HP Universal CMDB Configuration Manager

voor de besturingssystemen Windows en Linux

Softwareversie: 9.20

Implementatiegids

Publicatiedatum document: juni 2011
Uitgavedatum software: juni 2011

Juridische kennisgevingen

Garantie

De enige garanties voor producten en services van HP zijn vastgelegd in de expliciete garantieverklaringen die bij die producten en services worden geleverd. Niets in deze documentatie kan worden uitgelegd of opgevat als rechtgevend op extra garantie.
HP is niet aansprakelijk voor technische of redactionele fouten of omissies in dit document.

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

Beperkte rechten

Vertrouwelijke computersoftware. Voor het bezit, gebruik of kopiëren hiervan is een geldige licentie van HP vereist. Conform FAR 12.211 en 12.212 worden commerciële computersoftware, computersoftwaredocumentatie en technische gegevens voor commerciële artikelen onder een standaard commerciële licentie van de leverancier aan de overheid van de Verenigde Staten in licentie gegeven.

Kennisgevingen inzake copyright

Bijgewerkte documentatie

De titelpagina van dit document bevat de volgende identificerende informatie:

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

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

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

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

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

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

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

Ondersteuning

Bezoek de website van HP Software Support op:

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

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

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

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

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

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

Ga voor meer informatie over toegangsniveaus naar

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

Inhoudsopgave

DEEL I: INSTALLATIE EN CONFIGURATIE

Deel I

Installatie en configuratie

1

Overzicht

In dit hoofdstuk vindt u de volgende informatie:

Componenten

HP Universal CMDB Configuration Manager is een gezamenlijke release van verschillende componenten:

- **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) is een configuratiebeheerdatabase (CMDB) voor enterprise-IT-organisaties om bedrijfsservicedefinities en gerelateerde infrastructuurrelaties te documenteren, op te slaan en te beheren.

  UCMDB Foundation implementeert een gegevensmodel, gegevensstroombeheer en gegevensmodellering en biedt tevens mogelijkheden voor impactanalyse, het bijhouden van geschiedenissen en rapportage. Hiermee kunnen CMDB-gegevens worden getransformeerd tot begrijpelijke en bruikbare informatie, die kan worden gebruikt voor het beantwoorden van belangrijke vragen en het oplossen van bedrijfsproblemen.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) introduceert nieuwe, op beleidsregels gebaseerde topologie en beheer van inventarisconfiguraties. Deze toepassing is speciaal ontwikkeld voor configuratiebeheerders en configuratie-eigenaars, zodat zij ingewikkelde analyses kunnen verrichten met de CI-gegevens en topologiecontent die in of via UCMDB beschikbaar is. Configuration Manager biedt configuratiebeheerders en configuratie-eigenaars de juiste middelen om gemakkelijk beleidsregels voor topologie en inventarisconfiguratie in te stellen en automatisch te controleren of aan de normen van de organisatie wordt voldaan.

Configuration Manager wordt geïmplementeerd als extra Tomcat-server. De communicatie met de UCMDB-server verloopt met behulp van de uitgebreide UCMDB-SDK.

➤ **HP Discovery and Dependency Mapping Advanced Edition**

HP Discovery and Dependency Mapping Advanced Edition (DDMA) is met zijn rijke en altijd actuele content de voorkeursmethode van UCMDB voor het verkrijgen en onderhouden van de IT-infrastructuurgegevens.

➤ **HP Operations Orchestration**

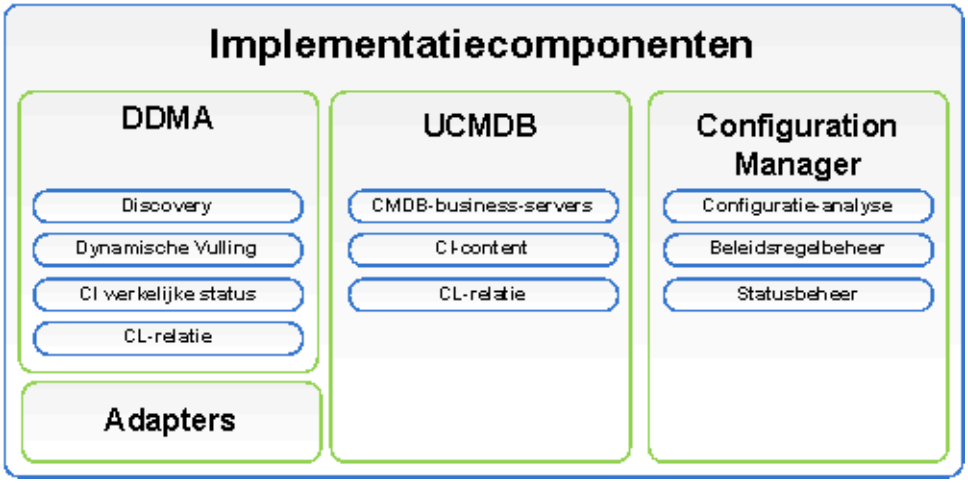
HP Operations Orchestration **(**OO) is een stroomautorisatie en implementatietool. Dankzij de intuïtieve methode van OO Studio voor slepen-en-verbinden kunnen gebruikers die weinig tot geen programmeerervaring hebben stromen ontwerpen, maken, delen en aanpassen. OO Studio ondersteunt de samenwerking tussen meerdere auteurs via functies voor versiebeheer. Met de krachtige, geïntegreerde foutopsporingsfunctie kunnen stromen in meerdere omgevingen worden getest, kan de ontwikkeling van content worden versneld en kunnen stromen worden gevalideerd voor een stabiele en betrouwbare uitvoering.

Tevens maakt OO Studio het mogelijk dat gebruikers gemakkelijk stromen kunnen implementeren. Met OO Studio kunnen gebruikers stromen vergelijken en promoveren in meerdere omgevingen (ontwikkelen, testen, klaarzetten en productie). Met Studio kunnen standaardprocessen worden gedocumenteerd en gestructureerde documentatie worden gegenereerd, ter ondersteuning van de compliancevereisten.

➤ **Integratie van Configuration Manager en OO**

Configuration Manager biedt de mogelijkheid om OO-stromen uit te voeren vanuit het Configuration Manager-framework. Er zijn twee hoofdmethoden voor het uitvoeren van OO-stromen:

- **Procesintegratie** – hiermee kunt u een RFC openen in een externe servicedesk-aanvraag waarmee een specifiek CI wordt afgestemd op een specifieke configuratiebeleidsregel.
- **Beleidsregelherstel** – hiermee kunt u een OO-stroom activeren die het configuratieprobleem herstelt. U kunt bijvoorbeeld extra geheugen toewijzen aan een virtuele hostmachine.



Uw omgeving

In deze handleiding wordt vanuit verschillende startpunten beschreven hoe HP Universal CMDB Configuration Manager moet worden geïmplementeerd:

Voor Configuration Manager

➤ Als Configuration Manager versie 9.10 is geïnstalleerd

Voor meer informatie over het upgraden van Configuration Manager naar de huidige versie, raadpleegt u "Configuration Manager upgraden" op pagina 40.

➤ Als Configuration Manager versie 9.10 niet is geïnstalleerd

Zie een van de volgende onderdelen voor meer informatie:

➤ "HP Universal CMDB Configuration Manager installeren op een Windows-platform" op pagina 17

➤ "HP Universal CMDB Configuration Manager installeren op een Linux-platform" op pagina 43

Voor UCMDB

➤ Als een lagere versie van UCMDB dan 9.03 is geïnstalleerd

Voert u de volgende stappen uit:

➤ Voer een upgrade uit naar UCMDB versie 9.03. Zie PDF *HP Universal CMDB – Implementatiehandleiding* voor meer informatie. U kunt de handleiding downloaden van www.hp.com/go/hpsoftwaresupport.

➤ Installeer Cumulative Update Pack 2. U vindt dit pakket op het installatiemedium van Configuration Manager of u kunt het downloaden van www.hp.com/go/hpsoftwaresupport.

Zie "Het database- of gebruikersschema configureren" op pagina 18 voor meer informatie over het configureren van bedrijfsklare toepassingen.

➤ Als UCMDB versie 9.03 is geïnstalleerd

Installeer Cumulative Update Pack 2. U vindt dit pakket op het installatiemedium van Configuration Manager of u kunt het downloaden van www.hp.com/go/hpsoftwaresupport.

Zie "Het database- of gebruikersschema configureren" op pagina 18 voor meer informatie over het configureren van bedrijfsklare toepassingen.

➤ Als er geen versie van UCMDB is geïnstalleerd

Voer een van de volgende stappen uit:

- ➤ Gebruik Deployment Manager (alleen voor Windows-systemen) om UCMDB tegelijk met Configuration Manager te installeren. Zie "HP Universal CMDB Configuration Manager installeren op een Windows-platform" op pagina 17 voor meer informatie.
- ➤ Installeer Configuration Manager op een Linux-systeem volgens de instructies in "HP Universal CMDB Configuration Manager installeren op een Linux-platform" op pagina 43.

Algemene informatie

Deze gids houdt tevens rekening met speciale UCMDB-implementaties die u mogelijk in uw omgeving hebt (bijvoorbeeld een High Availability-implementatie) en zorgt voor de noodzakelijke aanpassingen van de implementatieprocedure voor deze implementaties.

Opmerking: Installatie van UCMDB en Configuration Manager op dezelfde server wordt ondersteund. Voor aanpassing in een productieomgeving adviseert HP Software echter om deze componenten op afzonderlijke servers te installeren.

Voor het gebruik van Configuration Manager moet UCMDB met een geconsolideerde schemamodus worden geconfigureerd en moet er een nieuwe UCMDB-status worden gemaakt (geautoriseerde status). Deze configuraties worden in beide installatiesituaties automatisch door de implementatieprocedure uitgevoerd (ongeacht of er al een installatie van UCMDB bestaat of dat deze wordt geïnstalleerd door Deployment Manager).

Belangrijk: Als u naar een bestaande UCMDB-installatie verwijst en het bijbehorende schema nog niet is geconsolideerd, kan de consolidatiefase voor databases met een groot aantal vermeldingen (meer dan 5 miljoen CI's) lang duren (20 tot 60 minuten).

Als u alleen Configuration Manager implementeert (en dus een bestaande of bijgewerkte installatie van UCMDB gebruikt), moet de UCMDB-server actief zijn om de installatie van Configuration Manager te kunnen voltooien.

