerkt met de verificatieconfiguratie (initreeks LW-SSO) en de coderingsconfiguratie (Confidential Manager-communicatiecodering) voor de Confidential Manager-server. Wanneer de initreeks bijvoorbeeld is gewijzigd op de server, moet de probe de nieuwe initreeks kennen om te kunnen verifiëren.

De UCMDB-server controleert doorlopend of wijzigingen hebben plaatsgevonden in de configuratie van Confidential Manager-communicatiecodering en Confidential Manager-verificatie. Deze controle vindt elke 15 seconden plaats; indien een wijziging is opgetreden, wordt de bijgewerkte configuratie naar de probes verzonden. De configuratie wordt gecodeerd aan de probes doorgegeven en wordt in een beveiligde opslag op de probe opgeslagen. De codering van de configuratie die wordt verzonden, wordt uitgevoerd met een symmetrische coderingssleutel. Standaard worden de UCMDB-server en de Data Flow-probe geïnstalleerd met dezelfde algemene symmetrische coderingssleutel. Voor optimale beveiliging wordt ten zeerste aangeraden om deze sleutel te wijzigen alvorens referenties aan het systeem toe te voegen. Zie "De coderingssleutel genereren of bijwerken" op pagina 56 voor meer informatie over dit onderwerp.

Opmerking: Doordat een controle-interval van 15 seconden wordt gehanteerd, is het mogelijk dat de Confidential Manager-client op de probe gedurende 15 seconden niet is bijgewerkt met de meest recente configuratie.

Als u ervoor kiest om de automatische synchronisatie van de Confidential Manager-communicatieconfiguratie en de Confidential Manager-verificatieconfiguratie tussen de UCMDB-server en de Data Flow-probe uit te schakelen, moet u telkens wanneer u de Confidential Manager-communicatieconfiguratie en de Confidential Manager-verificatieconfiguratie bijwerkt op de UCMDB-server ook alle probes bijwerken met de nieuwe configuratie. Zie "Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" op pagina 49 voor meer informatie over dit onderwerp.

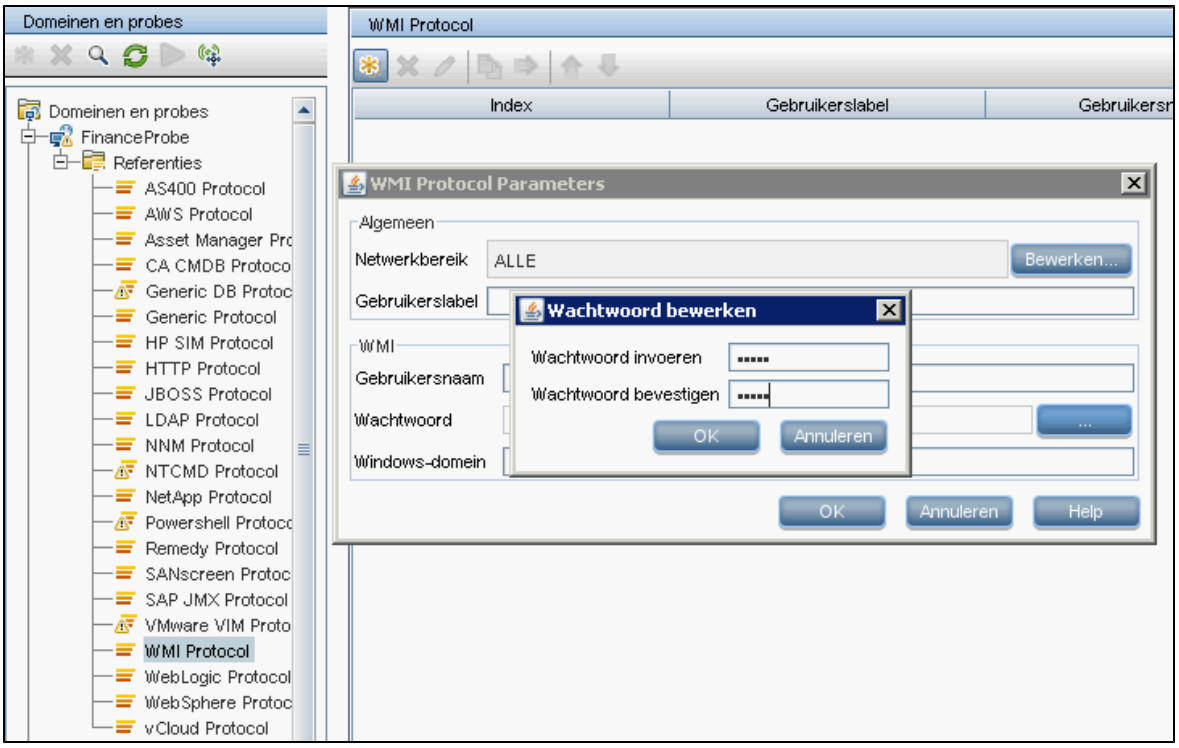
Beveiligde opslag op de probe

Alle gevoelige informatie (zoals de Confidential Manager-communicatieconfiguratie en -verificatieconfiguratie en de coderingssleutel) wordt in een beveiligde opslag op de probe opgeslagen in de vorm van het bestand **secured_storage.bin** in **C:\hp\UCMDB\DataFlowProbe\conf\security**. Deze beveiligde opslag is gecodeerd met DPAPI, een methode die het Windows-proces voor gebruikerswachtwoorden en codering gebruikt. DPAPI is een standaardmethode die wordt gebruikt voor de beveiliging van vertrouwelijke gegevens (zoals certificaten en persoonlijke sleutels) op Windows-systemen. De probe moet altijd onder dezelfde Windows-gebruiker worden uitgevoerd zodat de probe de informatie die in de beveiligde opslag is opgeslagen, nog steeds kan lezen als het wachtwoord wordt gewijzigd.

Referentie-informatie weergeven

Opmerking: In deze sectie wordt beschreven hoe u referentiegegevens weergeeft wanneer de richting van de gegevens van CMDB naar HP Universal CMDB loopt.

Wachtwoorden worden niet van de CMDB naar de applicatie verzonden. Dat wil zeggen dat HP Universal CMDB sterretjes (*) in het wachtwoordveld weergeeft, ongeacht de inhoud:



Referentie-informatie bijwerken

Opmerking: In deze sectie wordt beschreven hoe u referenties bijwerkt wanneer de richting

van de gegevens van HP Universal CMDB naar CMDB loopt.

- De communicatie in deze richting is niet gecodeerd, dus u moet verbinding maken met de UCMDB-server via https\SSL, of zorgen voor een beveiligde verbinding via een betrouwbaar netwerk.

  Hoewel de communicatie niet gecodeerd is, worden wachtwoorden niet als duidelijk herkenbare tekst via het netwerk verzonden. Ze worden gecodeerd met een standaardsleutel en het wordt derhalve ten zeerste aangeraden om SSL te gebruiken voor effectieve vertrouwelijkheid gedurende de overdracht.

- U kunt speciale tekens en niet-Engelse tekens gebruiken in wachtwoorden.

Verificatie- en coderingsinstellingen van de Confidential Manager-client configureren

In deze taak wordt beschreven hoe u de verificatie- en coderingsinstellingen van de Confidential Manager-client configureert op de UCMDB-server, en deze omvat de volgende stappen:

- "LW-SSO-instellingen configureren" beneden
- "Confidential Manager-communicatiecodering configureren " beneden

LW-SSO-instellingen configureren

Aan de hand van deze procedure kunt u de initreeks voor LW-SSO wijzigen op de UCMDB-server. Deze wijziging wordt automatisch (als gecodeerde tekenreeks) naar probes verzonden, tenzij de UCMDB-server is geconfigureerd om dit niet automatisch te doen. Zie "Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" op pagina 49 voor meer informatie over dit onderwerp.

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console**.
2. Klik op **UCMDB-UI:name=LW-SSO Configuration** om de weergavepagina van JMX MBEAN te openen.
3. Zoek naar de methode **setInitString**.
4. Voer een nieuwe LW-SSO-initreeks in.
5. Klik op Aanroepen.

Confidential Manager-communicatiecodering configureren

In deze procedure wordt beschreven hoe u de instellingen voor Confidential Manager-communicatiecodering kunt wijzigen op de UCMDB-server. Deze instellingen specificeren de codering van de communicatie tussen de Confidential Manager-client en de Confidential Manager-server. Deze wijziging wordt automatisch (als gecodeerde tekenreeks) naar probes verzonden, tenzij de UCMDB-server is geconfigureerd om dit niet automatisch te doen. Zie "Automatische

synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" op pagina 49 voor meer informatie over dit onderwerp.

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console.**
2. Klik op **UCMDB:service=Security Services** om de weergavepagina van JMX MBEAN te openen.
3. Klik op de methode **CMGetConfiguration**.
4. Klik op **Aanroepen**.

   De XML van de huidige Confidential Manager-configuratie wordt weergegeven.
5. Kopieer de inhoud van de weergegeven XML.
6. Navigeer terug naar de weergavepagina **Security Services** van JMX MBEAN.
7. Klik op de methode **CMSetConfiguration**.
8. Plak de gekopieerde XML in het veld **Waarde**.
9. Werk de relevante transportgerelateerde instellingen bij.

   Zie "Coderingsinstellingen van Confidential Manager" op pagina 60 voor meer informatie over de waarden die kunnen worden bijgewerkt.

   Voorbeeld:

```
<transport>
        <encryptTransportMode>true</encryptTransportMode>
        <CMEncryptionDecryption>
                <encryptDecryptInitString>radiohead</encryptDecryptInitString>
                <cryptoSource>lw</cryptoSource>
                <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
                <cipherType>symmetricBlockCipher</cipherType>
                <engineName>AES</engineName>
                <algorithmModeName>CBC</algorithmModeName>
                <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
                <keySize>256</keySize>
                <pbeCount>20</pbeCount>
                <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
                <encodingMode>Base64Url</encodingMode>
                <useMacWithCrypto>false</useMacWithCrypto>
                <macType>hmac</macType>
                <macKeySize>256</macKeySize>
```

```
                <macHashName>SHA256</macHashName>
            </CMEncryptionDecryption>
        </transport>
```

10. Klik op **Aanroepen**.

Verificatie- en coderingsinstellingen van de Confidential Manager-client handmatig configureren op de probe

Deze taak omvat de onderstaande stappen:

- "Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" beneden
- "Verificatie- en coderingsinstellingen van de Confidential Manager-client configureren op de probe" op volgende pagina
- "Confidential Manager-communicatiecodering configureren op de probe" op volgende pagina

Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen

De UCMDB-server is standaard geconfigureerd om de Confidential Manager/LW-SSO-instellingen automatisch naar alle probes te verzenden. Deze informatie wordt als gecodeerde tekenreeks verzonden naar de probes, waar de informatie bij aankomst wordt gedecodeerd. U kunt de UCMDB-server configureren om de Confidential Manager/LW-SSO-configuratiebestanden niet automatisch naar alle probes te verzenden. In dit geval is het uw verantwoordelijkheid om handmatig alle probes bij te werken met de nieuwe Confidential Manager/LW-SSO-instellingen.

Automatische synchronisatie van Confidential Manager/LW-SSO-instellingen uitschakelen:

1. Klik in UCMDB op **Beheer > Beheer van infrastructuurinstellingen > Algemene instellingen**.
2. Selecteer **Automatische synchronisatie van CM/LW-SSO-configuratie en initreeks met probe inschakelen**.
3. Klik op het veld **Waarde** en verander **True** in **False**.
4. Klik op de knop **Save**.
5. Start de UCMDB-server opnieuw op.

Verificatie- en coderingsinstellingen van de Confidential Manager-client configureren op de probe

Deze procedure is relevant als de UCMDB-server is geconfigureerd om de configuratie en instellingen van LW-SSO/Confidential Manager niet automatisch naar probes te verzenden. Zie "Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" op vorige pagina voor meer informatie over dit onderwerp.