Ondersteuningsmatrix

Systeemvereisten server

CPU	Minimaal 4 core
Geheugen (RAM)	Minimaal 4 GB
Platform	x64
Besturingssysteem	Windows (64-bits) ➤ Windows 2003 Enterprise SP2 en R2 SP2 ➤ Windows 2008 Enterprise SP2 en R2 Linux ➤ Red Hat Enterprise Linux x86 (64-bits)

Database	➤ Microsoft SQL Server 2005 SP2; 2005 compatibiliteitsmodus 80 (telkens Enterprise Edition) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Webserver	➤ Microsoft IIS 7 ➤ Apache 2
HP Universal CMDB	➤ HP Universal CMDB versie 9.03 met CUP 2 (reguliere CMDB-installatie) Zie PDF *HP Universal CMDB – Implementatiehandleiding* voor een complete lijst met systeemvereisten. **Opmerking:** ➤ Als de HP Universal CMDB-server wordt geïmplementeerd in combinatie met Configuration Manager, zijn de Enterprise Edition van Oracle en de Oracle Partitioning-optie vereist. ➤ Als u de HP Universal CMDB-server eerder hebt geïmplementeerd met de Standard Edition van Oracle en u Configuration Manager aan uw installatie wilt toevoegen, moet u uw Standard Edition-database eerst converteren naar een Enterprise Edition-database met de Partitioning-optie ingeschakeld.
LDAP (optioneel)	➤ Active Directory ➤ SunONE 6.x
Minimaal aanbevolen grootte databaseschema (optioneel)	2 GB

Clientvereisten

Besturingssysteem	➤ Windows XP x86 (32-bits) ➤ Windows Vista x86 (32-bits en 64-bits) ➤ Windows 7 x86 (32-bits en 64-bits)
Browser	➤ Microsoft Internet Explorer 7.0, 8.0 ➤ Mozilla Firefox 3.x, 4
Invoegtoepassing Flash Player voor browser	Flash Player 9 of hoger **NB:** U kunt Flash Player downloaden van: http://www.adobe.com/products/flashplayer/.
Schermresolutie	➤ Minimaal 1024 x 768 ➤ Aanbevolen 1280 x 1024
Kleurenkwaliteit	Minimaal 16 bits

HP Operations Orchestration (optioneel)

HP Operations Orchestration	➤ 7.51, 9.0

2

HP Universal CMDB Configuration Manager installeren op een Windows-platform

Belangrijk: Zorg ervoor dat u de releaseopmerkingen voor de meest actuele installatie-instructies leest.

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Configuratie voorafgaand aan de installatie

In dit gedeelte worden de volgende onderwerpen behandeld:

Het database- of gebruikersschema configureren

Opmerking: Deze taak wordt automatisch uitgevoerd als onderdeel van de installatie van Configuration Manager. Desgewenst kunt u dit echter ook handmatig doen.

Om met Configuration Manager te kunnen werken moet u een databaseschema opgeven. Configuration Manager en UCMDB gebruiken verschillende schema's. Configuration Manager ondersteunt Microsoft SQL Server en Oracle Database Server. In deze taak wordt beschreven hoe u een schema voor Configuration Manager kunt maken. Als u UCMDB installeert, moet u daar ook een aparte database of een apart gebruikersschema voor configureren. Zie PDF *HP Universal CMDB – Implementatiehandleiding* voor meer informatie.

Opmerking: Raadpleeg "Systeemvereisten server" op pagina 14 voor vereisten voor Microsoft SQL Server en Oracle Server.

Uw database configureren:

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

➤ Voor **Microsoft SQL Server**: activeer snapshotisolatie.

Nadat de database is gemaakt, voert u eenmaal de volgende opdracht uit:

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

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

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

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

✔	**Vereiste informatie**
	Hostnaam en poort DB
	Gebruikersnaam en wachtwoord DB
	Voor MS SQL: databasenaam
	Voor Oracle: SID

Configuration Manager installeren in een UCMDB-omgeving met High Availability

Als u Configuration Manager wilt gebruiken in een UCMDB-omgeving met High Availability, voert u de volgende stappen uit:

1 Schakel de reserveserver (passieve server) uit. Nadat de server is uitgeschakeld wacht u twee minuten.

2 Installeer Configuration Manager versie 9.20.

a Gebruik de hostdetails van uw netwerktaakverdeler.

b Installeer Configuration Manager op een derde server (dus niet op een van beide UCMDB-servers).

3 Controleer of UCMDB en Configuration Manager correct werken.

4 Start de reserveserver (passieve server) om High Availability te garanderen.

Opmerking: De High Availability-modus wordt niet ondersteund voor HP Universal CMDB Configuration Manager versie 9.20 zelf.

Configuration Manager installeren

Deployment Manager kan UCMDB, Configuration Manager en DDMA in verschillende configuraties (die op de pagina Products Selection van de installatiewizard zijn geselecteerd en geconfigureerd) installeren:

- Een nieuw exemplaar van UCMDB installeren
- Een nieuw exemplaar van Configuration Manager installeren en dit verbinden met een nieuw of bestaand exemplaar van UCMDB
- Een nieuw exemplaar van Configuration Manager integreren met een bestaand exemplaar van OO
- Meerdere exemplaren van DDMA installeren

Opmerking:

- Deployment Manager biedt u de mogelijkheid om producten, componenten en integraties op een doelmachine te installeren. Deployment Manager ondersteunt niet het ongedaan maken van productinstallaties, het wijzigen van producten en het installeren van patches op een geïnstalleerd product. Dit moet handmatig worden uitgevoerd.
- Zodra u op de pagina Product Selection op de knop **Next** klikt, kunt u niet meer naar die pagina terugkeren en de implementatieconfiguratie opnieuw selecteren. Als er wijzigingen in de implementatieconfiguratie moeten worden aangebracht, start u Deployment Manager opnieuw op.

Configuration Manager installeren:

1. U start de installatie door het installatiemedium van Configuration Manager in de machine te plaatsen en het bestand **setup.exe** te zoeken.
2. Dubbelklik op het bestand **setup.exe** om Deployment Manager uit te voeren.
3. Schakel de Windows-firewall op de doelmachine uit voor de duur van de installatie. Zie stap 6 van deze procedure voor meer informatie over de firewall.
4. Ga akkoord met de voorwaarden van de gebruiksrechtovereenkomst en klik op **Next** om de pagina Product Selection te openen.

Opmerking: De voorwaarden van de gebruiksrechtovereenkomst zijn van toepassing op alle producten die zijn geselecteerd in de pagina Product Selection van Deployment Manager.

---

5 Selecteer op de pagina Product Selection de producten die u wilt implementeren. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Server Location.

Op de pagina Product Selection kunt u de producten selecteren die u wilt installeren en kunt u de configuratieopties opgeven die tijdens de implementatie worden uitgevoerd.

a Selecteer een installatieoptie voor HP Universal CMDB Foundation.

Er zijn twee installatieopties voor UCMDB Foundation beschikbaar:

➤ **Connect to an Existing Server** – Als u deze optie selecteert, worden Configuration Manager of Discovery and Dependency Mapping verbonden met en geconfigureerd voor een bestaand exemplaar van een UCMDB Foundation-server.

Opmerking: De UCMDB-versie op een bestaande server moet versie 9.03 met CUP 2 of hoger zijn.

➤ **Install New Server** – Als u deze optie selecteert, wordt een nieuw exemplaar van een UCMDB Foundation-server geïnstalleerd, geconfigureerd en verbonden, en worden Configuration Manager of DDMA geconfigureerd voor en verbonden met het nieuwe exemplaar van de UCMDB Foundation-server.

b Schakel het selectievakje **Configuration Manager** in om een nieuw exemplaar van Configuration Manager te installeren en te configureren.

Selecteer indien gewenst de optie **Connect to an Existing HP Operation Orchestration instance**. Met deze optie wordt een integratie tussen Configuration Manager en Operations Orchestration geconfigureerd door de gegevens van de OO-serververbinding in te voeren in Configuration Manager.

c **HP Discovery and Dependency Mapping Advanced Edition.** Als u deze optie selecteert, worden er nieuwe exemplaren van DDMA geïnstalleerd en geconfigureerd.

Met de optie **Number of DDMA instances** kunt u meerdere DDMA-exemplaren installeren. Het aantal dat in het invoerveld is opgegeven, verwijst naar het aantal exemplaren van DDMA dat met één UCMDB-serverexemplaar verbonden is.

Opmerking: Deployment Manager ondersteunt meerdere implementaties van DDMA-exemplaren in dezelfde DMZ. Deployment Manager ondersteunt maximaal 10 exemplaren van discoverytests in elke implementatie. Als er meer discoverytests vereist zijn, moet u deze in groepen van tien in meerdere implementatiefasen installeren.

---

6 Geef voor elk product dat op de pagina Server Location voor implementatie is geselecteerd, de locatie op van de externe servers en de referenties van de doelimplementatiemachines. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Connections.

Implementatieopties

Selecteer een implementatieoptie voor de doellocatie. Er zijn twee opties beschikbaar:

- **Deploy on the local machine** – gebruik deze optie als u een product implementeert op dezelfde machine als Deployment Manager. In dit geval zijn de velden voor de details van de externe host en de referenties uitgeschakeld.
- **Deploy on the following machine** – als u deze optie selecteert, moet u het adres van de externe host en de gegevens van het besturingssysteem opgeven. De opgegeven gebruikersgegevens moeten beheerdersrechten hebben op de externe host.

Opmerking: Als u de hostnaam voor de productimplementatie opgeeft, zorg er dan voor dat u alleen letters (a-z), cijfers (0-9) en koppeltekens ('-') gebruikt.

De volgende informatie is relevant als u de gegevens van de externe machine opgeeft:

- **WMI and SMB Protocols** – worden gebruikt om verbinding te maken met de externe machine. Deployment Manager kan alleen verbinding maken met de externe machine als aan de volgende vereisten is voldaan:
  - **WMI Service** – de WMI-service moet op de externe machine worden uitgevoerd.
  - **Server Service** – om het SMB-protocol in te schakelen, moet de Server-service op de externe machine worden uitgevoerd.
  - **Windows Firewall** – de externe machine moet externe beheerders-verbindingen toestaan. Voer in de opdrachtpromptconsole op de externe machine de juiste opdracht uit:

Besturingssysteem	Opdracht
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

Verbinding testen

Klik op **Test Connection** om te controleren of de referenties en gegevens van de verbinding juist zijn en om de lokale en externe systeembronnen te analyseren.

Als de verbindingstest mislukt, geeft Deployment Manager een foutmelding met informatie over de fout. Als u op **Next** klikt, wordt de controle van de testverbinding automatisch geforceerd.

Bij het valideren van de machinebronnen wordt naar de volgende punten gekeken:

- **OS-platform** – controleert of het besturingssysteem gecertificeerd is voor de productimplementatie.
- **Schijfruimte** – controleert of er voldoende schijfruimte is.
- **Geheugen** – controleert of er voldoende fysiek geheugen is.
- **Poorten** – controleert of de vereiste poorten beschikbaar zijn.

Welke bronvalidaties door de testverbinding worden uitgevoerd, hangt af van de ondersteunde productmatrices.

Opmerking: Als de test de fout **Unknown** retourneert, controleer dan of de volgende services op de implementatiehostmachine worden uitgevoerd:

- Server
- Windows Management Instrumentation

Zorg ervoor dat User Account Control (UAC) is uitgeschakeld voordat u op **Next** klikt. Meer informatie over UAC vindt u op http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Configureer op de pagina Connections de verbindingen tussen de geselecteerde producten. Welke verbindingsopties op de pagina Connections worden weergegeven, hangt af van de componenten die op de pagina Product Selection zijn geselecteerd voor implementatie. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Installation Configuration.

➤ UCMDB to Configuration Manager Integration

Dit gedeelte wordt weergegeven als u ervoor kiest om Configuration Manager te installeren met de optie **Connect to an Existing Server**. Hier kunt u de integratie van Configuration Manager met UCMDB configureren.

Opmerking: Om verbinding te kunnen maken met een bestaand exemplaar van UCMDB, moet die installatie UCMDB-versie 9.03 met CUP 2 of hoger zijn.

Voer de volgende UCMDB-gegevens in:

Veld	Definitie
UCMDB Host Name/IP	Adres van de UCMDB-implementatielocatie. ➤ Als UCMDB in de High Availability-modus is geconfigureerd, volgt u de instructies op in "Configuration Manager installeren in een UCMDB-omgeving met High Availability" op pagina 19. ➤ Als UCMDB op de lokale machine is geïnstalleerd en Configuration Manager op een externe machine, moet de naam van het lokale UCMDB-exemplaar de FQDN zijn (niet localhost). ➤ Als UCMDB en Configuration Manager verschillende DNS-domeinnamen hebben en LW-SSO-integratie vereist is, moet u de FQDN opgeven in het invoerveld voor de bestaande UCMDB-host.
Protocol	HTTP- of HTTPS-protocol.
UCMDB HTTP(S) Port	De standaardwaarden van de HTTP- of HTTPS-poort zijn **8080** voor HTTP en **8443** voor HTTPS.
Client Certificate File	Dit veld wordt weergegeven als het HTTPS-protocol is geselecteerd. U moet het UCMDB-clientcertificaatbestand handmatig op de doelhost van Configuration Manager plaatsen en het volledige bestandspad (inclusief de bestandsnaam) in het naastgelegen invoerveld opgeven. Als UCMDB gebruikmaakt van HTTPS, is een sleuteluitwisseling vereist. De sleutel-uitwisseling wordt tijdens de verbindingstest niet gevalideerd.

Veld	Definitie
Customer Name	De standaard UCMDB-klantnaam is **Default Client**. De waarde van de klantnaam wordt gebruikt tijdens het configureren van de integratie van UCMDB en Configuration Manager. Deze waarde wordt tijdens de verbindingstest niet gevalideerd. Als u een onjuiste waarde opgeeft, mislukt de implementatie.
JMX Port	De standaardwaarde is **29601**.
UCMDB System User (JMX)	De UCMDB (JMX)-systeemgebruiker wordt gebruikt voor het activeren van JMX-functies, zoals het maken van een gebruiker van de Configuration Manager-integratie en de implementatie van het Configuration Manager-pakket. De standaardwaarde is **sysadmin**.
UCMDB System Password	Het wachtwoord van de UCMDB-systeemgebruiker. De standaardwaarde is **sysadmin**.

Opmerking: Configuration Manager wordt geconfigureerd met een interne gebruikersopslagplaats. Als u een externe LDAP als uw gebruikersopslagplaats wilt gebruiken, moet u Configuration Manager daarvoor configureren.
Zie "Systeeminstellingen" in de *Gebruikershandleiding van HP Universal CMDB Configuration Manager* voor meer informatie.

➤ Configuration Manager to OO Integration

Dit gedeelte wordt weergegeven als u de optie **Connect to an Existing HP Operation Orchestration instance** selecteert. Hier kunt u de integratie van Configuration Manager met OO configureren.

Voer de volgende OO-gegevens in:

Veld	Definitie
OO Version	Geldige OO-versies zijn 7.5 en 9.0.
OO Host Name/IP	De host of het IP-adres van de OO-servermachine.
OO Port Number	Het standaard poortnummer is **8443**.
OO Username	De standaard OO-gebruikersnaam is **admin**. De gebruiker moet in OO worden geconfigureerd als externe gebruiker.
OO Password	Het standaard OO-wachtwoord is **admin**.

➤ DDMA Configuration

Als u de optie **Discovery and Dependency Mapping Advanced Edition instance** selecteert, worden de volgende velden weergegeven en kunt u een DDMA-verbinding met UCMDB configureren.

Voer de volgende DDMA-gegevens in:

Veld	Definitie
Data Flow Probe Identifier	De standaardwaarde is de hostnaam van de DDMA-machine. Dit veld wordt automatisch ingevuld, maar u kunt deze waarde wijzigen.
Use Default Domain	Deze optie is standaard geselecteerd en is van invloed op de waarde van de domeinnaam. Als u dit selectievakje uitschakelt, kunt u een andere waarde voor de standaardnaam invoeren.
Domain Name	De standaardwaarde is ingesteld op **DefaultDomain**. Schakel het selectievakje **Use Default Domain** uit om dit veld te activeren.

Veld	Definitie
Initial Heap Size in MB	De geheugengrootte die oorspronkelijk is toegewezen aan de JVM van de DDMA. De standaardwaarde is 256 MB.
Maximum Heap Size in MB	De maximale geheugengrootte die aan de JVM is toegewezen. De standaardwaarde is 512 MB.

8 Stel de implementatiedoelmapgegevens in voor de productimplementaties die u hebt geselecteerd op de pagina Installation Configuration. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Database Configuration.

Voor elk geselecteerd product is een standaard mappad ingevoerd. Als u de implementatie op een lokale machine uitvoert, is de optie Browse beschikbaar zodat u een ander mappad kunt selecteren. Als u de installatie op een externe machine uitvoert, is deze optie uitgeschakeld.

Opmerking: De naam van de installatiemap mag geen geen spaties bevatten en mag alleen bestaan uit Engelse letters, (a-z), cijfers (0-9) en koppeltekens ('-').

---

9 Configureer op de pagina Database Configuration de databaseverbinding en het databaseschema voor elk product. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Ports Configuration.

U kunt de volgende databases (schema's) configureren:

- UCMDB-CM-schema
- UCMDB-schema

➤ UCMDB-geschiedenisschema

Veld	Definitie
Database Host Name/IP	Het adres van de databaseserverlocatie.
Port	MSSQL en Oracle gebruiken verschillende standaardpoorten. De standaard Oracle-databasepoort is 1521 en de standaard MSSQL-databasepoort is 1433.
SID (Oracle)	De naam van het exemplaar van de Oracle-database.
Admin Username (Oracle)	Voer de gebruikersnaam van de Oracle-beheerder in overeenkomstig de Oracle-server.
Admin Password (Oracle)	Voer het wachtwoord van de Oracle-beheerder in overeenkomstig de Oracle-server.
Test Connection	Test de verbinding met de doeldatabasehost. Gebruik daarvoor de opgegeven referenties.
Schema Name (Oracle)	Voer de naam van het schema in.
Schema Password (Oracle)	Voer het wachtwoord van het schema in. Dit veld wordt weergegeven als u een nieuw schema maakt.
Default Tablespace (Oracle)	Voer de standaard tabelruimtenaam in.
Temporary Tablespace (Oracle)	Voer de tijdelijke tabelruimtenaam in.
Database Name (MSSQL)	Voer de naam van het databaseschema in om de MSSQL-server te gebruiken of te maken.
Database Username (MSSQL)	Voer de gebruikersnaam van de MSSQL-beheerder in overeenkomstig de MSSQL-server.
Database Password (MSSQL)	Voer het wachtwoord van de MSSQL-beheerder in overeenkomstig de MSSQL-server.

Opmerking:

- Indien de UCMDB-tabelruimte vol is, wordt de productimplementatie wel uitgevoerd maar zullen de producten en componenten niet correct werken.
- Het maken van een nieuw UCMDB-schema en verbinding maken met een bestaand UCMDB-geschiedenisschema wordt niet ondersteund.
- Het gebruik van NTLM-verificatie tijdens het configureren van UCMDB-schema's met een MSSQL-database als UCMDB extern wordt geïnstalleerd, wordt om beveiligingsredenen niet ondersteund. Als NTLM-verificatie vereist is, moet UCMDB lokaal worden geïmplementeerd.

Schemamodus

Voor Configuration Manager moet UCMDB met een geconsolideerde schemamodus worden geconfigureerd en moet er een nieuwe UCMDB-status worden gemaakt.

Als u naar een bestaande UCMDB-installatie verwijst en het bijbehorende schema nog niet is geconsolideerd, kan de automatische consolidatiefase voor databases met een groot aantal vermeldingen (meer dan 5 miljoen CI's) lang duren (20 tot 60 minuten).

Opmerking: Oracle Real Application Cluster (RAC) en NTLM-verbindingen voor SQL-servers worden niet ondersteund als onderdeel van deze installatie. Als deze verbindingen vereist zijn, moet u eerst Configuration Manager met een eenvoudige databaseverbinding installeren en wanneer de installatie voltooid is de verbinding van de specifieke productconfiguratie wijzigen. U doet dit door het bestand **database.properties** volgens uw databasespecificaties aan te passen. Zie "Geavanceerde databaseconfiguratie (voor Configuration Manager)" op pagina 33 voor meer informatie.

Databaseconfiguratiemodus

Configuration Manager en UCMDB moeten verschillende schema's gebruiken.

Met Configuration Manager kan de gebruiker elke database op een Oracle- of MSSQL-databaseserver configureren.

Configuratietypen

U kunt verbinding maken met een bestaand schema of een nieuw schema maken. Als u verbinding maakt met een bestaand schema, wordt de inhoud ervan overschreven.

Databaseconfiguratie

Deze stap wordt automatisch uitgevoerd door Deployment Manager. Zie "Het database- of gebruikersschema configureren" op pagina 18 als u deze stap handmatig wilt uitvoeren.

Geavanceerde databaseconfiguratie (voor Configuration Manager)

Een databaseverbinding moet worden geconfigureerd en gekoppeld aan een standaard URL-verbinding. Als er geavanceerde functies (zoals Oracle Real Application Cluster) vereist zijn, moet u een standaardverbinding instellen en vervolgens het bestand **database.properties** handmatig bewerken om de geavanceerde functies te configureren.

Configuration Manager gebruikt systeemeigen stuurprogramma's voor de Oracle- en Microsoft SQL-serverdatabases. Alle systeemeigen stuurprogrammafuncties worden ondersteund, mits deze functies kunnen worden geconfigureerd met behulp van de database-URL. Deze URL bevindt zich in het bestand **database.properties**.

Zodra de wizard Deployment Manager voltooid is, kunnen aanvullende database- en schemaconfiguraties worden uitgevoerd.

Databaseconfiguratievelden

Er zijn twee databasetypen beschikbaar: Oracle en MSSQL. Afhankelijk van het geselecteerde databasetype worden er verschillende invoervelden weergegeven.

10 Geef op de pagina Port Configuration de verbindingspoorten van Configuration Manager op. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Users Configuration.

Configuration Manager biedt standaard poortinstellingen die worden weergegeven in de invoervelden van de wizardpagina Port Configuration.

Als een poortnummer conflicteert met een bestaande installatie, neem dan contact op met een IT-manager voordat u het poortnummer wijzigt.

Veld	Definitie
Application HTTP Port	8180
JMX HTTP Port	39900
Tomcat Port	8005
AJP Port	8009 (Apache Java-protocol)
Application HTTPS Port	8143
JMX Remote Port	39600

Klik op de knop **Revert to Default Values** om de poorten te herstellen naar de standaardwaarden van Deployment Manager.

11 Maak de volgende gebruikers op de pagina User Configuration:

- Gebruiker met beheerdersrechten voor eerste aanmelding UCMDB-CM.
- Integratiegebruiker in UCMDB: in UCMDB wordt op aanvraag door Configuration Manager een integratiegebruiker gemaakt om de integratie tussen deze twee producten te ondersteunen.

Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Security Configuration.

12 Op de pagina Security Configuration activeert u algemene LW-SSO in een nieuw exemplaar van UCMDB en Configuration Manager. LW-SSO wordt alleen in nieuwe exemplaren van Configuration Manager of UCMBD geconfigureerd, afhankelijk van de selectie die is gemaakt op de pagina Product Selection. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Summary.

LW-SSO is een modulair framework dat wordt gebruikt om verschillende soorten verificatie- en beveiligingstokens (zoals LW-SSO en SAML2) te valideren. LW-SSO wordt gebruikt om geverifieerde gegevens van verschillende omgevingen te koppelen en te gebruiken in toepassing-beveiligingscontexten binnen een toepassings- of beveiligingsframework.

De LW-SSO-configuratie hangt af van de geselecteerde productcomponenten.

Als Configuration Manager wordt verbonden met een bestaand UCMDB- of OO-exemplaar, wordt LW-SSO alleen geconfigureerd in Configuration Manager. U moet de LW-SSO-reeks uit UCMDB of OO ophalen en deze reeks invoeren in het invoerveld LW-SSO String. Als u zowel met UCMDB als OO verbinding maakt, moet u controleren of de LW-SSO-reeksen die in de UCMDB- en OO-exemplaren zijn gedefinieerd, met elkaar overeenkomen.