1. Start de webbrowser op de probe-machine en voer het volgende adres in: **http://localhost:1977**.

   Opmerking: Wanneer de probe-manager en probe-gateway als afzonderlijke processen worden uitgevoerd, moet het adres op de machine waarop de probe-manager wordt uitgevoerd, als volgt worden ingevoerd: **http://localhost:1978**.

2. Klik op **type=CMClient** om de weergavepagina van JMX MBEAN te openen.
3. Zoek naar de methode **setLWSSOInitString** en geef dezelfde initreeks op die werd opgegeven voor de LW-SSO-configuratie van UCMDB.
4. Klik op de knop **setLWSSOInitString**.

Confidential Manager-communicatiecodering configureren op de probe

Deze procedure is relevant als de UCMDB-server is geconfigureerd om de configuratie en instellingen van LW-SSO/Confidential Manager niet automatisch naar probes te verzenden. Zie "Automatische synchronisatie van verificatie- en coderingsinstellingen van de Confidential Manager-client tussen de server en probes uitschakelen" op vorige pagina voor meer informatie over dit onderwerp.

1. Start de webbrowser op de probe-machine en voer het volgende adres in: **http://localhost:1977**.

   Opmerking: Wanneer de probe-manager en probe-gateway als afzonderlijke processen worden uitgevoerd, moet het adres op de machine waarop de probe-manager wordt uitgevoerd, als volgt worden ingevoerd: **http://localhost:1978**.

2. Klik op **type=CMClient** om de weergavepagina van JMX MBEAN te openen.
3. Werk de volgende transportgerelateerde instellingen bij:

   Opmerking: u moet dezelfde instellingen bijwerken die u hebt bijgewerkt op de UCMDB-server. Voor sommige methoden die u bijwerkt op de probe moet u mogelijk meerdere

parameters bijwerken. Klik op **displayTransportConfiguration** in de weergavepagina van JMX MBEAN om de huidige probe-configuratie te bekijken. Zie "Confidential Manager-communicatiecodering configureren " op pagina 47 voor meer informatie over dit onderwerp. Zie "Coderingsinstellingen van Confidential Manager" op pagina 60 voor meer informatie over de waarden die kunnen worden bijgewerkt.

a. **setTransportInitString** wijzigt de instelling **encryptDecryptInitString**.

b. **setTransportEncryptionAlgorithm** wijzigt Confidential Manager-instellingen op de probe op basis van het volgende overzicht:

   - **Engine name** verwijst naar het item <engineName>
   - **Key size** verwijst naar het item <keySize>
   - **Algorithm padding name** verwijst naar het item <algorithmPaddingName>
   - **PBE count** verwijst naar het item <pbeCount>
   - **PBE digest algorithm** verwijst naar het item <pbeDigestAlgorithm>

c. **setTransportEncryptionLibrary** wijzigt Confidential Manager-instellingen op de probe op basis van het volgende overzicht:

   - **Encryption Library name** verwijst naar het item <cryptoSource>
   - **Support previous lightweight cryptography versions** verwijst naar het item <lwJCEPBECompatibilityMode>

d. **setTransportMacDetails** wijzigt Confidential Manager-instellingen op de probe op basis van het volgende overzicht:

   - **Use MAC with cryptography** verwijst naar het item <useMacWithCrypto>
   - **MAC key size** verwijst naar het item <macKeySize>

4. Klik op de knop **reloadTransportConfiguration** om de wijzigingen door te voeren op de probe.

Zie "Coderingsinstellingen van Confidential Manager" op pagina 60 voor meer informatie over de verschillende instellingen en hun mogelijke waarden.

De cache van de Confidential Manager-client configureren

Deze taak omvat de onderstaande stappen:

- "De cachemodus van de Confidential Manager-client configureren op de probe" op volgende pagina
- "De instellingen voor cachecodering van de Confidential Manager-client configureren op de probe" op volgende pagina

De cachemodus van de Confidential Manager-client configureren op de probe

De Confidential Manager-client slaat referentiegegevens op in de cache en werkt deze bij wanneer informatie verandert op de server. De cache kan worden opgeslagen in het bestandssysteem of in het geheugen:

- **Wanneer de cache wordt opgeslagen in het bestandssysteem**, blijven de referentiegegevens beschikbaar, ook als de probe opnieuw wordt opgestart en geen verbinding kan maken met de server.
- **Wanneer de cache wordt opgeslagen in het geheugen**, wordt de cache leeggemaakt en wordt alle informatie weer van de server opgehaald wanneer de probe opnieuw wordt opgestart. Als de server niet beschikbaar is, bevat de probe geen referenties en kan dus geen discovery of integratie worden uitgevoerd.

Deze instelling wijzigen:

1. Open het bestand **DataFlowProbe.properties** in een teksteditor. Dit bestand bevindt zich in de map **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Zoek het volgende attribuut:
   com.hp.ucmdb.discovery.common.security.storeCMData=true
   - Als u de informatie wilt opslaan in het bestandssysteem, behoudt u de standaardinstelling (**true**).
   - Als u de informatie in het geheugen wilt opslaan, geeft u **false** op.
3. Sla het bestand **DataFlowProbe.properties** op.
4. Start de probe opnieuw op.

De instellingen voor cachecodering van de Confidential Manager-client configureren op de probe

Deze procedure beschrijft hoe u de coderingsinstellingen voor het cachebestand van het bestandssysteem van de Confidential Manager-client kunt wijzigen. Door de coderingsinstellingen voor de bestandssysteemcache van de Confidential Manager-client te wijzigen, wordt het cachebestand van het bestandssysteem opnieuw gemaakt. Hiervoor moet de probe opnieuw worden gestart en volledig worden gesynchroniseerd met de UCMDB-server.

1. Start de webbrowser op de probe-machine en voer het volgende adres in:
   http://localhost:1977.

   Opmerking: Wanneer de probe-manager en probe-gateway als afzonderlijke processen worden uitgevoerd, moet het adres op de machine waarop de probe-manager wordt uitgevoerd, als volgt worden ingevoerd: **http://localhost:1978**.
2. Klik op **type=CMClient** om de weergavepagina van JMX MBEAN te openen.

3. Werk de volgende cachegerelateerde instellingen bij:

   Opmerking: voor sommige methoden die u bijwerkt op de probe moet u mogelijk meerdere parameters instellen. Klik op **displayCacheConfiguration** in de weergavepagina van JMX MBEAN om de huidige probe-configuratie te bekijken.

   a. **setCacheInitString** wijzigt de instelling <encryptDecryptInitString> van de bestandssysteemcache.

   b. **setCacheEncryptionAlgorithm** wijzigt de instellingen van de bestandssysteemcache op basis van het volgende overzicht:

      - **Engine name** verwijst naar het item <engineName>
      - **Key size** verwijst naar het item <keySize>
      - **Algorithm padding name** verwijst naar het item <algorithmPaddingName>
      - **PBE count** verwijst naar het item <pbeCount>
      - **PBE digest algorithm** verwijst naar het item <pbeDigestAlgorithm>

   c. **setCacheEncryptionLibrary** wijzigt de instellingen van de bestandssysteemcache op basis van het volgende overzicht:

      - **Encryption Library name** verwijst naar het item <cryptoSource>
      - **Support previous lightweight cryptography versions** verwijst naar het item <lwJCEPBECompatibilityMode>

   d. **setCacheMacDetails** wijzigt de instellingen van de bestandssysteemcache op basis van het volgende overzicht:

      - **Use MAC with cryptography** verwijst naar het item <useMacWithCrypto>
      - **MAC key size** verwijst naar het item <macKeySize>

4. Klik op de knop **reloadCacheConfiguration** om de wijzigingen door te voeren op de probe. Hierdoor wordt de probe opnieuw opgestart.

   Opmerking: zorg ervoor dat er geen taken op de probe worden uitgevoerd tijdens deze actie.

Zie "Coderingsinstellingen van Confidential Manager" op pagina 60 voor meer informatie over de verschillende instellingen en hun mogelijke waarden.

Referentie- en bereikgegevens gecodeerd exporteren en importeren

U kunt referentie- en bereikgegevens gecodeerd exporteren en importeren om de referenties van de ene naar de andere UCMDB-server te kopiëren. Dit kan bijvoorbeeld aan de orde zijn bij herstelwerkzaamheden na een systeemcrash of tijdens een upgrade.

- **Bij het exporteren van referentiegegevens** moet u een (zelfgekozen) wachtwoord invoeren. De informatie wordt gecodeerd met dit wachtwoord.
- **Bij het importeren van referentiegegevens** moet u hetzelfde wachtwoord invoeren als voor het exporteren van het DSD-bestand.

Opmerking: Het geëxporteerde document met referenties bevat bereikgegevens die werden gedefinieerd op het systeem van waaruit het document werd geëxporteerd. Tijdens het importeren van het referentiesdocument worden ook de bereikgegevens geïmporteerd.

Let op: Als u referentiegegevens wilt importeren uit een domainScopeDocument van UCMDB versie 8.02, moet u het bestand key.bin van het versie 8.02-systeem gebruiken.

Referentiegegevens exporteren vanaf de UCMDB-server:

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console**. Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.
2. Klik op **UCMDB:service=DiscoveryManager** om de weergavepagina van JMX MBEAN te openen.
3. Zoek naar de bewerking **exportCredentialsAndRangesInformation**. Ga als volgt te werk:
   - Voer uw klant-ID in (de standaardwaarde is 1).
   - Voer een naam in voor het geëxporteerde bestand.
   - Voer uw wachtwoord in.
   - Stel **isEncrypted=True** in als het geëxporteerde bestand moet worden gecodeerd met het opgegeven wachtwoord, of stel **isEncrypted=False** in als u het geëxporteerde bestand niet wilt coderen (wachtwoorden en andere gevoelige gegevens worden niet geëxporteerd).
4. Klik op **Aanroepen** om te exporteren.

   Wanneer het exportproces succesvol wordt voltooid, wordt het bestand opgeslagen op de volgende locatie: **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

Referentiegegevens importeren vanaf de UCMDB-server:

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console**.

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.
2. Klik op **UCMDB:service=DiscoveryManager** om de weergavepagina van JMX MBEAN te openen.
3. Selecteer een van de onderstaande bewerkingen:
   - Zoek naar de bewerking **importCredentialsAndRangesInformation** als het bestand dat u importeert, werd geëxporteerd vanaf een UCMDB-server hoger dan versie 8.02.
   - Zoek naar de bewerking **importCredentialsAndRangesWithKey** als het bestand dat u importeert, werd geëxporteerd vanaf een UCMDB-server van versie 8.02.
4. Voer uw klant-ID in (de standaardwaarde is 1).

5. Voer de naam in van het bestand dat moet worden geïmporteerd. Dit bestand moet zich bevinden in **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.
6. Voer het wachtwoord in. Dit moet hetzelfde wachtwoord zijn dat werd gebruikt toen het bestand werd geëxporteerd.
7. Als het bestand werd geëxporteerd vanaf een UCMDB-systeem met versie 8.02, voert u de bestandsnaam **key.bin** in. Dit bestand moet zich bevinden in de map **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**, samen met het bestand dat moet worden geïmporteerd.
8. Klik op **Aanroepen** om de referenties te importeren.

Het niveau van logboekbestandberichten voor de Confidential Manager-client wijzigen

De probe biedt twee logboekbestanden die informatie bevatten met betrekking tot Confidential Manager-gerelateerde communicatie tussen de Confidential Manager-server en de Confidential Manager-client. Dit zijn de bestanden:

- "Logboekbestand Confidential Manager-client" beneden
- "Logboekbestand LW-SSO" beneden

Logboekbestand Confidential Manager-client

Het bestand **security.cm.log** bevindt zich in de map **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Het logboek bevat informatieberichten die werden uitgewisseld tussen de Confidential Manager-server en de Confidential Manager-client. Standaard is het logboekniveau van deze berichten ingesteld op INFO.