Als u een nieuw exemplaar van Configuration Manager verbindt met een bestaand exemplaar van UCMDB, moet u de FQDN gebruiken als de UCMDB-hostnaam.

De LW-SSO-reeks ophalen uit UCMDB:

a Open UCMDB en selecteer **Beheer** > **Beheer infrastructuurinstellingen**.

b Selecteer in de kolom **Naam** het veld LW-SSO - Initreeks en dubbelklik op dit veld.

c Kopieer de reeks uit het invoerveld Huidige waarde.

d Plak deze waarde in het invoerveld LW-SSO String op de pagina Security Configuration.

Als Configuration Manager wordt verbonden met een nieuw UCMDB-exemplaar, wordt LW-SSO automatisch geconfigureerd in UCMDB en Configuration Manager.

13 Controleer de installatie- en configuratie-instellingen op de pagina Summary. Als u klaar bent, klikt u op **Next** om door te gaan naar de pagina Validation.

Op de pagina Summary vindt u een overzicht van alle configuratie-gegevens en gebruikersinvoergegevens. Desgewenst kunt u de inhoud van het overzicht aanpassen, door te klikken op de knop Back op de verschillende pagina's totdat u de gewenste pagina bereikt. Vervolgens kunt u de implementatie-instellingen aanpassen. U keert terug naar de pagina Summary door zo vaak als nodig op **Next** te klikken.

14 Deployment Manager voert nu een reeks acties uit om te controleren of de systeembronnen van de externe machines voldoende zijn, na te gaan of de ingevoerde gebruikersgegevens correct zijn en de instellingen van de databaseconfiguratie te valideren. Deze validaties geven aan of de gebruikersdefinitie-instellingen voldoen aan bekende beperkingen van de omgeving. Het validatieproces start automatisch. Als u naar een eerdere pagina in Deployment Manager bent teruggekeerd en wijzigingen hebt aangebracht, klikt u op **Run Validation** om het validatieproces te starten. Als u klaar bent, klikt u op **Deploy** om door te gaan naar de pagina Deployment.

15 De pagina Deployment geeft de voortgangsstatus van de implementatie weer. Het implementatieproces bevat productinstallaties, de start-procedures en de integratie en verbindingen daarvan met andere producten.

Het implementatieproces is voltooid zodra alle producten zijn gestart.

Klik op **Details** om de details van de implementatievoortgang weer te geven, met inbegrip van de stappen die door Deployment Manager zijn ondernomen voor de implementatie van elk geselecteerd product.

Klik op **Cancel** om de implementatie op de juiste wijze te annuleren. Hierdoor wordt de actieve implementatiebewerking voltooid voordat de implementatie wordt gestopt.

Klik op **Abort** (alleen beschikbaar nadat u op **Cancel** hebt geklikt) om de uitgevoerde bewerking en de implementatie geforceerd te beëindigen. Het afbreken van de implementatie kan ertoe leiden dat de producten een onbepaalde status hebben.

Validaties

In de volgende tabel vindt u een lijst met validaties die door Deployment Manager worden uitgevoerd.

Validatie	Foutmelding	Beschrijving
Aanmeldingsreferenties controleren	Credentials verification failed	De opgegeven gebruikers-gegevens zijn onjuist.
		De verbinding is niet gemaakt.
Compatibiliteit met het besturingssysteem controleren	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	Het doelbesturingssysteem komt niet overeen met de lijst van gecertificeerde besturingssystemen voor het product.
Geheugen controleren	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	Er is onvoldoende geheugen op de doel-machine voor alle toegewezen producten.
	<Memory> MB of memory are verified to be available on <Target Machine>	De validatie is geslaagd.

Validatie	Foutmelding	Beschrijving
Schijfruimte controleren	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	Er is onvoldoende schijfruimte op de doelmachine voor alle toegewezen producten.
	<Memory> MB of disk space are verified to be available on drive <Target>	De validatie is geslaagd.
Controleren of alle verplichte eigenschappen zijn ingevoerd	Missing the target storage device for the product: <Target>	De installatiemap van het product is niet ingesteld.
Controleren of er een implementatiemachine is gedefinieerd	No deployment machine is defined for <Product Name>	Het product is niet geconfigureerd om te worden geïmplenteerd op een machine.
Aanmeldingsreferenties controleren	Credentials verification failed	De aanmeldingsreferenties zijn onjuist.
Controleren of UAC is uitgeschakeld	The UAC is enabled	De UAC is ingeschakeld op de doelmachine.
Vrije poorten controleren	The required port number <Port> is already in use on <Target>	De vereiste poort op de doelmachine is reeds in gebruik.
Controleren of het doelopslagapparaat bestaat	The target storage device <Device> does not exist on <Target>	Het geselecteerde doelopslagapparaat bestaat niet op de doelmachine.
Aanwezigheid van schema valideren	Schema <Name> does not exist/ already exist	Het schema op de doelmachine bestaat / bestaat niet.
Aanwezigheid van schemamachtiging valideren	Validate <Permissions> schema tables user permissions existence	DB-gebruiker heeft onvoldoende machtigingen

Validatie	Foutmelding	Beschrijving
Aanwezigheid van schematabellen valideren	Schema Tables <Tables> on the database: <Tables> already exist	De schematabellen in de database bestaan al.
Aanwezigheid van gebruikersmachtigingen schematabellen valideren	The database user does not have the correct permissions	De databasegebruiker beschikt niet over de juiste machtigingen.
UCMDB-verbinding controleren	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	De testverbinding met UCMDB is met de opgegeven verbindings-instellingen mislukt.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	De bestaande UCMDB-versie moet 9.03 met CUP 2 of hoger zijn.
DB-verbinding controleren	The host name/IP address validation failed	De opgegeven database-hostnaam/het opgegeven IP-adres is niet bereikbaar.
	The username or password validation failed	De opgegeven gebruikers-gegevens zijn ongeldig.
	The port validation failed	De opgegeven database-poort is niet bereikbaar.
	The SID validation failed	De opgegeven database-SID bestaat niet in de DB.
Installatie controleren	The product is already installed	Het product is al op de doelhost geïnstalleerd.

Configuration Manager upgraden

Alvorens te beginnen controleert en valideert de upgradeprocedure automatisch:

- of de verbinding met de UCMDB-server werkt.
- of de CUP 2-patch is geïnstalleerd voor UCMDB.
- of de JMX-poort correct is.

Als een van deze onderdelen niet correct geïnstalleerd of geconfigureerd is, ziet u een foutmelding die u hierover informeert. U kunt het aangegeven probleem oplossen en vervolgens de upgrade uitvoeren.

- Als de upgrade mislukt omdat u geen verbinding kunt maken met UCMDB, controleert u of de UCMDB-server actief is.
- Als de upgrade mislukt omdat de patch niet is geïnstalleerd, installeert u CUP 2 volgens de instructies die u kunt vinden op: http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- Als de upgrade mislukt vanwege een onjuiste UCMDB JMX-poort, selecteert u de juiste JMX-poort. U doet dit door de eigenschap ucmdb.jmx.port in het bestand **upgrade.properties** te wijzigen. Dit bestand bevindt zich in de map **<installatiemap van Configuration Manager>\utilities\Upgrade**.

Voer de volgende stappen uit om te upgraden:

Opmerking: Controleer of de UCMDB-server actief is als u met de upgradeprocedure begint.

---

1. Maak een back-up van uw Configuration Manager- en UCMDB-schema's.
2. Zoek het bestand **setup-win64.msi** in de Windows-submap van het installatiemedium van Configuration Manager.
3. Dubbelklik op het bestand om de installatiewizard van Configuration Manager uit te voeren.
4. Klik op **Next** om de pagina van de licentieovereenkomst voor de eindgebruiker te openen.
5. Ga akkoord met de voorwaarden van de licentie en klik op **Next** om de pagina Customer Information te openen.
6. Voer uw gegevens in en klik op **Next** om de pagina Setup Type te openen.
7. Selecteer de map waar Configuration Manager wordt geïnstalleerd. Zorg ervoor dat u een andere locatie selecteert dan de locatie die voor de vorige versie werd gebruikt.

   Configuration Manager wordt standaard geïnstalleerd in de volgende map: **c:\hp\cnc920**. Klik op **Next** om de standaardlocatie te accepteren, of klik op **Browse** om een andere locatie te selecteren en klik vervolgens op **Next**.

   Opmerking: De naam van de installatiemap mag geen geen spaties bevatten.

   ---

8. Klik op **Next** om te bevestigen en de installatie te starten.

   Nadat de installatiewizard voltooid is, wordt de wizard voor voltooiing van de installatie van Configuration Manager automatisch gestart.
9. Klik op **Next** totdat u wordt gevraagd of u een nieuwe installatie van Configuration Manager wilt uitvoeren of een upgrade.
10. Selecteer **Upgrade** en klik op **Next**.

11 Als de installatie voltooid is, controleert u het bestand **post_installation.log** (dit bestand bevindt zich in de map **<installatiemap van Configuration Manager/tmp/log**) om na te gaan of de installatie zonder fouten is voltooid.

Als er tijdens het upgraden een fout optreedt, verschijnt er een melding en kunt u de wizard sluiten. Als dit gebeurt, neem dan contact op met HP Support.

12 Start de Configuration Manager-service.

Opmerking: Na het upgraden moet u de SSL-configuratie nogmaals uitvoeren. Zie "Hardening" op pagina 89 voor meer informatie.

3

HP Universal CMDB Configuration Manager installeren op een Linux-platform

Belangrijk: Zorg ervoor dat u de releaseopmerkingen voor de meest actuele installatie-instructies leest.

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Configuratie voorafgaand aan de installatie

In dit gedeelte worden tevens de volgende onderwerpen behandeld:

Vereisten

- Minimaal 400 MB vrije schijfruimte
- X-display aanbevolen

Het bestand setup.bin ophalen

Het Linux-installatiebestand (**setup.bin**) bevindt zich op het installatiemedium of op de ISO-image die u kunt downloaden van de website van HP. Open het bestand op een van de volgende manieren:

➤ Activeer een dvd op uw Linux-machine:

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ Koppel een ISO-bestand als loopback-block-device:

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ Kopieer het bestand **setup.bin** naar een tijdelijke locatie op uw Linux-machine.

Configuration Manager installeren

In deze taak wordt beschreven hoe u Configuration Manager op uw server installeert en hoe u de databaseverbinding en de UCMDB-integratie configureert.

Als u een X-display hebt, verschijnt de wizard voor voltooiing van de installatie in de gebruikersinterface. Hebt u geen X-display, dan wordt de wizardinformatie weergegeven in de consolemodus.

Opmerking: De stappen in deze handleiding zijn van toepassing op de consolemodus. Er verschijnen echter vergelijkbare stappen als u de wizard van de gebruikersinterface gebruikt.

Configuration Manager installeren:

1 Als u Configuration Manager op uw huidige positie wilt installeren, voert u de volgende opdracht uit:

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 Er wordt een gebruiksrechtovereenkomst (EULA) weergegeven waarmee u akkoord dient te gaan. Druk herhaaldelijk op de spatiebalk om door de EULA omlaag te schuiven tot u het einde van de EULA bereikt. Typ **yes** en druk op **Enter** om akkoord te gaan en door te gaan met de installatie.

HP Universal CMDB Configuration Manager wordt geïnstalleerd in de huidige positie in de submap **cnc**.

Welkomstpagina

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Druk op **Enter** om door te gaan naar de volgende pagina.

Databaseleverancier selecteren

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Druk op **Enter** om Oracle te selecteren of typ **2** en druk op **Enter** om Microsoft te selecteren.

Database-hostnaam

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ de hostnaam van uw database en druk op **Enter**. De standaardwaarde van de hostnaam is **localhost**.

Databasepoort

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

De standaardpoort voor Oracle is 1521, de standaardpoort voor Microsoft is 1433. Als u een ander poortnummer wilt gebruiken, typt u het nummer hier en drukt u op **Enter**.

SID of databasenaam

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Voor Oracle wordt in dit veld de database-SID opgegeven. Voor Microsoft wordt in dit veld de databasenaam opgegeven. Typ een geldige waarde en druk op **Enter**.

Gebruikersnaam en schemawachtwoord

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ uw gebruikersnaam voor de database en druk op **Enter**.

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ uw schemawachtwoord en druk op **Enter**.

Databaseverbinding testen

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om uw databaseverbinding te testen.

Aangezien deze wizard tabellen in het databaseschema probeert te maken, wordt sterk aanbevolen uw databaseverbinding te testen. Als u de verbinding niet wilt testen, typt u **No** en drukt u op **Enter**.

Zodra het testen van de databaseverbinding voltooid is, verschijnt de volgende melding:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om door te gaan. Als er tijdens de verbindingstest een fout optreedt, verschijnt er een foutmelding en wordt u gevraagd de test nogmaals uit te voeren. Los het verbindingsprobleem op, voer de test nogmaals uit en ga verder met de installatie.

Hostnaam toepassingsserver

```
<============================>
Application Server Configuration
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

De standaardwaarde voor de hostnaam is de werkelijke hostnaam van de machine. Als u de installatie uitvoert achter een netwerktaakverdeling of een reverse proxy, voert u hier de externe naam in.

Poorten van de toepassingsserver aanpassen

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Als u de standaardpoorten voor Configuration Manager wilt gebruiken, drukt u op **Enter**. Als u aangepaste poorten wilt gebruiken, typt u **Yes** en drukt u op **Enter**. De standaard poortnummers zijn:

Poortnaam	Poortnummer
HTTP	8180
HTTPS	8443
Tomcat management	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

Als u ervoor kiest om de poorten aan te passen, wordt u voor elke poort die hierboven is vermeld gevraagd een waarde in te voeren. Typ voor elke poort de nieuwe waarde en druk op **Enter**:

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Initiële gebruiker met beheerdersrechten

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Er wordt een initiële gebruiker met beheerdersrechten gemaakt, die bij de eerste aanmelding fungeert als beheerder of hoofdgebruiker van het systeem. Typ de gewenste gebruikersnaam voor de beheerder en druk op **Enter**.

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ het wachtwoord voor de beheerder en druk op **Enter**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ ter bevestiging nogmaals het wachtwoord voor de beheerder en druk op **Enter**.

Integratiegebruiker

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Kies een naam voor de UCMDB-integratiegebruiker. Deze gebruiker wordt tijdens dit post-installatieproces in UCMDB gemaakt. HP adviseert om een gebruikersnaam te kiezen waaruit duidelijk blijkt dat deze voor integratie is bestemd (bijvoorbeeld cm_integration). Typ de gekozen gebruikersnaam en druk op **Enter**.

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ het wachtwoord voor de integratiegebruiker en druk op **Enter**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ ter bevestiging nogmaals het wachtwoord voor de integratiegebruiker en druk op **Enter**.

Hostnaam HP Universal CMDB-server

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Typ de hostnaam voor de UCMDB-server en druk op **Enter**. Waarschijnlijk komt deze naam niet overeen met de standaard localhost, omdat het niet wordt aanbevolen om in een productieomgeving zowel UCMDB als Configuration Manager op dezelfde machine te installeren.

HP Universal CMDB-serverpoort

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om het standaard poortnummer (8080) voor de UCMDB-server te accepteren, of typ een ander poortnummer en druk op **Enter**.

HP Universal CMDB-serverprotocol

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om HTTP te gebruiken, of typ 2 en druk op **Enter** om HTTPS te gebruiken.

Opmerking: Als u HTTPS selecteert, moet u sleutels uitwisselen met UCMDB. Zie "Hardening" op pagina 89 voor meer informatie. In deze procedure wordt HTTPS ingesteld met een niet-beveiligd, zelfondertekend certificaat.

Klant van de HP Universal CMDB-server

```
Customer:
----
Set
----
         = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om de standaard klantnaam voor de UCMDB-server te accepteren, of typ een andere klantnaam en druk op **Enter**.

Sysadmin-gegevens HP Universal CMDB-server

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Voer de sysadmin-gebruikersnaam voor de UCMDB-server in. Dit is de gebruiker die JMX-methoden op de UCMDB--server mag uitvoeren. Deze wordt niet tijdens de installatie gemaakt maar is een bestaande gebruiker. Neem contact op met uw UCMDB-serverbeheerder om de gegevens voor de sysadmin-gebruiker te verkrijgen.

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Typ het wachtwoord voor de sysadmin-gebruiker van de UCMDB-server en druk op **Enter**.

Verbinding van de HP Universal CMDB-server testen

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om de UCMDB-serververbinding te testen. Aangezien deze wizard probeert pakketten te implementeren en de UCMDB-server te configureren, wordt sterk aanbevolen om de serververbinding te testen. Als u de verbinding niet wilt testen, typt u **No** en drukt u op **Enter**.

Zodra het testen van de serververbinding voltooid is, verschijnt de volgende melding:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Druk op **Enter** om door te gaan. Als er tijdens de verbindingstest een fout optreedt, verschijnt er een foutmelding en wordt u gevraagd de test nogmaals uit te voeren. Los het verbindingsprobleem op, voer de test nogmaals uit en ga verder met de installatie.

Overzicht

De wizard toont een overzicht van alle selecties die u hebt gemaakt, alvorens deze daadwerkelijk uit te voeren:

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Database
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Druk op **Enter** om door te gaan met de configuratiefase. Tijdens het uitvoeren van de configuratie wordt een voortgangsbalk weergegeven. De wizard voert de volgende taken uit:

1. Databasetabellen en -objecten maken.
2. Database invullen met standaard- en beginwaarden.
3. Initiële gebruiker met beheerdersrechten maken.
4. Integratiegebruiker in de UCMDB-server maken.
5. UCMDB-server consolideren.
6. Geautoriseerde status in de UCMDB-server maken.
7. Configuration Manager-pakketten implementeren op de UCMDB-server.

Zodra de configuratie voltooid is, verschijnt de volgende melding:

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Druk op **Enter** om de wizard af te sluiten.

Optie voor installatie op de achtergrond

U kunt Configuration Manager op de achtergrond installeren (stille modus). In deze modus worden alleen de bestanden van het installatiepakket uitgepakt. Er worden na de installatie geen configuraties uitgevoerd. Als u de installatie in de stille modus wilt uitvoeren, voert u de volgende opdracht uit:

```
$ /path/to/installation/kit/setup.bin –silent
```

De Configuration Manager-toepassingsserver uitvoeren

Als u Configuration Manager wilt uitvoeren, gebruikt u de volgende opdrachten:

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

U kunt in de map **/etc/init.d** een script maken om Configuration Manager automatisch te starten tijdens het opstarten van de machine.

4

Aanmelden bij Configuration Manager

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Configuration Manager openen

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

Voor meer informatie over webbrowservereisten en de minimumvereisten voor de weergave van Configuration Manager raadpleegt u "Ondersteuningsmatrix" op pagina 14.

Voor meer informatie over beveiligde toegang tot Configuration Manager raadpleegt u "Hardening" op pagina 89.

Voor meer informatie over probleemoplossing bij het openen van Configuration Manager raadpleegt u "Probleemoplossing" op pagina 123.

Aanmelden bij Configuration Manager

1. Voer in de webbrowser de URL van de Configuration Manager-server in, bijvoorbeeld http://<servernaam of IP-adres>.<domeinnaam>:<poort>/cnc, waarbij <**servernaam of IP-adres**>.<**domeinnaam**> de volledig gekwalificeerde domeinnaam (FQDN) van de Configuration Manager-server is en <**poort**> de poort is die tijdens de installatie werd geselecteerd.
2. Voer de gebruikersnaam en het wachtwoord in dat u in de wizard voor voltooiing van de installatie van Configuration Manager hebt ingevoerd.
3. Klik op **Aanmelden**. Na het aanmelden verschijnt de gebruikersnaam in de rechterbovenhoek van het scherm.
4. (Aanbevolen) Maak verbinding met de LDAP-organisatieserver en wijs administratieve rollen toe aan LDAP-gebruikers om het voor Configuration Manager-beheerder mogelijk te maken om toegang te krijgen tot het systeem. Voor meer informatie over de toewijzing van rollen in het Configuration Manager-systeem raadpleegt u "Gebruikersbeheer" in de *Gebruikershandleiding* voor *HP Universal CMDB Configuration Manager*.

Afmelden

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

Klik op **Afmelden** boven aan de pagina.

Opmerking: Standaard verloopt de sessie na 30 minuten.

De JMX-console voor Configuration Manager openen

Indien u problemen moet oplossen of bepaalde configuraties moet aanpassen, moet u mogelijk de JMX-console gebruiken.

U opent de JMX-console als volgt:

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

5

Extra use-cases

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Een installatie van Configuration Manager naar een andere machine verplaatsen

Gebruik deze procedure als u een installatie van Configuration Manager van een machine naar een andere machine wilt verplaatsen, terwijl het databaseschema intact blijft en met dezelfde UCMDB-server verbinding wordt gemaakt.

1. Voer in de map **<installatiemap van Configuration Manager>\cnc\bin** de volgende opdracht uit: edit-server-0.bat.
2. Noteer alle parameters die u ziet, inclusief poorten (bijvoorbeeld JMX-poorten).
3. Stop de Configuration Manager-server op de bronmachine (als de bronmachine op een Windows-systeem is geïnstalleerd, moet u hiervoor de Configuration Manager-service stoppen).

4 Installeer Configuration Manager op de doelmachine:

   ➤ Onder Windows: voer het bestand **setup-win64.msi** uit (dit bestand bevindt zich in de map **\windows** van het installatiemedium).

   ➤ Onder Linux: voer de instructies uit die beschreven zijn in "Configuration Manager installeren" op pagina 44.

5 Annuleer de wizard voor voltooiing van de installatie als deze wordt geopend.

6 Kopieer alle bestanden uit de vorige installatiemap op de bronmachine naar de locatie van de nieuwe installatie op de doelmachine.

7 Wijzig op de doelmachine in de bestanden **client-config.properties** en **resources.properties** (deze bevinden zich in de map **\conf**) de hostnaam in de naam van de doelmachine.

Opmerking: Als de doelmachine zich in een ander domein bevindt dan de bronmachine, wijzigt u tevens de oude domeinverwijzing in het bestand **lwssofmconf.xml**.

---

8 Voer op de doelmachine het bestand **bin/create-windows-service.bat** uit om de Windows-service te maken. Stel de vlag **-h** in om de beschikbare opties te zien en gebruik indien nodig de parameters van de bron-machineservice (die u hebt genoteerd in stap 2). Voor de domein-naamparameter gebruikt u server-0. Als de standaardwaarden worden gebruikt, ziet de opdracht er als volgt uit:

   c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 Start de Configuration Manager-server op de doelmachine.