Het logboekniveau van de berichten wijzigen in DEBUG:

1. Navigeer op de Data Flow Probe Manager-server naar **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Open het bestand **security.properties** in een teksteditor.
3. Wijzig de volgende regel:

   ```
   loglevel.cm=INFO
   ```

   in:

   ```
   loglevel.cm=DEBUG
   ```

4. Sla het bestand op.

Logboekbestand LW-SSO

Het bestand **security.lwsso.log** bevindt zich in de map **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Het logboek bevat berichten die betrekking hebben op LW-SSO. Standaard is het logboekniveau van deze berichten ingesteld op INFO.

Het logboekniveau van de berichten wijzigen in DEBUG:

1. Navigeer op de Data Flow Probe Manager-server naar **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Open het bestand security.properties in een teksteditor.
3. Wijzig de volgende regel:

   `loglevel.lwsso=INFO`

   in:

   `loglevel.lwsso=DEBUG`
4. Sla het bestand op.

De coderingssleutel genereren of bijwerken

U kunt een coderingssleutel genereren of bijwerken die wordt gebruikt voor de codering of decodering van Confidential Manager-communicatie- en -verificatieconfiguraties die worden uitgewisseld tussen de UCMDB-server en de Data Flow-probe. In beide gevallen (genereren of bijwerken) maakt de UCMDB-server een nieuwe coderingssleutel gebaseerd op parameters die u verstrekt (bijvoorbeeld de sleutellengte, extra PBE-cycli, JCE-provider) en distribueert deze naar de probes.

Het resultaat van het uitvoeren van de methode **generateEncryptionKey** is een nieuw gegenereerde coderingssleutel. Deze sleutel wordt uitsluitend in beveiligde opslag opgeslagen en de datum en details zijn niet bekend. Als u een bestaande Data Flow-probe opnieuw installeert of een nieuwe probe verbindt met de UCMDB-server, wordt deze nieuw gegenereerde sleutel niet herkend door de nieuwe probe. In deze gevallen verdient het de voorkeur om de methode **changeEncryptionKey** te gebruiken voor het wijzigen van coderingssleutels. Wanneer u dan een probe opnieuw installeert of een nieuwe probe installeert, kunt u de bestaande sleutel (waarvan u de naam en locatie kent) importeren door de methode **importEncryptionKey** uit te voeren op de JMX-console van de probe.

Opmerking:

- Het verschil tussen de twee methoden die worden gebruikt om een sleutel te maken (**generateEncryptionKey**) en een sleutel bij te werken (**changeEncryptionKey**), is dat met **generateEncryptionKey** een nieuwe, willekeurige coderingssleutel wordt gemaakt terwijl met **changeEncryptionKey** een coderingssleutel met de door u opgegeven naam wordt geïmporteerd.
- Ongeacht het aantal geïnstalleerde probes kan slechts één coderingssleutel op een systeem aanwezig zijn.

Deze taak omvat de onderstaande stappen:

- "Een nieuwe coderingssleutel genereren" op volgende pagina
- "Een coderingssleutel bijwerken op een UCMDB-server" op pagina 58

Een nieuwe coderingssleutel genereren

U kunt een nieuwe sleutel genereren die door de UCMDB-server en de Data Flow-probe moet worden gebruikt voor codering of decodering. De UCMDB-server vervangt de oude sleutel door de nieuw gegenereerde sleutel en distribueert deze sleutel onder de probes.

Een nieuwe coderingssleutel genereren via de JMX-console:

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console**.

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

2. Klik op **UCMDB:service=DiscoveryManager** om de weergavepagina van JMX MBEAN te openen.

3. Zoek naar de bewerking generateEncryptionKey.

   a. Typ 1 (de standaardwaarde) in het parametervak **customerId**.

   b. Geef voor **keySize** de lengte op van de coderingssleutel. Geldige waarden zijn 128, 192 of 256.

   c. Geef **True** of **False** op voor **usePBE**:

      - **True:** extra PBE-hash-cycli gebruiken.
      - **False:**geen extra PBE-hash-cycli gebruiken.

   d. Voor **jceVendor** kunt u ervoor kiezen om een niet-standaard JCE-provider te gebruiken. Als het vak leeg is, wordt de standaardprovider gebruikt.

   e. Geef **True** of **False** op voor **autoUpdateProbe**:

      - **True:** de server distribueert de nieuwe sleutel automatisch naar de probes.
      - **False:** de nieuwe sleutel moet handmatig op de probes worden geplaatst.

   f. Geef **True** of **False** op voor **exportEncryptionKey**:

      - **True:** Naast het maken van het nieuwe wachtwoord en dit op te slaan in beveiligde opslag, exporteert de server het nieuwe wachtwoord naar het bestandssysteem (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Hierdoor kunt u probes handmatig bijwerken met het nieuwe wachtwoord.
      - **False:** het nieuwe wachtwoord wordt niet naar het bestandssysteem geëxporteerd. Als u probes handmatig wilt bijwerken, stelt u **autoUpdateProbe** in op False en **exportEncryptionKey** op True.

Opmerking: Zorg ervoor dat de probe actief is en verbonden is met de server. Als de probe wordt uitgeschakeld, kan de sleutel de probe niet bereiken. Als u de sleutel wijzigt voordat de probe wordt uitgeschakeld, wordt de sleutel opnieuw naar de probe verzonden als de probe weer actief is. Als u de sleutel echter meerdere malen hebt gewijzigd voordat de probe wordt uitgeschakeld, moet u de sleutel handmatig wijzigen via de JMX-console. (Selecteer **False** voor **exportEncryptionKey**).

4. Klik op **Aanroepen** om de coderingssleutel te genereren.

Een coderingssleutel bijwerken op een UCMDB-server

U gebruikt de methode **changeEncryptionKey** om uw eigen coderingssleutel te importeren naar de UCMDB-server en deze onder de probes te distribueren.

Een coderingssleutel bijwerken via de JMX-console:

1. Start de webbrowser op de UCMDB-server en voer het volgende adres in: **http://localhost:8080/jmx-console.**

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

2. Klik op **UCMDB:service=DiscoveryManager** om de weergavepagina van JMX MBEAN te openen.

3. Zoek naar de bewerking **changeEncryptionKey**.

   a. Typ **1** in het parametervak **customerId**.

   b. Geef voor **newKeyFileName** de naam op van de nieuwe coderingssleutel.

   c. Geef voor **keySizeInBits** de lengte op van de coderingssleutel. Geldige waarden zijn 128, 192 of 256.

   d. Geef **True** of **False** op voor **usePBE**:

      - **True:** extra PBE-hash-cycli gebruiken.
      - **False:**geen extra PBE-hash-cycli gebruiken.

   e. Voor **jceVendor** kunt u ervoor kiezen om een niet-standaard JCE-provider te gebruiken. Als het vak leeg is, wordt de standaardprovider gebruikt.

   f. Geef **True** of **False** op voor **autoUpdateProbe**:

      - **True:** de server distribueert de nieuwe sleutel automatisch naar de probes.
      - **False:** de nieuwe sleutel moet handmatig worden gedistribueerd via de JMX-console van de probe.

> **Opmerking:** Zorg ervoor dat de probe actief is en verbonden is met de server. Als de probe wordt uitgeschakeld, kan de sleutel de probe niet bereiken. Als u de sleutel wijzigt voordat de probe wordt uitgeschakeld, wordt de sleutel opnieuw naar de probe verzonden als de probe weer actief is. Als u de sleutel echter meerdere malen hebt gewijzigd voordat de probe wordt uitgeschakeld, moet u de sleutel handmatig wijzigen via de JMX-console. (Selecteer **False** voor **autoUpdateProbe**).

4. Klik op **Aanroepen** om de coderingssleutel te genereren en bij te werken.

Een coderingssleutel bijwerken op een probe

Als u ervoor kiest om een coderingssleutel niet automatisch van de UCMDB-server naar alle probes te distribueren (om veiligheidsredenen), moet u de nieuwe coderingssleutel downloaden naar alle probes en de methode **importEncryptionKey** uitvoeren op de probe:

1. Plaats het bestand met de coderingssleutel in de map **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. Start de webbrowser op de probe-machine en voer het volgende adres in: **http://localhost:1977**.

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

   > **Opmerking:** Wanneer de probe-manager en probe-gateway als afzonderlijke processen worden uitgevoerd, moet het adres op de machine waarop de probe-manager wordt uitgevoerd, als volgt worden ingevoerd: **http://localhost:1978**.

3. Klik in het probe-domein op **type=SecurityManagerService**.
4. Zoek naar de methode **importEncryptionKey**.
5. Voer de naam in van het coderingssleutelbestand in **C:\hp\UCMDB\DataFlowProbe\conf\security**. Dit bestand bevat de sleutel die moet worden geïmplementeerd.
6. Klik op de knop **importEncryptionKey**.
7. Start de probe opnieuw.

De coderingssleutel handmatig wijzigen wanneer de probe-manager en de probe-gateway op afzonderlijke machines zijn geïnstalleerd

1. Start de probe-managerservice op de probe-managermachine (**Start > Programma's > HP UCMDB > Probe-manager**).

2. Importeer de sleutel van de server met behulp van de JMX-console van de probe-manager. Zie "Een nieuwe coderingssleutel genereren" op pagina 57 voor meer informatie over dit onderwerp.
3. Nadat de coderingssleutel is geïmporteerd, start u de probe-manager- en probe-gatewayservice opnieuw.

Meerdere JCE-providers definiëren

Wanneer u een coderingssleutel genereert via de JMX-console, kunt u meerdere JCE-providers definiëren via de methoden **changeEncryptionKey** en **generateEncryptionKey**.

De standaard JCE-provider wijzigen:

1. Registreer de JAR-bestanden van de JCE-provider in **$JRE_HOME/lib/ext**.
2. Kopieer de JAR-bestanden naar de map $JRE_HOME:
   - Voor de UCMDB-server: $JRE_HOME bevindt zich op: **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - Voor de Data Flow-probe: $JRE_HOME bevindt zich op: **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Voeg de providerklasse toe aan het einde van de providerlijst in het bestand **$JRE_HOME\lib\security\java.security**.
4. Update de bestanden **local_policy.jar** en **US_export_policy.jar** zodat deze onbeperkt JCE-beleid bevatten. U kunt deze JAR-bestanden downloaden van de Sun-website.
5. Start de UCMDB-server en de Data Flow-probe opnieuw op.
6. Zoek het JCE-leverancierveld voor de methode **changeEncryptionKey** of **generateEncryptionKey** en voeg de naam van de JCE-provider toe.

Coderingsinstellingen van Confidential Manager

Deze tabel biedt een overzicht van de coderingsinstellingen die kunnen worden gewijzigd via de verschillende JMX-methoden. Deze coderingsinstellingen zijn relevant voor de codering van communicatie tussen de Confidential Manager-client en de Confidential Manager-server, alsmede voor de codering van de cache van de Confidential Manager-client.

Instelling Confidential Manager	Instelling Confidenti-al Manager - Probe	Beschrijving instelling	Mogelijke waarden	Standaardwaar-de
cryptoSource	Encryption Library name	Deze instelling definieert de coderingsbibliotheek die moet worden gebruikt.	lw, jce, windowsDPAPI, lwJCECompatib-le	lw

Instelling Confidential Manager	Instelling Confidenti-al Manager - Probe	Beschrijving instelling	Mogelijke waarden	Standaardwaar-de
lwJCEPBE Compatibiliteit-s-Modus	Support previous lightweight cryptograph-y versions	Deze instelling definieert of eerdere lichte cryptografie moet worden ondersteund of niet.	true, false	true
engineName	Engine name	Naam coderingsmechanisme	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Lengte van coderingssleutel in bits	Voor AES - 128, 192 of 256; Voor DES - 64; Voor 3DES - 192; Voor Blowfish - elk getal tussen 32 en 448	256
algorithm Opvullings-Naam	Algorithm padding name	Standaarden opvullingsalgoritme	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE count	Het aantal keren dat de hash moet worden uitgevoerd om de sleutel te maken op basis van het wachtwoord (initreeks)	Een positief getal	20
pbeDigest Algoritme	PBE digest algorithm	Hash-type	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Use MAC with cryptograph-y	Geeft aan of MAC met cryptografie moet worden gebruikt	true, false	false
macKeySize	MAC key size	Afhankelijk van MAC-algoritme	256	256

Probleemoplossing en beperkingen

Als u de standaarddomeinnaam op de UCMDB-server wijzigt, controleert u eerst of de Data Flow Probe niet wordt uitgevoerd. Nadat de standaard domeinnaam is toegepast, moet u het script **DataFlowProbe\tools\clearProbeData.bat** starten vanaf Data Flow Probe.

Opmerking: Door het script clearProbeData.bat uit te voeren, ontstaat er een detectiecyclus aan de kant van de probe zodra deze is gestart.

Hoofdstuk 5

Beveiliging Data Flow-probe

In dit hoofdstuk vindt u de volgende informatie:

Het gecodeerde wachtwoord voor de MySQL-database wijzigen

In dit gedeelte wordt beschreven hoe u het gecodeerde wachtwoord voor de MySQL-databasegebruiker kunt wijzigen.

1. Maak de gecodeerde vorm van een wachtwoord (AES, 192-bits sleutel)
   a. Open de JMX-console voor de Data Flow-probe. Open een webbrowser en voer het volgende adres in: **http://<naam of IP-adres Data Flow probe-machine>:1977**. Als u de Data Flow-probe lokaal uitvoert, voert u **http://localhost:1977** in.

      Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

> **Opmerking:** Als u nog geen gebruiker hebt aangemaakt, gebruikt u de standaardgebruikersnaam sysadmin en het standaardwachtwoord sysadmin om u aan te melden.

b. Zoek de **Type=MainProbe**-service en klik op de koppeling om de pagina Bewerkingen te openen.

c. Zoek naar de bewerking **getEncryptedDBPassword**.

d. Voer in het veld **Databasewachtwoord** het wachtwoord in dat moet worden gecodeerd.

e. Klik op de knop **getEncryptedDBPassword** om de bewerking aan te roepen.

Het resultaat van het aanroepen is een gecodeerde wachtwoordreeks, bijvoorbeeld:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,
112,65,61,61
```

2. Stop de Data Flow-probe

Start > Alle programma's > HP UCMDB > Data Flow-probe stoppen

3. Voer het script set_dbuser_password.cmd uit

Dit script bevindt zich in de volgende map:
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd

Voer het script **set_dbuser_password.cmd** uit met het nieuwe wachtwoord als eerste argument en het wachtwoord voor het MySQL-hoofdaccount als tweede argument (of laat dit leeg als het MySQL-hoofdaccount niet met een wachtwoord wordt beschermd).

Bijvoorbeeld:

set_dbuser_password <mijn_wachtwoord><wachtwoord_hoofdaccount>.

Het wachtwoord moet worden ingevoerd in niet-gecodeerde vorm (gewone tekst).

4. Werk het wachtwoord bij in de configuratiebestanden van de Data Flow-probe

a. Het wachtwoord moet gecodeerd in de configuratiebestanden aanwezig zijn. U haalt de gecodeerde vorm van het wachtwoord op met behulp van de JMX-methode **getEncryptedDBPassword**, zoals uitgelegd in stap 1.

b. Voeg het gecodeerde wachtwoord toe aan de volgende eigenschappen in het bestand **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

- **appilog.agent.probe.jdbc.pwd**

  Bijvoorbeeld:

  ```
  appilog.agent.probe.jdbc.user = mamprobe
  appilog.agent.probe.jdbc.pwd =
  66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,
  114,112,65,61,61
  ```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Start de Data Flow-probe

Start > Alle programma's > HP UCMDB > Data Flow Probe starten.

Het script clearProbeData.bat gebruiken

Met het script **clearProbeData.bat** wordt de databasegebruiker opnieuw gemaakt zonder het huidige wachtwoord te wijzigen.

Het script verwacht het wachtwoord van het MySQL-hoofdaccount als eerste argument te ontvangen. Als er geen parameters worden overgebracht, neemt het script aan dat het wachtwoord voor het MySQL-hoofdaccount leeg is.

Na uitvoering van het script:

- Controleer het bestand op de volgende fouten:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log
- Verwijder het volgende bestand, omdat dit het databasewachtwoord bevat:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

Het gecodeerde wachtwoord voor de JMX-console

In dit gedeelte wordt beschreven hoe u het wachtwoord voor de JMX-gebruiker kunt coderen. Het gecodeerde wachtwoord wordt opgeslagen in het bestand DataFlowProbe.properties. Gebruikers moeten zich aanmelden voor toegang tot de JMX-console.

1. **Maak de gecodeerde vorm van een wachtwoord (AES, 192-bits sleutel)**

   a. Open de JMX-console voor de Data Flow-probe. Open een webbrowser en voer het volgende adres in: **http://<naam of IP-adres Data Flow probe-machine>:1977**. Als u de Data Flow-probe lokaal uitvoert, voert u **http://localhost:1977** in.

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

   > **Opmerking:** Als u nog geen gebruiker hebt aangemaakt, gebruikt u de standaardgebruikersnaam sysadmin en het standaardwachtwoord sysadmin om u aan te melden.

   b. Zoek de **Type=MainProbe**-service en klik op de koppeling om de pagina Bewerkingen te openen.

   c. Zoek naar de bewerking **getEncryptedKeyPassword**.

   d. Voer in het veld **Sleutelwachtwoord** het wachtwoord in dat moet worden gecodeerd.

   e. Klik op de knop **getEncryptedKeyPassword** om de bewerking aan te roepen.

   Het resultaat van het aanroepen is een gecodeerde wachtwoordreeks, bijvoorbeeld:

   ```
   85,-9,-61,11,105,-93,-81,118
   ```

2. **Stop de Data Flow-probe**

   Start > Alle programma's > HP UCMDB > Data Flow-probe stoppen

3. **Voeg het gecodeerde wachtwoord toe**

   Voeg het gecodeerde wachtwoord toe aan de volgende eigenschap in het bestand **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Bijvoorbeeld:

   ```
   appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
   appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,
   38,80,-111,-99,-64,-5,35,-122
   ```

   Opmerking: laat deze velden leeg als u verificatie wilt uitschakelen. In dat geval kunnen gebruikers de hoofdpagina van de JMX-console van de probe openen zonder referenties in te voeren.

4. **Start de Data Flow-probe**

   Start >Alle programma's > HP UCMDB > Data Flow Probe starten

   Test het resultaat in een webbrowser.

Het wachtwoord voor UpLoadScanFile instellen

In deze sectie wordt uitgelegd hoe u het wachtwoord instelt voor **UpLoadScanFile**, dat wordt gebruikt voor het offsite opslaan van scans. Het gecodeerde wachtwoord wordt opgeslagen in het bestand **DataFlowProbe.properties**. Gebruikers moeten zich aanmelden voor toegang tot de JMX-console.

1. **Maak de gecodeerde vorm van een wachtwoord (AES, 192-bits sleutel)**

   a. Open de JMX-console voor de Data Flow-probe. Open een webbrowser en voer het volgende adres in: **http://<naam of IP-adres Data Flow probe-machine>:1977**. Als u de Data Flow-probe lokaal uitvoert, voert u **http://localhost:1977** in.

      Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

      Opmerking: Als u nog geen gebruiker hebt aangemaakt, gebruikt u de standaardgebruikersnaam sysadmin en het standaardwachtwoord sysadmin om u aan te melden.

   b. Zoek de **Type=MainProbe**-service en klik op de koppeling om de pagina Bewerkingen te openen.

   c. Zoek naar de bewerking **getEncryptedKeyPassword**.

   d. Voer in het veld **Sleutelwachtwoord** het wachtwoord in dat moet worden gecodeerd.

   e. Klik op de knop **getEncryptedKeyPassword** om de bewerking aan te roepen.

      Het resultaat van het aanroepen is een gecodeerde wachtwoordreeks, bijvoorbeeld:

      ```
      85,-9,-61,11,105,-93,-81,118
      ```

2. **Stop de Data Flow-probe**

   Start > Alle programma's > HP UCMDB > Data Flow-probe stoppen

3. **Voeg het gecodeerde wachtwoord toe**

   Voeg het gecodeerde wachtwoord toe aan de volgende eigenschap in het bestand **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Bijvoorbeeld:

   ```
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,
   77,-108,14,127,4,-89,101,-33,-31,116,53
   ```

4. **Start de Data Flow-probe**

   Start >Alle programma's > HP UCMDB > Data Flow Probe starten

   Test het resultaat in een webbrowser.

Externe toegang tot de MySQL-server

In deze sectie wordt uitgelegd hoe u toegang tot het account van de MySQL Data Flow-probe vanaf externe machines verleent/beperkt.

Opmerking:

- Standaard is de toegang beperkt.
- U kunt vanaf externe machines geen toegang krijgen tot het MySQL-hoofdaccount.

Toegang tot MySQL toestaan:

1. Voer het volgende script uit in een opdrachtpromptvenster:

   C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd

2. Wanneer u hierom wordt gevraagd, voert u het wachtwoord voor het MySQL-hoofdaccount in als eerste argument (dit wachtwoord is hetzelfde als het wachtwoord dat u hebt ingevoerd tijdens de installatie van de probe).

Toegang tot MySQL beperken:

1. Voer het volgende script uit in een opdrachtpromptvenster:

   C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd

2. Wanneer u hierom wordt gevraagd, voert u het wachtwoord voor het MySQL-hoofdaccount in als eerste argument (dit wachtwoord is hetzelfde als het wachtwoord dat u hebt ingevoerd tijdens de installatie van de probe).

SSL met wederzijdse verificatie tussen de UCMDB-server en Data Flow-probe inschakelen

U kunt verificatie voor zowel de Data Flow-probe als de UCMDB-server instellen met certificaten. Het certificaat voor elke component wordt verzonden en geverifieerd voordat de verbinding tot stand wordt gebracht.

Opmerking: De volgende methode voor het inschakelen van SSL met wederzijdse verificatie op de Data Flow-probe, is de veiligste methode en derhalve de aanbevolen communicatiemodus. Deze methode vervangt de procedure voor basisverificatie.

In dit gedeelte vindt u de volgende onderwerpen:

Overzicht

UCMDB ondersteunt de volgende communicatiemodi tussen de UCMDB-server en de Data Flow-probe:

- **Serververificatie.** Deze modus gebruikt SSL en de probe verifieert het UCMDB-servercertificaat. Zie "SSL met serververificatie inschakelen (1 richting)" op volgende pagina voor meer informatie over dit onderwerp.
- **Wederzijdse verificatie.** Deze modus gebruikt SSL en maakt zowel serververificatie door de probe als clientverificatie door de server mogelijk. Zie "(Tweerichtings) certificaatverificatie inschakelen" op pagina 71 voor meer informatie over dit onderwerp.
- **Standaard-HTTP.** Geen SSL-communicatie. Dit is de standaardmodus en de Data Flow Probe-component in UCMDB vereist geen certificaten. De Data Flow-probe communiceert met de server via het standaard-HTTP-protocol.

Opmerking: Discovery kan geen certificaatketens gebruiken wanneer u werkt met SSL. Als u certificaatketens gebruikt, moet u daarom een zelfondertekend certificaat genereren om de Data Flow-probe te laten communiceren met de UCMDB-server.

Keystores en truststores

De UCMDB-server en de Data Flow-probe werken met keystores en truststores:

- **Keystore.** Een bestand met sleutelvermeldingen (een certificaat en bijbehorende persoonlijke sleutel).
- **Truststore.** Een bestand met certificaten die worden gebruikt voor verificatie van een externe host (wanneer bijvoorbeeld serververificatie wordt gebruikt, moet de truststore van de Data Flow-probe het UCMDB-servercertificaat bevatten).

Beperking wederzijdse verificatie

De keystore van de Data Flow-probe (zoals gedefinieerd in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) mag slechts 1 (één) sleutelvermelding bevatten.

SSL met serververificatie inschakelen (1 richting)

Hierbij wordt SSL gebruikt en de probe verifieert het servercertificaat.

Deze taak omvat het volgende:

- "Vereisten" beneden
- "Configuratie UCMDB-server" beneden
- "Data Flow-probe configureren" op pagina 71
- "De machines opnieuw starten" op pagina 71

Vereisten

1. Controleer of zowel de UCMDB als de Data Flow-probe actief is.

   Opmerking: Als de probe in de afzonderlijke modus is geïnstalleerd, zijn deze instructies van toepassing op de probe-gateway.

2. Als UCMDB of de Data Flow-probe niet geïnstalleerd is in de standaardmappen, noteert u de correcte locatie en wijzigt u de opdrachten.

Configuratie UCMDB-server

1. **Het UCMDB-certificaat exporteren**

   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore-alias> -keystore <locatie Keystore-bestand> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   waarbij:

   - **keystore-alias** de naam is die aan de keystore is gegeven.
   - **bestandslocatie Keystore** het volledige pad is naar de locatie van het keystore-bestand.

   Gebruik voor de kant-en-klare server.keystore bijvoorbeeld de volgende opdracht:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -
alias hpcert -keystore
C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

b. Voer het keystore-wachtwoord in. Het wachtwoord van de kant-en-klare keystore is bijvoorbeeld **hppass**.

c. Controleer of het certificaat is gemaakt in de volgende map: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **De Data Flow-probe-connector beveiligen in UCMDB**

a. Open de JMX-console van UCMDB. Typ in de webbrowser de volgende URL: **http://<naam of IP-adres van UCMDB-machine>:8080/jmx-console**. Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

b. Selecteer de service: **Ports Management Services**.

c. Roep de methode **PortsDetails** aan en noteer het poortnummer voor HTTPS. (Standaard: 8443) Zorg ervoor dat de waarde in de kolom **Is Enabled** is ingesteld op **True**.

d. Ga terug naar **Ports Management Services**.

e. Als u de Data Flow-probe-connector wilt toewijzen aan de modus voor serververificatie, roept u de methode **mapComponentToConnectors** aan met de volgende parameters:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Alle andere vlaggen**: false

Het volgende bericht wordt weergegeven:

Bewerking geslaagd. Component mam-collectors is nu toegewezen aan: HTTPS-poorten.

f. Ga terug naar **Ports Management Services**.

g. Als u de Confidential Manager-connector wilt toewijzen aan de modus voor serververificatie, roept u de methode **mapComponentToConnectors** aan met de volgende parameters:

- **componentName**: cm
- **isHTTPS**: true
- **Alle andere vlaggen**: false

Het volgende bericht wordt weergegeven:

Bewerking geslaagd. Component cm is nu toegewezen aan: HTTPS-poorten.

3. **Het UCMDB-certificaat kopiëren naar elke probe-machine**

Kopieer het certificaatbestand **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** op de UCMDB-servermachine naar de volgende map op elke Data Flow-probe-machine **C:\HP\UCMDB\DataFlowProbe\conf\security**

Data Flow-probe configureren

Opmerking: U moet elke Data Flow-probe-machine configureren.

1. **Importeer het bestand server.cert dat is gemaakt in** "Het UCMDB-certificaat exporteren" op pagina 69 **naar de truststore van de probe.**
   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -
   keystore
   C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -
   file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias
   ucmdbcert
   ```