Poortnummers wijzigen na de installatie

1. Stop de Configuration Manager-server.
2. Maak een back-up van de inhoud van de map **<installatiemap van Configuration Manager>\servers\server-0**.
3. Verwijder de map **<installatiemap van Configuration Manager>\servers\server-0**.
4. Voer het script **create-node.bat** uit met de vlag **-h** om de beschikbare opties te zien. Geef alle vereiste poortnummers door aan het hulpprogramma.
5. Wijzig op de doelmachine in de bestanden **client-config.properties** en **resources.properties** (deze bestanden bevinden zich in de map **\conf**) het poortnummer in het nieuwe HTTP-poortnummer.
6. Voer het script **edit-server-0.bat** uit. Dit script bevindt zich in de map **<installatiemap van Configuration Manager>\bin**.
7. (Voor Windows-systemen) In het venster Properties van HP Universal CMDB Configuration Manager dat wordt geopend, klikt u op het tabblad Java en wijzigt u de instellingen voor **jmx.http.port** en **com.sun.management.jmxremote.port** in de nieuwe poortnummers.
8. Start de Configuration Manager-service op de doelmachine.

Systeeminstellingen naar een ander systeem kopiëren

1. Open Configuration Manager op de bronmachine. Ga naar **Systeem** > **Instellingen** en klik op de knop **Configuratieset exporteren naar een ZIP-bestand**.

   Voordat u gaat exporteren kunt u specifieke onderdelen van de configuratie uitsluiten. Schakel hiervoor het selectievakje naast het betreffende configuratie-item uit.
2. Kopieer de geëxporteerde configuratie naar de doelmachine.
3. Open Configuration Manager op de doelmachine. Ga naar **Systeem** > **Instellingen** en klik op de knop **Configuratieset importeren**.

Back-ups maken en terugzetten

U kunt een back-up maken van een installatie van Configuration Manager, zodat u problemen kunt oplossen waarvoor anders een volledig nieuwe installatie vereist zou zijn.

Back-up maken

Maak een back-up van de volgende gegevens:

- de submappen **conf** en **security** in de installatiemap van Configuration Manager (dit kan worden gedaan terwijl het systeem actief is, zonder het te hoeven onderbreken)
- het databaseschema

Back-up terugzetten (op een Windows-systeem)

Deze procedure moet worden uitgevoerd op een nieuw systeem dat geen installatie van Configuration Manager bevat.

1. Installeer Configuration Manager op de doelmachine door het bestand **setup-win64.msi** (in de map **\windows** van het installatiemedium) als volgt in stille modus uit te voeren:

   ```
   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
   ```

2. Zet de mappen **conf** en **security** terug. Gebruik de methode voor het terugzetten van de back-up die overeenkomt met de methode die u hebt gebruikt om de back-up te maken. Overschrijf de mappen die zijn gemaakt tijdens de installatie die u hebt uitgevoerd in stap 1.
3. Zet het databaseschema terug. Als u de back-up op een andere databaseserver terugzet, moet u de eigenschap **url** in het bestand **database.properties** (in de map **conf**) aanpassen zodat deze overeenkomt met de naam van de nieuwe databaseserver.
4. Gebruik het hulpprogramma **create-windows-service** (met de vlag **-h** om de beschikbare opties te zien) om een Windows-service te maken.
5. Start de Configuration Manager-server.

Back-up terugzetten (op een Linux-systeem)

1. Installeer Configuration Manager op de doelmachine door het bestand **setup.bin** uit te voeren (dit bestand bevindt zich op het installatie-medium). Raadpleeg voor meer informatie "Configuration Manager installeren" op pagina 44 (u moet echter de installatie annuleren in de eerste stap van de wizard voor voltooiing van de installatie). Alle bestanden worden geïmplementeerd, maar de configuratie van uw systeem wordt ongedaan gemaakt.
2. Zet de mappen **conf** en **security** terug. Gebruik de methode voor het terugzetten van de back-up die overeenkomt met de methode die u hebt gebruikt om de back-up te maken. Overschrijf de mappen die zijn gemaakt tijdens de installatie die u hebt uitgevoerd in stap 1.
3. Zet het databaseschema terug. Als u de back-up op een andere databaseserver terugzet, moet u de eigenschap **url** in het bestand **database.properties** (in de map **conf**) aanpassen zodat deze overeenkomt met de naam van de nieuwe databaseserver.
4. Start de Configuration Manager-server.

6

Geavanceerde configuratie

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Geavanceerde databaseverbindingsopties

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

Opmerking: Ga als volgt te werk als u een geavanceerde configuratie uitvoert op een Linux-systeem:

- Wijzig de richting van de slashes in de instructies in forward-slashes (/).
- Vervang in scriptuitvoeringen **.bat** door **.sh**.

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

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

  Bijvoorbeeld:

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

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

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

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

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

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

Databaseconfiguratie - MLU-ondersteuning (Multi-Lingual Unit)

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

Oracle-serverinstellingen

In de onderstaande tabel vindt u de vereiste instellingen voor Oracle Server:

Optie	Ondersteund	Aanbevolen	Opmerkingen
Tekenset	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Microsoft SQL Server-instellingen

In de onderstaande tabel vindt u de vereiste instellingen voor Microsoft SQL Server:

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

Opmerking:

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

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

Single Sign-On (SSO)

Single sign-on tussen Configuration Manager en UCMDB wordt uitgevoerd met behulp van de LWSSO-technologie van HP. Zie "LW-SSO-verificatie (Lightweight Single Sign-On) – Algemene referentie" op pagina 119 voor meer informatie.

In dit gedeelte worden de volgende onderwerpen behandeld:

LW-SSO inschakelen tussen Configuration Manager en UCMDB

Sommige gebruikers van Configuration Manager zijn ook gemachtigd om zich bij UCMDB aan te melden. Configuration Manager biedt een handige rechtstreekse koppeling met de gebruikersinterface van UCMDB (selecteer **Beheer** > **UCMDB Foundation**). Als u SSO wilt gebruiken (zodat u zich niet bij UCMDB hoeft aan te melden nadat u zich bij Configuration Manager hebt aangemeld), moet u LW-SSO inschakelen voor zowel Configuration Manager als UCMDB en controleren of beide toepassingen met dezelfde initString werken. Deze taak moet handmatig worden uitgevoerd, tenzij de taak al werd uitgevoerd als onderdeel van de installatie van Deployment Manager.

LW-SSO inschakelen:

1. Bewerk in de installatiemap van Configuration Manager het bestand **\conf\lwssofmconf.xml**.
2. Zoek het volgende gedeelte:

   enableLWSSO enableLWSSOFramework="true"

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

3 Zoek het volgende gedeelte:

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

en voer na <**domein**> het domein van de Configuration Manager-server in.

4 Zoek het volgende gedeelte:

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

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

5 Zoek het volgende gedeelte:

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

Opmerking: Het tweede DNS-domein moet alleen worden toegevoegd als Configuration Manager en een andere toepassing zich in verschillende domeinen bevinden.

Verwijder het opmerkingenteken aan het begin en voer (indien nodig) alle serverdomeinen in de DNSDomain-elementen in (in plaats van This value should be replaced by your application domain of This value should be replaced by domain of other application). De lijst moet het serverdomein bevatten dat werd ingevoerd in stap 3 op pagina 75.

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

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

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

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

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

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

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

11 Selecteer de methode **setInitString**. Voer dezelfde initString in die u voor Configuration Manager hebt ingevoerd in stap 4 op pagina 75 en klik op **Invoke**.

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

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

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

LW-SSO configureren in Operations Orchestration

Als LW-SSO zowel in Configuration Manager als in Operations Orchestration (OO) is ingeschakeld, kunnen gebruikers die zijn aangemeld bij Configuration Manager zich via de webtier bij Operations Orchestration aanmelden zonder een gebruikersnaam en wachtwoord (voor systeembeheerders) te hoeven opgeven.

Opmerking:

- In de volgende procedure staat <OO_HOME> voor de basismap van Operations Orchestration.
- Voor LW-SSO is vereist dat de accounts die worden gebruikt voor aanmelding bij Operations Orchestration en Configuration Manager dezelfde accountnaam hebben (wel mogen de accounts verschillende wachtwoorden hebben).
- Voor LW-SSO is vereist dat de account in Operations Orchestration geen interne account is.

LW-SSO configureren in Operations Orchestration:

1. Stop de RSCentral-service.
2. Activeer in **<OO_HOME>\Central\WEB-INF\applicationContext.xml** de importoptie tussen LWSSO_SECTION_BEGIN en LWSSO_SECTION_END, zoals hieronder weergegeven:

```
<!--  LWSSO_SECTION_BEGIN-->
        <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 Activeer in <**OO_HOME**>**Central****WEB-INF****web.xml** alle filters en toewijzingen tussen LWSSO_SECTION_BEGIN en LWSSO_SECTION_END, zoals hieronder weergegeven:

```
<!-- LWSSO_SECTION_BEGIN  -->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
    ......
    </filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
       <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
     <filter-mapping>
          <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
     </filter-mapping>
     <filter-mapping>
          <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
     pattern>/*</url-pattern>
          </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4 Bewerk in <**OO_HOME**>**Central****conf****lwssofmconf.xml** de volgende twee parameters:

- domain: domeinnaam van de OO-server.
- initString: moet overeenkomen met de initString-waarde in de LW-SSO-configuratie van OO (minimumlengte: 12 tekens). Bijvoorbeeld: smintegrationlwsso.

Bijvoorbeeld:

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation  id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 Start de RSCentral-service opnieuw op om de configuratie van kracht te laten worden.

Identity Manager-verificatie uitvoeren

In deze taak wordt beschreven hoe u HP Universal CMDB Configuration Manager configureert om Identity Manager-verificatie te accepteren.

U moet deze taak uitvoeren als u Identity Manager gebruikt en HP Universal CMDB Configuration Manager wilt toevoegen.

In deze taak worden de volgende stappen behandeld:

➤ "Vereisten" op pagina 80

➤ "HP Universal CMDB Configuration Manager configureren om Identity Manager te accepteren" op pagina 80

Vereisten

De Configuration Manager Tomcat-server moet verbonden zijn met uw webserver (IIS of Apache) en door uw Identity Manager via een Tomcat Java (AJP13)-connector beveiligd zijn.

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

HP Universal CMDB Configuration Manager configureren om Identity Manager te accepteren

Tomcat Java (AJP13) met IIS6 configureren:

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

   Bijvoorbeeld:

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

   a. Activeer de functie door het opmerkingenteken te verwijderen.

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

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

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

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

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

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

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

In deze taak wordt beschreven hoe Java Connector moet worden geïnstalleerd en geconfigureerd zodat Identity Management kan worden geconfigureerd voor gebruik met Configuration Manager terwijl IIS6 wordt uitgevoerd op het besturingssysteem Windows 2003.

Java Connector installeren en configureren voor IIS6 onder Windows 2003:

1 Download de recentste versie van Java Connector (bijvoorbeeld **djk-1.2.21**) van de Apache-website.

a Klik op http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/.

b Selecteer de recentste versie.

c Download het bestand **isapi_redirect.dll** uit de map **amd64**.