   b. Voer het keystore-wachtwoord in: logomania
   c. Wanneer wordtgevraagd of het certificaat moet worden vertrouwd, drukt u op **j** en vervolgens op **Enter**.

   Het volgende bericht wordt weergegeven:

   Certificaat is toegevoegd aan keystore.

2. **Open het bestand DiscoveryProbe.properties dat zich bevindt in: C:\HP\UCMDB\DataFlowProbe\conf**
   a. Werk de eigenschap **appilog.agent.probe.protocol** bij naar **HTTPS**.
   b. Werk de eigenschap **serverPortHttps** bij naar het relevante poortnummer. (Gebruik het poortnummer uit stap 2c van "Configuratie UCMDB-server" op pagina 69.)

De machines opnieuw starten

Start de UCMDB-server en de probe-machines opnieuw.

(Tweerichtings) certificaatverificatie inschakelen

Deze modus gebruikt SSL en maakt zowel serververificatie door de probe als clientverificatie door de server mogelijk. Zowel de server als de probe probeert een certificaat naar de andere entiteit te sturen ter verificatie.

Deze taak omvat het volgende:

- "Vereisten" op volgende pagina
- "Eerste configuratie UCMDB-server" op volgende pagina
- "Data Flow-probe configureren" op pagina 73

- "Verdere configuratie van UCMDB-server" op pagina 75
- "De machines opnieuw starten" op pagina 76

Vereisten

1. Controleer of zowel de UCMDB als de Data Flow-probe actief is.

   Opmerking: Als de probe in de afzonderlijke modus is geïnstalleerd, zijn deze instructies van toepassing op de probe-gateway.

2. Als UCMDB of de Data Flow-probe niet geïnstalleerd is in de standaardmappen, noteert u de correcte locatie en wijzigt u de opdrachten.

Eerste configuratie UCMDB-server

1. **Het UCMDB-certificaat exporteren**

   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore-alias> -keystore <locatie Keystore-bestand> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   waarbij:

   - **keystore-alias** de naam is die aan de keystore is gegeven.
   - **bestandslocatie Keystore** het volledige pad is naar de locatie van het keystore-bestand.

   Gebruik voor de kant-en-klare server.keystore bijvoorbeeld de volgende opdracht:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -
   alias hpcert -keystore
   C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Voer het keystore-wachtwoord in. Het wachtwoord van de kant-en-klare keystore is bijvoorbeeld **hppass**.

   c. Controleer of het certificaat is gemaakt in de volgende map: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **De Data Flow-probe-connector beveiligen in UCMDB**

   a. Open de JMX-console van UCMDB. Typ in de webbrowser de volgende URL: **http://<naam of IP-adres van UCMDB-machine>:8080/jmx-console**. Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

   b. Selecteer de service: **Ports Management Services**.

   c. Roep de methode **PortsDetails** aan en noteer het poortnummer voor HTTPS met clientverificatie. (Standaard: 8444) Zorg ervoor dat de waarde in de kolom **Is Enabled** is ingesteld op **True**.

   d. Ga terug naar **Ports Management Services**.

e. Als u de Data Flow-probe-connector wilt toewijzen aan de modus voor wederzijdse verificatie, roept u de methode **mapComponentToConnectors** aan met de volgende parameters:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Alle andere vlaggen**: false

Het volgende bericht wordt weergegeven:

Bewerking geslaagd. Component mam-collectors is nu toegewezen aan: HTTPS_CLIENT_AUTH-poorten.

f. Ga terug naar **Ports Management Services**.

g. Als u de Confidential Manager-connector wilt toewijzen aan de modus voor wederzijdse verificatie, roept u de methode **mapComponentToConnectors** aan met de volgende parameters:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Alle andere vlaggen**: false

Het volgende bericht wordt weergegeven:

Bewerking geslaagd. Component cm is nu toegewezen aan: HTTPS_CLIENT_AUTH-poorten.

3. **Het UCMDB-certificaat kopiëren naar elke probe-machine**

Kopieer het certificaatbestand **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** op de UCMDB-servermachine naar de volgende map op elke Data Flow-probe-machine: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Data Flow-probe configureren

Opmerking: U moet elke Data Flow-probe-machine configureren.

1. **Importeer het bestand server.cert dat is gemaakt in** "Het UCMDB-certificaat exporteren" op vorige pagina **naar de truststore van de probe.**

a. Open de opdrachtprompt en voer de volgende opdracht uit:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore
C:\HP\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias ucmdbcert
```

b. Voer het keystore-wachtwoord in: logomania

c. Wanneer wordtgevraagd of het certificaat moet worden vertrouwd, drukt u op **j** en

vervolgens op **Enter**.

Het volgende bericht wordt weergegeven:

Certificaat is toegevoegd aan keystore.

2. **Een nieuw bestand client.keystore maken**

   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
   <ProbeName> -keyalg RSA -keystore
   C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
   ```

   waarbij **ProbeName** de unieke alias is van de Data Flow-probe.

   Opmerking: Om ervoor te zorgen dat deze alias uniek is, gebruikt u de Probe-ID die is toegekend aan de probe tijdens het definiëren van de probe.

   b. Typ het wachtwoord voor de keystore (minimaal 6 tekens) en noteer dit.

   c. Typ het wachtwoord nogmaals ter bevestiging.

   d. Druk op **Enter** om elk van de volgende vragen te beantwoorden:

   Wat zijn uw voornaam en achternaam? [Unknown]:

   Wat is de naam van uw eenheid in de organisatie?[Unknown]:

   Wat is de naam van uw organisatie?[Unknown]:

   Wat is de naam van uw plaats of gemeente?[Unknown]:

   Wat is de naam van uw provincie of staat?[Unknown]:

   Wat is de landcode van twee letters voor deze eenheid?[Unknown]:

   e. Typ **yes** wanneer u het volgende wordt gevraagd: **Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?**

   f. Druk op **Enter** om de volgende vraag te beantwoorden:

   Typ het sleutelwachtwoord voor <probekey> (RETURN als dit hetzelfde is als het keystore-wachtwoord):

   g. Controleer of het bestand is gemaakt in de volgende map en of de bestandsgrootte groter is dan 0: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Het nieuwe clientcertificaat exporteren**

   a. Open de opdrachtprompt en voer de volgende opdracht uit:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias
   <ProbeName> -keystore
   C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file
   C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert
   ```

   b. Voer het keystore-wachtwoord in wanneer dit wordt gevraagd. (Het wachtwoord uit

bovenstaande stap 2b.)

Het volgende bericht wordt weergegeven:

Certificaat opgeslagen in bestand <C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert>

4. **Open het bestand DiscoveryProbe.properties dat zich bevindt in: C:\HP\UCMDB\DataFlowProbe\conf**
   a. Werk de eigenschap **appilog.agent.probe.protocol** bij naar **HTTPS**.
   b. Werk de eigenschap **serverPortHttps** bij naar het relevante poortnummer. (Gebruik het poortnummer uit stap 2c van "Eerste configuratie UCMDB-server" op pagina 72.)
5. **Open het bestand ssl.properties dat zich bevindt in: C:\HP\UCMDB\DataFlowProbe\conf\security**
   a. Werk de eigenschap **javax.net.ssl.keyStore** bij naar **client.keystore**.
   b. Codeer het wachtwoord uit bovenstaande stap 2b:
      i. Start de Data Flow-probe (of controleer of deze al wordt uitgevoerd).
      ii. Open de probe-JMX. Ga naar: **http://<probe-hostnaam>:1977**

      Als de probe lokaal wordt uitgevoerd, gaat u bijvoorbeeld naar: **http://localhost:1977**.
      iii. Druk op de koppeling **type=MainProbe**.
      iv. Schuif omlaag naar de bewerking **getEncryptedKeyPassword**.
      v. Typ het wachtwoord in het veld **Sleutelwachtwoord**.
      vi. Klik op de knop **getEncryptedKeyPassword**.
   c. Kopieer en plak het gecodeerde wachtwoord om de eigenschap **javax.net.ssl.keyStorePassword** bij te werken.

   Opmerking: Nummers worden van elkaar gescheiden met komma's. Bijvoorbeeld: -20,50,34,-40,-50.)
6. **Het probe-certificaat kopiëren naar de UMCDB-machine**

   Kopieer het bestand **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** van de Data Flow-probe-machine naar de UCMDB-machine in **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert**.

Verdere configuratie van UCMDB-server

1. **Elk probe-certificaat toevoegen aan de truststore van UCMDB**

   Opmerking: Voer voor elk probe-certificaat de volgende stappen uit.

a. Open de opdrachtprompt en voer de volgende opdracht uit:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -
keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore
-file C:\hp\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert -
alias <ProbeName>
```

b. Voer het keystore-wachtwoord in. Het wachtwoord van de kant-en-klare keystore is bijvoorbeeld **hppass**.

c. Wanneer wordtgevraagd of het certificaat moet worden vertrouwd, drukt u op **j** en vervolgens op **Enter**.

Het volgende bericht wordt weergegeven:

Certificaat is toegevoegd aan keystore

De machines opnieuw starten

Start de UCMDB-server en de probe-machines opnieuw.

De locatie van het bestand domainScopeDocument beheren

Het bestandssysteem van de probe bevat (standaard) zowel de coderingssleutel als het bestand **domainScopeDocument**. Elke keer wanneer de probe wordt gestart, haalt de probe het bestand **domainScopeDocument** op van de server en slaat het dit op in het eigen bestandssysteem. Ten einde te voorkomen dat niet-geautoriseerde gebruikers deze referenties kunnen ophalen, kunt u de probe zodanig configureren dat het bestand **domainScopeDocument** in het geheugen van de probe wordt opgeslagen en niet in het bestandssysteem van de probe.

De locatie van het bestand domainScopeDocument beheren:

1. Open **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** en wijzig het volgende:

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   in:

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   Het bestand **domainScopeDocument** is niet meer aanwezig in de serverData-mappen van de probe-gateway en probe-manager.

   Zie "Beheer van Data Flow-referenties" op pagina 42 voor meer informatie over het gebruik van het bestand **domainScopeDocument** om DFM te beveiligen.

2. Start de probe opnieuw op.

Een keystore maken voor de Data Flow-probe

1. Voer de volgende opdracht uit op de probe-machine:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool -genkey -alias
   probekey -keyalg RSA -keystore
   C:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
   ```

2. Voer een wachtwoord in voor de nieuwe keystore.
3. Voer desgevraagd uw gegevens in.
4. Wanneer wordt gevraagd **Is CN=… C=… Correct?**, antwoordt u **ja** en drukt u op **Enter**.
5. Druk opnieuw op **Enter** om het keystore-wachtwoord te accepteren als het sleutelwachtwoord.
6. Controleer of **client.keystore** is gemaakt in de volgende map: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Wachtwoorden voor de probe-keystore en probe-truststore coderen

De wachtwoorden voor de probe-keystore en probe-truststore worden gecodeerd opgeslagen in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Deze procedure laat zien hoe u het wachtwoord kunt coderen.

1. Start Data Flow Probe (of controleer of het programma al wordt uitgevoerd).
2. Open de JMX-console van de Data Flow-probe: Open een webbrowser en voer het volgende adres in: http://<machinenaam of IP-adres van Data Flow-probe>:1977. Als u de Data Flow-probe lokaal uitvoert, voert u http://localhost:1977 in.

   Opmerking: Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord. Als u nog geen gebruiker hebt aangemaakt, gebruikt u de standaardgebruikersnaam sysadmin en het standaardwachtwoord sysadmin om u aan te melden.

3. Zoek de **Type=MainProbe**-service en klik op de koppeling om de pagina Bewerkingen te openen.
4. Zoek naar de bewerking **getEncryptedKeyPassword**.
5. Voer in het veld **Sleutelwachtwoord** uw keystore- of truststore-wachtwoord in en roep de bewerking aan door te klikken op **getEncryptedKeyPassword**.
6. Het resultaat van het aanroepen is een gecodeerde wachtwoordreeks, bijvoorbeeld:

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,
   112,65,61,61
   ```

7. Kopieer en plak het gecodeerde wachtwoord op de regel voor de keystore of de truststore in het volgende bestand: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

Standaardkeystore en -truststore voor server en Data Flow-probe

In dit gedeelte vindt u de volgende onderwerpen:

UCMDB-server

De bestanden bevinden zich in de volgende map: **C:\HP\UCMDB\UCMDBServer\conf\security.**

Entiteit	Bestandsnaam/Term	Wachtwoord/Term	Alias
Server-keystore	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Server-truststore	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (standaard vertrouwde invoer)
Client-keystore	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow-probe

De bestanden bevinden zich in de volgende map: **C:\HP\UCMDB\DataFlowProbe\conf\security.**

Entiteit	Bestandsnaam/Term	Wachtwoord/Term	Alias
Probe-keystore	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Data Flow Probe gebruikt de **cKeyStoreFile**-keystore als de standaard keystore tijdens de pocedure voor wederzijdse verificatie. Dit is een client-keystore die deel uitmaakt van de UCMDB-installatie.			
Probe-truststore	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (standaard vertrouwde invoer)
Het **cKeyStorePass**-wachtwoord is het standaardwachtwoord van **cKeyStoreFile**.			

Hoofdstuk 6

Lightweight Single Sign-On Authentication (LW-SSO) – Algemene leidraad

In dit hoofdstuk vindt u de volgende informatie:

Overzicht LW-SSO-verificatie

LW-SSO is een methode voor toegangscontrole waarmee de gebruiker zich één keer kan aanmelden om toegang te krijgen tot de bronnen van meerdere softwaresystemen zonder dat hem wordt gevraagd om zich opnieuw aan te melden. De applicaties 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.

- **Verloop van het LW-SSO-token**

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

- **Aanbevolen configuratie van de verlooptijd van het LW-SSO-token**

  Voor elke applicatie die gebruikmaakt van LW-SSO moet tokenverloop geconfigureerd zijn. De aanbevolen waarde is 60 minuten. Voor een applicatie 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 applicaties 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.

Systeemvereisten LW-SSO

Applicatie	Versie	Opmerkingen
Java	1.5 en later	
HTTP Servlets API	2.1 en later	
Internet Explorer	6.0 en later	Browser moet HTTP-sessiecookies en HTTP 302 Redirect-functie inschakelen.
Firefox	2.0 en later	Browser moet HTTP-sessiecookies en HTTP 302 Redirect-functie inschakelen.
JBoss-verificaties	JBoss 4.0.3 JBoss 4.3.0	
Tomcat-verificaties	Zelfstandige versie Tomcat 5.0.28 Zelfstandige versie Tomcat 5.5.20	
Acegi-verificaties	Acegi 0.9.0 Acegi 1.0.4	
Engines webservices	Axis 1 - 1,4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO-beveiligingswaarschuwingen

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 applicatie maakt een

token aan en elke applicatie die dezelfde initString-parameter gebruikt, valideert het token.

Let op:

- 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 applicaties 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 zijn uitgeschakeld, tenzij het vereist is.
- **Niveau van verificatiebeveiliging**. De applicatie die het zwakste verificatieframework gebruikt en die een LW-SSO-token uitgeeft dat door andere geïntegreerde applicaties wordt vertrouwd, bepaalt het niveau van beveiligingsinformatie voor alle applicaties.

  Het is aanbevolen dat enkel applicaties 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 applicatie die LW-SSO gebruikt, een token uitgeven dat moet worden vertrouwd door alle andere applicaties die dezelfde initString-parameter delen. Dit risico is relevant wanneer een applicatie die een initString deelt, zich op een niet-vertrouwde locatie bevindt of vanaf een niet-vertrouwde locatie kan worden geopend.
- **Gebruikerstoewijzing (synchronisatie).**Het LW-SSO-framework stelt de gebruikerstoewijzing tussen de geïntegreerde applicaties niet zeker. Daarom moet de geïntegreerde applicatie gebruikerstoewijzing controleren. We raden u aan om hetzelfde gebruikersregister (als LDAP/AD) te delen tussen alle geïntegreerde applicaties.

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

  Bovendien: wanneer een gebruiker zich aanmeldt bij een applicatie (AppA) en vervolgens toegang krijgt tot een tweede applicatie (AppB) die container- of applicatieverificatie gebruikt, en de gebruiker kan niet worden toegewezen, dan is de gebruiker verplicht om zich handmatig aan te melden bij AppB en een gebruikersnaam in te voeren. Als de gebruiker een andere gebruikersnaam invoert dan de gebruikersnaam die werd ingevoerd voor aanmelding bij AppA, dan kan het volgende gedrag ontstaan: als de gebruiker zich daarna toegang verschaft tot een derde applicatie (AppC) vanuit AppA of AppB, dan zal hij zich toegang verschaffen met behulp van de gebruikersnamen die werden gebruikt om zich aan te melden bij respectievelijk AppA of AppB.
- **Identity Manager.** Indien gebruikt ter verificatie, moeten alle onbeschermde bronnen in de Identity Manager worden geconfigureerd met de instelling **nonsecureURLs** in het configuratiebestand voor LW-SSO.
- **Demo-modus LW-SSO.**

- De Demo-modus dient uitsluitend ter demonstratie te worden gebruikt.
- De Demo-modus dient uitsluitend in onbeveiligde netwerken te worden gebruikt.
- De Demo-modus moet niet in productie worden gebruikt. Elke combinatie van de Demo-modus met de productiemodus moet worden vermeden.

Probleemoplossing en beperkingen

In dit gedeelte worden de bekende problemen en beperkingen voor werken met LW-SSO-verificatie beschreven.

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.** In de afmeldingsfunctionaliteit voor meerdere domeinen kunnen in de volgende omstandigheden fouten optreden:

  - De gebruikte browser is Internet Explorer 7 en de applicatie 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 applicatie in de afmeldingsprocedure te verlagen.

Beperkingen

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

- **Clienttoegang tot de applicatie.**

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

  - De applicatieclients moeten zich toegang tot de applicatie 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 applicatie zonder een FQDN in de aanmeldings-URL. In dit geval wordt specifiek voor één machine zonder domeininformatie een LW-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 applicaties 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 de ene applicatie naar de andere en wordt het invoeren van een URL in een browservenster niet ondersteund, tenzij beide applicaties 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 applicatie niet (alleen het verzoek **HTTP GET** wordt ondersteund). Als uw applicatie bijvoorbeeld een HTTP-koppeling naar een tweede applicatie heeft, wordt wel een **HTTP GET**-verzoek ondersteund maar niet een **HTTP FORM**-verzoek. 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 applicatie in één bepaald domein naar een andere applicatie 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. Zie voor een voorbeeld: `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`
  - Gedrag van cookies van derden in Internet Explorer:

    Microsoft Internet Explorer 6 bevat een module die het "Platform for Privacy Preferences (P3P) Project" ondersteunt. Dit betekent dat cookies die afkomstig zijn van een domein van derden, standaard worden geblokkeerd in de beveiligingszone Internet. Sessiecookies worden door Internet Explorer ook beschouwd als cookies van derden en worden daarom geblokkeerd, zodat LW-SSO niet meer werkt. Voor meer informatie over dit onderwerp, gaat u naar: `http://support.microsoft.com/kb/323752/en-us`.