2 Sla dit bestand op in <**installatiemap van Configuration Manager**>**tomcat****bin****win32**.

3 Maak een nieuw tekstbestand met de naam **isapi_redirect.properties** in de map die ook isapi_redirect.dll bevat.

Dit bestand heeft de volgende inhoud:

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=<installatiemap van Configuration Manager>\servers
\server-0\logs\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file==<installatiemap van Configuration Manager>\tomcat
\conf\workers.properties.minimal
# Full path to the uriworkermap.properties file
worker_mount_file==<installatiemap van Configuration Manager>\tomcat
\conf\uriworkermap.properties
```

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

Dit bestand heeft de volgende inhoud:

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
        worker.list=ajp13w
        worker.ajp13w.type=ajp13
        worker.ajp13w.host=localhost
        worker.ajp13w.port=8009
#END
```

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

Dit bestand heeft de volgende inhoud:

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

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

/cnc|/*=ajp13w

---

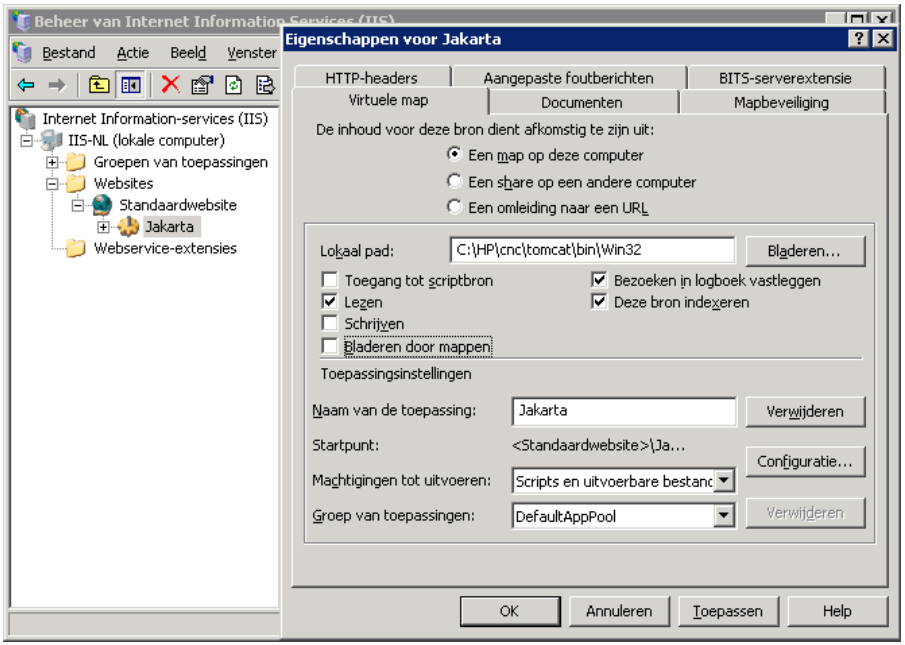
6 Maak de virtuele map in het bijbehorende websiteobject in de IIS-configuratie.

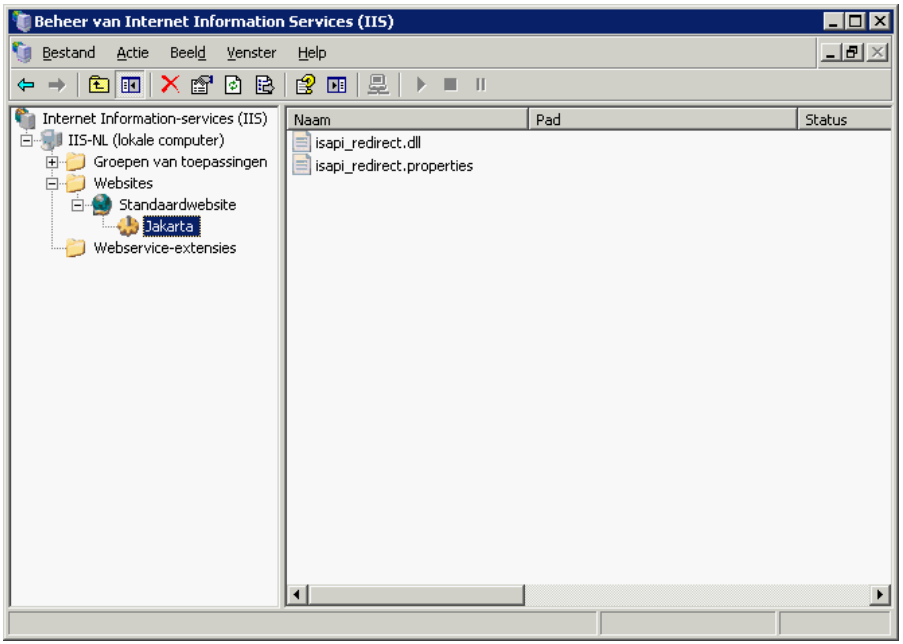
a Open in het startmenu van Windows **Instellingen** > **Configuratiescherm** > **Systeembeheer** >**Beheer van Internet Information Services (IIS)**.

b In het rechterdeelvenster klikt u met de rechtermuisknop op **<Naam lokale computer>\Websites\<Naam van uw website>** en selecteert u **Nieuw\Virtuele map**.

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

Het venster van IIS-beheer ziet er ongeveer zo uit:





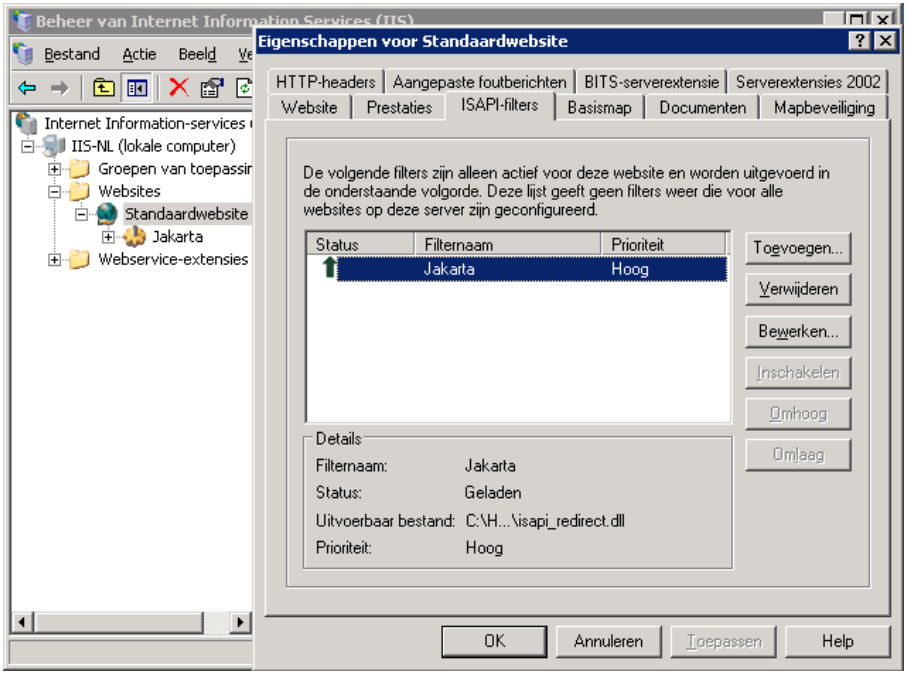
7 **Isapi_redirect.dll** toeveoegen als ISAPI-filter.

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

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

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

Het configuratievenster ziet er ongeveer zo uit:



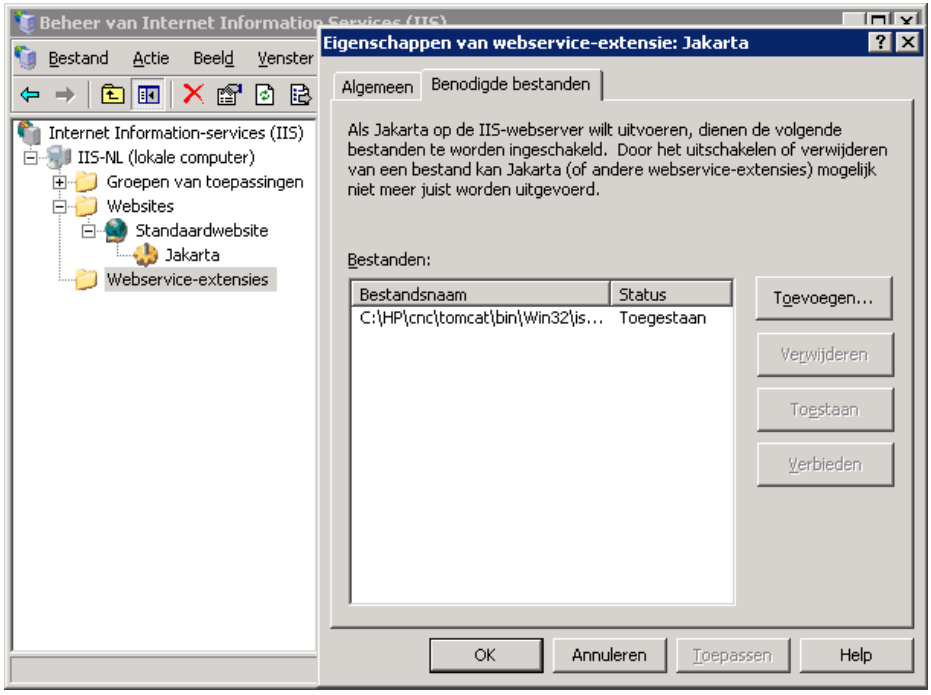
d Klik op de knop **Toepassen**.

8 Definieer een nieuwe webservice-extensie en sta deze toe.

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

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

Opmerking: Voordat u op **OK** klikt, moet u het selectievakje **Status van extensie instellen op Toegestaan** inschakelen.



9 Start de IIS-webserver opnieuw en open de toepassing via de webservice.

IPv6-ondersteuning

Configuration Manager ondersteunt alleen IPv6-URL's voor klant-URL's.

Werken met Configuration Manager met behulp van een IPv6-adres:

1. Controleer of uw besturingssysteem zowel IPv6 als IPv4 ondersteunt. Raadpleeg voor meer informatie de documentatie van het besturingssysteem.
2. Open het bestand **client-config.properties** in de map **<installatiemap van Configuration Manager>/conf** en wijzig de volgende waarden:
   - Wijzig de waarde van de parameter **bsf.server.url** en zorg ervoor dat deze de hostnaam gebruikt. Bijvoorbeeld:

     bsf.server.url=http://mijncomputer:8080/bsf

   - Wijzig de waarde van de parameter **bsf.server.services.url** en zorg ervoor dat de Configuration Manager-URL het hostnaamadres is. Bijvoorbeeld:

     bsf.server.services.url=http://<naam van Configuration Manager-host>:<poort van Configuration Manager>/bsf

3 Open het Tomcat-bestand **servers\server-0\conf\server.xml** en wijzig de volgende waarden:

➤ Voeg de IPv6-adressen toe aan de SHUTDOWN-hook door **address="[::]"** toe te voegen aan de volgende tag:

<Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

➤ Dupliceer de HTTP-connector. Voeg voor de tweede connector het IPv6-adres [::] toe. Bijvoorbeeld:

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ Dupliceer de AJP-connector. Voeg voor de tweede connector het IPv6-adres [::] toe. Bijvoorbeeld:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 Voeg de omgevingsvariabele toe aan de server: useIPv6="true":

Open het bestand **edit_server-0.bat** in de map <**installatiemap van Configuration Manager**>/**bin**. Voeg in het tabblad Java de volgende eigenschap toe aan de Java-opties: -DuseIPv6.

5 Start de server opnieuw op.

LDAP

Het is mogelijk om LDAP te configureren binnen Configuration Manager. Raadpleeg voor meer informatie "Systeeminstellingen" in de *Gebruikershandleiding van HP Universal CMDB Configuration Manager*.

Hardening

In dit gedeelte worden de volgende onderwerpen behandeld**:**

Opmerking: Na het upgraden moet u de SSL-configuratie nogmaals uitvoeren. Zie "Configuration Manager upgraden" op pagina 40 voor meer informatie.

Beveiliging van Configuration Manager

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

Configuration Manager is ontworpen om deel uit te kunnen maken van een beveiligde architectuur en is daardoor bestand tegen eventuele beveiligingsproblemen waaraan de toepassing blootgesteld kan zijn.