    U kunt dit probleem oplossen door de applicatie die u hebt gestart (of een DNS-domeinsubset zoals *.mijndomein.com) toe te voegen aan de zone Intranet/Vertrouwde websites op uw computer (selecteer in Microsoft Internet Explorer **Menu > Extra > Internetopties > Beveiliging > Lokaal intranet > Websites > Geavanceerd**), waardoor de cookies worden geaccepteerd.

> **Let op:** De LW-SSO-sessiecookie is slechts één van de door de applicatie van derden gebruikte cookies die wordt geblokkeerd.

- **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 applicatie, wordt een gebruiker die zichzelf uit de eerste applicatie afmeldt, niet uit de tweede applicatie afgemeld.
  - **De verlooptijd van het SAML2-token wordt niet weergegeven in het sessiebeheer van de applicatie.**

    Als het SAML2-token gebruikt wordt om toegang te krijgen tot een tweede applicatie, wordt het sessiebeheer van elke applicatie 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.**Een load balancer die door LW-SSO wordt gebruikt, moet zo zijn geconfigureerd dat "sticky sessions" kunnen worden gebruikt.
- **Demo-modus.** In de Demo-modus ondersteunt LW-SSO koppelingen van de ene applicatie naar de andere maar wordt niet het typen van een URL in een browservenster ondersteund. In dit geval is dit te wijten aan afwezigheid van de koptekst van de verwijzende site.

Hoofdstuk 7

HP Universal CMDB-Aanmeldingsverificatie

In dit hoofdstuk vindt u de volgende informatie:

Een verificatiemethode instellen

Voor het uitvoeren van verificatie kunt u kiezen voor de volgende mogelijkheden:

- **Ten opzichte van de interne HP Universal CMDB-service.**
- **Via het Lightweight Directory Access Protocol (LDAP).** U kunt een speciale, externe LDAP-server gebruiken voor het opslaan van de verificatiegegevens in plaats van de interne HP Universal CMDB-service te gebruiken. De LDAP-server moet zich in hetzelfde subnet als alle HP Universal CMDB-servers bevinden.

  Zie de sectie over LDAP-toewijzing in de *HP Universal CMDB – Handleiding Beheer* voor meer informatie over LDAP.

  De standaardverificatiemethode maakt gebruik van de interne HP Universal CMDB-service. Als u de standaardmethode gebruikt, hoeft u geen wijzigingen aan te brengen in het systeem.

  Deze opties zijn van toepassing op aanmeldingen die worden uitgevoerd via webservices alsmede aanmeldingen via de gebruikersinterface.

- **Via LW-SSO.** HP Universal CMDB is geconfigureerd met LW-SSO. Met LW-SSO kunt u zich aanmelden bij HP Universal CMDB en automatisch toegang krijgen tot overige geconfigureerde applicaties die in hetzelfde domein worden uitgevoerd zonder dat u zich bij deze applicaties hoeft aan te melden.

  Wanneer ondersteuning van LW-SSO-verificatie is ingeschakeld (standaard is deze methode uitgeschakeld), moet u ervoor zorgen dat LW-SSO is ingeschakeld voor de andere applicaties in de Single Sign-On-omgeving en dat deze werken met dezelfde initString-parameter.

Aanmelding bij HP Universal CMDB via LW-SSO inschakelen

Als u LW-SSO wilt inschakelen voor HP Universal CMDB, gebruikt u de volgende procedure:

1. Open de JMX-console door het volgende adres in te voeren in de webbrowser: **http://<servernaam>:8080/jmx-console**, waarbij **<servernaam>** staat voor de naam van de machine waarop HP Universal CMDB is geïnstalleerd.
2. Klik onder **UCMDB-UI** op **name=LW-SSO Configuration** om de pagina Bewerkingen te openen.
3. Stel de initreeks in met behulp van de methode **setInitString**.
4. Stel de domeinnaam van de machine waarop UCMDB is geïnstalleerd in met behulp van de methode **setDomain**.
5. Roep de methode **setEnabledForUI** aan met de parameter ingesteld op **True**.
6. **Optioneel**. Als u wilt werken met ondersteuning van meerdere domeinen, selecteert u de methode **addTrustedDomains**, voert u de domeinwaarden in en klikt u op **Aanroepen**.
7. **Optioneel.** Als u wilt werken met een reverse proxy, selecteert u de methode **updateReverseProxy**, stelt u de parameter **Reverse proxy ingeschakeld** in op **True**, voert u een URL in voor de parameter **Reverse proxy volledige server-URL** en klikt u op Aanroepen. Als u zowel direct als met een reverse proxy toegang wilt krijgen tot UCMDB, stelt u de volgende aanvullende configuratie in: selecteer de methode **setReverseProxyIPs**, voer het IP-adres in voor de parameter Reverse proxy IP-adressen en klik op **Aanroepen**.
8. **Optioneel**. Als u toegang tot UCMDB wilt krijgen met een extern verificatiepunt, selecteert u de methode **setValidationPointHandlerEnable**, stelt u de parameter **Validatiepunt-handler is ingeschakeld** in op **True**, voert u de URL voor het verificatiepunt in bij de parameter **Server voor verificatiepunt** en klikt u op **Aanroepen**.
9. Als u de LW-SSO-configuratie wilt weergeven zoals deze in het instellingenmechanisme is opgeslagen, selecteert u de methode **retrieveConfigurationFromSettings**.
10. Als u de werkelijk geladen LW-SSO-configuratie wilt weergeven, selecteert u de methode **retrieveConfiguration**.

Opmerking: U kunt LW-SSO niet inschakelen via de gebruikersinterface.

Een beveiligde verbinding instellen met het SSL (Secure Sockets Layer)-protocol

Aangezien tijdens het aanmeldingsproces vertrouwelijke gegevens worden uitgewisseld tussen HP Universal CMDB en de LDAP-server, kunt u een bepaald niveau van beveiliging aan de inhoud toekennen. Dit doet u door SSL-communicatie op de LDAP-server in te schakelen en HP Universal CMDB te configureren voor het werken met SSL.

HP Universal CMDB ondersteunt SSL dat een certificaat gebruikt dat wordt uitgegeven door een vertrouwde certificeringsinstantie (Certification Authority, CA).

De meeste LDAP-servers, waaronder Active Directory, kunnen een veilige poort vrijmaken voor een SSL-verbinding. Als u Active Directory gebruikt met een persoonlijke CA, moet u de CA wellicht aan de vertrouwde CA's in de JRE toevoegen.

Zie "Secure Sockets Layer-communicatie (SSL) inschakelen" op pagina 18 voor meer informatie over het configureren van het HP Universal CMDB-platform voor ondersteuning van SSL.

Een CA toevoegen aan vertrouwde CA's om een veilige poort vrij te maken voor een SSL-verbinding:

1. Exporteer een certificaat van uw CA en importeer het in de JVM die door HP Universal CMDB wordt gebruikt:
   a. Open op de UCMDB-servermachine de map **UCMDBServer\bin\JRE\bin**.
   b. Voer de volgende opdracht uit:

   ```
   Keytool -import -file <uw certificaatbestand> -keystore
   C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Bijvoorbeeld:

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore
   C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

2. Selecteer **Beheer > Infrastructuurinstellingen > LDAP - algemeen**.

   Opmerking: u kunt deze instellingen ook configureren met de JMX-console. Zie "LDAP-instellingen configureren via de JMX-console" op volgende pagina voor meer informatie over dit onderwerp.

3. Selecteer **URL LDAP-server** en geef een waarde op in de volgende indeling:

   ```
   ldaps://<ldapHost>[:<poort>]/[<baseDN>][??scope]
   ```

   Bijvoorbeeld:

   ```
   ldaps://mijn.ldap.server:389/ou=People,o=mijnOrg.com??sub
   ```

   Let op de **s** in **ldaps**.

4. Klik op **Opslaan** om de nieuwe waarde op te slaan of klik op **Standaardwaarde** om de waarde te vervangen door de standaardwaarde (een lege URL).

De JMX-console gebruiken om LDAP-verbindingen te testen

In dit gedeelte wordt beschreven hoe u de LDAP-verificatieconfiguratie kunt testen met behulp van de JMX-console.

1. Open uw webbrowser en voer het volgende adres in: **http://<servernaam>:8080/jmx-console**, waarbij **<servernaam>** staat voor de naam van de machine waarop HP Universal

CMDB is geïnstalleerd.

Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

2. Klik onder **UCMDB** op **UCMDB-UI:name=LDAP Settings** om de pagina Bewerkingen te openen.
3. Zoek naar **testLDAPConnection**.
4. In het vak **Waarde** voor de parameter **customerID** voert u de klant-ID in.
5. Klik op **Aanroepen**.

   Op de pagina met resultaten van de JMX MBEAN-bewerking wordt aangegeven of de LDAP-verbinding geslaagd is. Als de verbinding geslaagd is, worden op de pagina tevens de LDAP-hoofdgroepen weergegeven.

LDAP-instellingen configureren via de JMX-console

In dit gedeelte wordt beschreven hoe u LDAP-verificatie-instellingen kunt configureren met behulp van de JMX-console.

LDAP-verificatie-instellingen configureren:

1. Open uw webbrowser en voer het volgende adres in: **http://<servernaam>:8080/jmx-console**, waarbij **<servernaam>** staat voor de naam van de machine waarop HP Universal CMDB is geïnstalleerd.

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.
2. Klik onder **UCMDB** op **UCMDB-UI:name=LDAP Settings** om de pagina Bewerkingen te openen.
3. Zoek naar de **methode getLDAPSettings** om de huidige LDAP-verificatie-instellingen weer te geven. Klik op **Aanroepen**. De LDAP-instellingen en bijbehorende waarden worden weergegeven in een tabel.
4. Zoek naar de methode **configureLDAP** om de waarden van de LDAP-verificatie-instellingen te wijzigen. Voer de waarden voor de relevante instellingen in en klik op **Aanroepen**. Op de pagina met resultaten van de JMX MBEAN-bewerking wordt aangegeven of de LDAP-verificatie-instellingen correct werden bijgewerkt.

   Opmerking: als u geen waarde invoert voor een instelling, behoudt de instelling de huidige waarde.
5. Na configuratie van de LDAP-instellingen kunt u de LDAP-gebruikersreferenties verifiëren. Zoek naar de methode **verifyLDAPCredentials**. Voer de klant-ID, de gebruikersnaam en het wachtwoord in en klik op Aanroepen. Op de pagina met resultaten van de JMX MBEAN-bewerking wordt aangegeven of de gebruiker de LDAP-verificatie heeft doorstaan.

De LDAP-verificatiemethode inschakelen en definiëren

U kunt de LDAP-verificatiemethode voor een HP Universal CMDB-systeem inschakelen en definiëren.

De LDAP-verificatiemethode inschakelen en definiëren:

1. Selecteer **Beheer > Infrastructuurinstellingen > LDAP - algemeen**.
2. Selecteer **URL LDAP-server** en geef de LDAP URL op in de volgende indeling:

   ```
   ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   Bijvoorbeeld:

   ```
   ldap://mijn.ldap.server:389/ou=People,o=mijnOrg.com??sub
   ```

3. Selecteer **LDAP - groepsdefinitie** en voer vervolgens onder **Basis-DN voor groepen** een unieke naam in voor de algemene groep.
4. Ga naar **Basis-DN hoofdgroepen** en voer de unieke naam van de hoofdgroep in.
5. Selecteer **LDAP - algemeen** en controleer onder **Synchronisatie van gebruikersrechten inschakelen** of de waarde is ingesteld op **True**.
6. Selecteer **LDAP algemene verificatie**, ga naar **Wachtwoord van zoekgerechtigde gebruiker** en geef het wachtwoord op.
7. Selecteer de categorie **LDAP - opties voor klassen en attributen**, zoek **Object groepsklasse** en vul de klassenaam van het object in (**group** voor Microsoft Active Directory en **groupOfUniqueNames** voor Oracle Directory Server).
8. Zoek **Attribuut groepslid** en vul de attribuutnaam in (**member** voor Microsoft Active Directory en **uniqueMember** voor Oracle Directory Server).
9. Zoek **Objectklasse gebruikers** en vul de naam van de objectklasse in (**user** voor Microsoft Active Directory en **inetOrgPerson** voor Oracle Directory Server).
10. Zoek **Attribuut UUID** en vul het unieke identificerende attribuut in voor een gebruiker op uw adreslijstserver. Zorg dat u een attribuut selecteert dat uniek is op uw adreslijstserver. Wanneer u SunOne/Oracle Directory Server gebruikt, is het UID-attribuut bijvoorbeeld niet uniek. In zo'n geval gebruikt u het attribuut van het e-mailadres of de Distinguished Name. Als u een niet-uniek attribuut gebruikt als het unieke identificerende attribuut in de UCMDB, leidt dit mogelijk tot inconsistent gedrag tijdens het aanmelden.
11. Sla de nieuwe waarden op. Als u een item door de standaardwaarde wilt vervangen, klikt u op **Standaardwaarde**.
12. Als de infrastructuurinstelling **Is gedwongen hoofdlettergevoelig bij verificatie met LDAP** onder **LDAP -algemeen** wordt ingesteld op **True**, is de verificatie hoofdlettergevoelig.

> **Let op:** Wanneer de waarde van deze infrastructuurinstelling wordt gewijzigd, moeten alle externe gebruikers handmatig worden verwijderd door de UCMDB-beheerder.

13. Wijs LDAP-gebruikersgroepen toe aan UCMDB-gebruikersgroepen. Zie "HP Universal CMDB-Aanmeldingsverificatie" op pagina 85 voor meer informatie over dit onderwerp.
14. Als u een standaardset met rechten wilt definiëren voor gebruikers in een LDAP-groep zonder groepstoewijzing, selecteert u de categorie **LDAP - Algemeen**, zoekt u **Automatisch toegewezen gebruikersgroep** en voert u de groepsnaam in.

Het standaardprotocol dat voor communicatie met de LDAP-server wordt gebruikt is TCP, maar u kunt het protocol wijzigen in SSL. Zie "Een beveiligde verbinding instellen met het SSL (Secure Sockets Layer)-protocol" op pagina 86 voor meer informatie over dit onderwerp.

> **Opmerking:** Voor elke LDAP-gebruiker is er een voornaam, achternaam en e-mailadres opgeslagen in de lokale opslagplaats. Als de opgeslagen waarde van een van deze parameters op de LDAP-server afwijkt van de waarde in de lokale opslagplaats, worden de lokale waarden bij elke aanmelding overschreven door de waarden op de LDAP-server.

De huidige LW-SSO-configuratie ophalen in een gedistribueerde omgeving

Wanneer UCMDB is opgenomen in een gedistribueerde omgeving, bijvoorbeeld een BSM-implementatie, voert u de volgende procedure uit om de huidige LW-SSO-configuratie op de verwerkende machine op te halen.

De huidige LW-SSO-configuratie ophalen:

1. Open een webbrowser en voer het volgende adres in:
   `http://localhost.<domeinnaam>:8080/jmx-console.`

   Wellicht wordt naar uw gebruikersnaam en wachtwoord gevraagd.
2. Zoek de **UCMDB:service=Security Services**-service en klik op de koppeling om de pagina Bewerkingen te openen.
3. Zoek naar de bewerking **retrieveLWSSOConfiguration**.
4. Klik op **Aanroepen** om de configuratie op te halen.

Hoofdstuk 8

Confidential Manager

In dit hoofdstuk vindt u de volgende informatie:

Confidential Manager - overzicht

Het Confidential Manager-framework biedt een oplossing voor het probleem van beheer en distributie van gevoelige gegevens voor HP Universal CMDB en overige softwareproducten van HP.

Confidential Manager bestaat uit twee hoofdcomponenten: de client en de server. Deze twee componenten zijn verantwoordelijk voor het veilig overbrengen van gegevens.

- De Confidential Manager-client is een bibliotheek die door applicaties wordt gebruikt voor toegang tot gevoelige gegevens.
- De Confidential Manager-server ontvangt verzoeken van Confidential Manager-clients, of van clients van derden, en voert de vereiste taken uit. De Confidential Manager-server is verantwoordelijk voor het veilig opslaan van de gegevens.

Confidential Manager codeert referenties tijdens het overbrengen, in de clientcache, in persistentie en in het geheugen. Confidential Manager gebruikt symmetrische cryptografie voor het overbrengen van referenties tussen de Confidential Manager-client en de Confidential Manager-server door het gebruik van een gedeeld geheim. Confidential Manager gebruikt verschillende geheimen voor de codering van cache, persistentie en transport, al naargelang de configuratie.

Zie "Beheer van Data Flow-referenties" op pagina 42 voor uitvoerige richtlijnen voor het beheren van referentiecodering in de Data Flow-probe.

Veiligheidsoverwegingen

- U kunt de volgende sleutelgrootten gebruiken voor het beveiligingsalgoritme: 128-, 192- en 256-bits. Het algoritme werkt sneller met de kleinere sleutel, maar is dan minder veilig. De grootte van 128-bits is doorgaans veilig genoeg.
- Gebruik MAC om het systeem veiliger te maken: stel **useMacWithCrypto** in op **true.** Zie "Coderingseigenschappen" op pagina 93 voor meer informatie over dit onderwerp.
- Voor krachtige beveiligingsproviders kunt u de JCE-modus gebruiken.

De HP Universal CMDB-server configureren

Tijdens het werken met HP Universal CMDB moet u het geheim en de crypto-eigenschappen van de codering configureren. Hiervoor gebruikt u de volgende JMX-methoden:

1. Start de webbrowser op de HP Universal CMDB-servermachine en voer het volgende serveradres in: **http://<hostnaam of IP-adres UCMDB-server>:8080/jmx-console.**

   Wellicht zult u zich moeten aanmelden met een gebruikersnaam en wachtwoord.

2. Klik onder UCMDB op **UCMDB:service=Security Services** om de pagina Bewerkingen te openen.

3. Voor het ophalen van de huidige configuratie zoekt u de bewerking **CMGetConfiguration**.

   Klik op **Aanroepen** om het XML-bestand met de Confidential Manager-serverconfiguratie weer te geven.

4. Kopieer het XML-bestand dat u in de vorige stap hebt aangeroepen, naar een teksteditor om wijzigingen aan te brengen in de configuratie. Breng wijzigingen aan op basis van de tabel in "Coderingseigenschappen" op volgende pagina.

   Zoek naar de bewerking **CMSetConfiguration**. Kopieer de bijgewerkte configuratie naar het vak **Waarde** en klik op **Aanroepen**. De nieuwe configuratie wordt naar de UCMDB-server geschreven.

5. Zoek naar de bewerking **CMAddUser** om gebruikers aan Confidential Manager toe te voegen voor autorisatie en replicatie. Dit proces is ook handig bij het replicatieproces. Bij replicatie moet de serverslave communiceren met de servermaster, via een geprivilegieerde gebruiker.

   - **username**. De gebruikersnaam.
   - **customer.** De standaardwaarde is ALL_CUSTOMERS.
   - **resource.** De bronnaam. De standaard is ROOT_FOLDER.
   - **permission.** Kies tussen ALL_PERMISSIONS, CREATE, READ, UPDATE en DELETE. De standaard is ALL_PERMISSIONS.

   Klik op **Aanroepen**.

6. Start HP Universal CMDB indien nodig opnieuw op.

   Opmerking: In de meeste gevallen hoeft de server niet opnieuw te worden opgestart. mogelijk moet de server opnieuw worden opgestart wanneer een van de volgende bronnen wordt gewijzigd:

   - Opslagtype
   - Tabel- of kolomnaam in de database
   - De maker van de databaseverbinding
   - De verbindingseigenschappen van de database (URL, gebruiker, wachtwoord, naam van stuurprogrammaklasse)
   - Databasetype

Opmerking:

- Het is belangrijk dat de UCMDB-server en de clients dezelfde crypto-eigenschappen voor transport hebben. Als deze eigenschappen worden gewijzigd op de UCMDB-server, moet u ze ook op alle clients wijzigen. (Dit is niet relevant voor de Data Flow-probe, omdat deze wordt uitgevoerd binnen hetzelfde proces als de UCMDB-server. De crypto-configuratie voor transport hoeft dus niet te worden gewijzigd.)
- Confidential Manager-replicatie is niet standaard geconfigureerd en kan zo nodig worden geconfigureerd.
- Als Confidential Manager-replicatie is ingeschakeld en de **initString** voor transport of andere crypto-eigenschappen van de master veranderen, moeten alle slaves de wijzigingen overnemen.

Definities

Crypto-eigenschappen opslag. De configuratie die definieert hoe de server de gegevens opslaat en codeert (in database of bestand, welke crypto-eigenschappen moeten de gegevens coderen en decoderen, enzovoort), hoe referenties veilig worden opgeslagen, hoe codering wordt verwerkt en op basis van welke configuratie.

Crypto-eigenschappen transport. De transportconfiguratie definieert hoe de server en de clients het transport tussen elkaar coderen, welke configuratie wordt gebruikt, hoe referenties veilig worden overgebracht, hoe codering wordt verwerkt en op basis van welke configuratie. U moet dezelfde crypto-eigenschappen gebruiken voor codering en decodering van transport, op zowel de server als de client.

Crypto-eigenschappen voor replicaties en replicatie. Gegevens die veilig door Confidential Manager worden bijgehouden, worden veilig tussen verschillende servers gerepliceerd. Deze eigenschappen definiëren hoe de gegevens worden overgebracht tussen de slaveserver and masterserver.

Opmerking:

- De databasetabel die de Confidential Manager-serverconfiguratie bevat, is: **CM_ CONFIGURATION.**
- Het standaardconfiguratiebestand voor de Confidential Manager-server bevindt zich in app-infra.jar en heeft de naam **defaultCMServerConfig.xml**.

Coderingseigenschappen

De volgende tabel bevat een overzicht van de coderingseigenschappen. Zie "De HP Universal CMDB-server configureren" op vorige pagina voor meer informatie over het gebruik van de parameters.

Parameter	Beschrijving	Aanbevolen waarde
encryptTransportMode	De getransporteerde gegevens coderen: true false	true
encryptDecrypt initString	Wachtwoord voor codering	Langer dan 8 tekens
cryptoSource	Te gebruiken bibliotheek voor implementatie van de codering: • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Ondersteunt eerdere versies van lichtgewicht cryptografie • true • false	true
cipherType	Het type coderingsmethode dat Confidential Manager gebruikt. Confidential Manager ondersteunt slechts één waarde: **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • Null. Geen codering	AES
algorithmModeName	Modus van het blokcoderingsalgoritme: • CBC	CBC
algorithmPaddingName	Standaarden opvullingsalgoritme: • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	Afhankelijk van algoritme (wat **engineName** ondersteunt)	256
pbeCount	Het aantal keren dat de hash moet worden uitgevoerd om de sleutel te maken op basis van	1000

Parameter	Beschrijving	Aanbevolen waarde
	encryptDecryptInitString. Een positief getal.	
pbeDigestAlgorithm	Hash-type: • SHA1 • SHA256 • MD5	SHA256
encodingMode	ASCII-representatie van het gecodeerde object: • Base64 • Base64Url	Base64Url
useMacWithCrypto	Definieert of MAC bij de cryptografie wordt gebruikt: • true • false	false
macType	Type berichtverificatiecode (MAC): • hmac	hmac
macKeySize SHA256	Afhankelijk van MAC-algoritme	256
macHashName	Het hash MAC-algoritme: • SHA256	SHA256


Java™
COMPATIBLE