In de beveiligingsrichtlijnen wordt de configuratie besproken die vereist is voor een beter beveiligde (hardened) implementatie van Configuration Manager.

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

Aanbevolen voorbereiding voordat u begint met de beveiliging van uw systeem:

- Breng de beveiligingsrisico's en de beveiligingsstatus van uw algemene netwerk in kaart en beslis op basis van uw conclusies hoe u Configuration Manager het beste in uw netwerk kunt integreren.
- Zorg ervoor dat u goed inzicht hebt in het technische framework van Configuration Manager en de beveiligingsmogelijkheden van Configuration Manager.
- Lees alle beveiligingsrichtlijnen door.
- Controleer of Configuration Manager volledig functioneel is voordat u de beveiligingsprocedures start.
- Voer de stappen van de beveiligingsprocedure in elk gedeelte chronologisch uit.

Belangrijk:

- De beveiligingsprocedures zijn gebaseerd op de veronderstelling dat u uitsluitend de instructies implementeert die in de volgende paragrafen worden beschreven en dat u geen beveiligingsstappen uitvoert die elders beschreven zijn.
- Waar de beveiligingsprocedures gericht zijn op een bepaalde gedistribueerde architectuur, betekent dit niet per definitie dat dit ook de meest geschikte architectuur is voor uw organisatie.
- Verondersteld wordt dat de procedures in de volgende paragrafen worden uitgevoerd op machines die speciaal zijn toegewezen aan Configuration Manager. Als de machines behalve voor Configuration Manager ook voor andere doeleinden worden gebruikt, kunnen er problemen optreden.
- De beveiligingsinformatie in dit gedeelte is niet bedoeld als leidraad om de beveiligingsrisico's voor uw computersystemen te beoordelen.

Databasewachtwoord coderen

Het databasewachtwoord is opgeslagen in het bestand **<installatiemap van Configuration Manager>\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. Meer informatie over de parameters die voor het coderen worden gebruikt, vindt u in "Coderingsparameters" op pagina 92.

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 **<installatiemap van Configuration Manager>\conf\encryption.properties** en bewerk de volgende velden:
   - **engineName.** Voer de naam van het coderingsalgoritme in.
   - **keySize.** Voer de grootte van de hoofdsleutel in voor het geselecteerde algoritme.
2. Voer het script **generate-keys.bat** uit. Dit script maakt de volgende map: **cnc920\security\encrypt_repository** en genereert de coderingssleutel.
3. Voer het hulpprogramma **bin\encrypt-password** 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**.

Coderingsparameters

In de onderstaande tabel vindt u de parameters die zijn opgenomen in het bestand **encryption.properties** dat voor de databasewachtwoordcodering wordt gebruikt. Zie "Databasewachtwoord coderen" op pagina 91 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.

SSL inschakelen op de servermachine met een zelfondertekend certificaat

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 als toepassingsserver.

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

---

1 Vereisten

Voordat u de onderstaande procedure gaat uitvoeren, moet u het oude **tomcat.keystore**-bestand verwijderen. Dit bestand bevindt zich op de volgende locatie: **<installatiemap van Configuration Manager>\java\lib\security\tomcat.keystore**.

2 Een server-keystore genereren

Maak een keystore (JKS-type) 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 wachtwoord van de keystore in. Indien het wachtwoord gewijzigd is, moet u het handmatig in het bestand wijzigen.

➤ Beantwoord de vraag wat uw **voor- en achternaam** is. Voer de naam van de Configuration Manager-webserver in. Voer alle overige organisatiespecifieke parameters in.

➤ 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.

Zie "Clientcertificaten" op pagina 101 voor meer informatie over het gebruik van clientcertificaten.

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

---

4 De configuratie-instellingen van de client controleren

Open het bestand **client-config.properties**. Dit bestand bevindt zich in de map **conf** van de installatiemap van Configuration Manager. Stel het protocol van **bsf.server.url** in op **https** en de poort op **8443**.

5 Het bestand server.xml wijzigen

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

Connector port="8443"

in de opmerkingen. 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 op pagina 94)
keystorePass="<wachtwoord>"

Maak de volgende regel tot commentaarregel:

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

6 De server opnieuw starten

7 De beveiliging van de server controleren

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

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

SSL inschakelen op de servermachine met een certificaat van een certificeringsinstantie

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

1 Vereisten

Voordat u met de volgende procedure begint, moet u het oude **tomcat.keystore**-bestand verwijderen. Dit bestand bevindt zich op de volgende locatie: **<installatiemap van Configuration Manager>\java\lib\security\tomcat.keystore**.

2 Een server-keystore genereren

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

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

➤ Voer een willekeurige tekenreeks in als wachtwoord voor het **pfx**-bestand. (U hebt dit wachtwoord aangevraagd toen u het keystore-type converteerde 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: **<installatiemap van Configuration Manager>\java\lib\security**.

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

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

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

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

3 De configuratie-instellingen van de client controleren

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

4 Het bestand server.xml wijzigen

Open het bestand **server.xml**. Dit bestand bevindt zich op de locatie **<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" />
```

5 De server opnieuw starten

6 De beveiliging van de server controleren

Om te controleren of de Configuration Manager-server beveiligd is, voert u in uw webbrowser de volgende URL in: **https://<Naam Configuration Manager-server of IP-adres>:8443/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 met een Client-certificaat

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 map **<installatiemap van Configuration Manager>\java\bin** op de servermachine.
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. Voer de wijzigingen door zoals beschreven in stap 5 op pagina 95.
   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 stap 7 op pagina 96.

SLL inschakelen voor uitsluitend verificatie

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

1. Volg een van de procedures voor het inschakelen van SLL op de servermachine zoals beschreven in "SSL inschakelen op de servermachine met een zelfondertekend certificaat" op pagina 94 tot en met stap 6 op pagina 96, of "SSL inschakelen op de servermachine met een certificaat van een certificeringsinstantie" op pagina 96 tot en met stap 5 op pagina 98.
2. Voer in de webbrowser de volgende URL in:
   http://<Naam Configuration Manager-server of IP-adres>:8180/cnc.

Clientcertificaatverificatie inschakelen

In deze taak wordt beschreven hoe u Configuration Manager instelt om certificaatverificatie aan clientzijde te accepteren.

1. Volg de procedure om SSL in te schakelen op de servermachine zoals beschreven in "SSL inschakelen op de servermachine met een zelfondertekend certificaat" op pagina 94.
2. Open het volgende bestand:
   <Configuration Manager installatiemap>\conf\lwssofmconf.xml.
   Zoek het gedeelte dat begint met in-client certificate. Bijvoorbeeld:

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

   Activeer de functie van het clientcertificaat door het opmerkingenteken te verwijderen.
3. Haal de gebruikersnaam uit het certificaat volgens de onderstaande procedure:
   a. De parameter **userIdentifierRetrieveField** geeft aan welk certificaatveld de gebruikersnaam bevat. De opties zijn:
      - **SubjectDN**
      - **SubjectAlternativeName**

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

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

c Indien **userIdentifierRetrieveMode** de waarde **FieldPart** heeft, geeft de parameter **userIdentifierRetrieveFieldPart** aan welk deel van het betreffende veld de gebruikersnaam is. De waarde is een codeletter gebaseerd op een legenda die in het certificaat zelf is gedefinieerd.

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

- Wijzig **bsf.server.url** zodat het HTTPS-protocol wordt gebruikt en wijzig de HTTPS-poort in de poort beschreven in "SSL inschakelen op de servermachine met een zelfondertekend certificaat" op pagina 94.
- Wijzig **bsf.server.services.url** zodat het HTTP-protocol wordt gebruikt en wijzig de poort in de oorspronkelijke HTTP-poort.

Clientcertificaten

In dit gedeelte worden de volgende onderwerpen behandeld**:**

Clientcertificaatgegevens

In deze sectie vindt u informatie over de gegevens van een clientcertificaat en hoe u een gebruikers-ID uit een clientcertificaat kunt halen.

- **Gebruikers-ID**

  De gebruikers-ID zijn de unieke gegevens van het clientcertificaat die worden gebruikt om de identiteit van de gebruiker aan te geven.

➤ **Basisgegevens van een clientcertificaat**

De basisgegevens van een clientcertificaat bevatten de volgende informatie:

Certificaatveld	Beschrijving
Versie	De versie van het gecodeerde certificaat. Voorbeeld: 1 (0x1)
Serienummer	Een positief geheel getal dat door de certificeringsinstantie aan elk certificaat wordt toegewezen. Voorbeeld: 0 (0x0)
Algoritme voor handtekening	De algoritme-ID voor het algoritme dat door de certificeringsinstantie wordt gebruikt om het certificaat te ondertekenen. Voorbeeld: md5WithRSAEncryption
Verlener	De entiteit die het certificaat heeft ondertekend en uitgegeven. Voorbeeld: CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com
Geldigheid	De tijdsinterval waarbinnen de certificeringsinstantie garandeert om de informatie over de status van het certificaat te onderhouden: ➤ **Geldig van**: bevat de datum waarop de geldigheidsduur van het certificaat aanvangt. Voorbeeld: Nov 25 04:34:49 2009 GMT ➤ **Geldig tot**. Bevat de datum waarop de geldigheidsduur van het certificaat eindigt. Voorbeeld: Nov 25 04:34:49 2010 GMT

Certificaatveld	Beschrijving
Onderwerp	De entiteit die is gekoppeld aan de openbare sleutel opgeslagen in het veld Openbare sleutel onderwerp.
Gegevens openbare sleutel onderwerp	Dit veld bevat de openbare sleutel en het algoritme waarmee de sleutel wordt gebruikt (bijvoorbeeld RSA, DSA of Diffie-Hellman).

Zie voor meer informatie: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" via

http://tools.ietf.org/html/rfc5280

➤ **Veld Onderwerp**

Het veld Onderwerp (ook wel Subject Distinguished Name of SubjectDN genoemd) bevat de entiteit die aan de openbare sleutel is gekoppeld.

Het veld Onderwerp bevat de volgende relevante attributen (en kan daarnaast ook andere attributen bevatten):

Onderwerp-attribuut	Beschrijving onderwerp-attribuut	Voorbeeld
CN	Algemene naam	CN=Bob BobFamily
emailAddress	E-mailadres	*emailAddress=bob@example.com*
C	Land	C=US
ST	Staat of provincie	ST=NY
L	Plaats	L=New York
O	Organisatie	O=Work Organization
OU	Organisatie-eenheid	OU=Managers

Als u de gebruikers-ID uit het onderwerp wilt ophalen, kunt u het volledige SubjectDN-veld of het SubjectDN-attribuut gebruiken.

➤ **Extensies voor clientcertificaatgegevens**

De extensies die voor X.509 v3-certificaten worden gedefinieerd, bieden methoden om extra attributen te koppelen aan gebruikers of openbare sleutels en de relaties tussen certificeringsinstanties te beheren. Het Veld Alternatieve naam voor onderwerp kan de gebruikers-ID bevatten.

➤ **Veld Alternatieve naam voor onderwerp**

Met de extensie Alternatieve naam voor het onderwerp kunnen identiteiten afhankelijk worden gemaakt van het onderwerp van het certificaat. Deze identiteiten kunnen naast of in plaats van de identiteit in het onderwerpveld van het certificaat worden opgenomen.

Het veld Alternatieve naam voor onderwerp kan de volgende identiteiten bevatten:

Identiteit	**Voorbeeld**
otherName	Other Name: Principal Name= *bobOtherAltName@example.com*
rfc822Name	RFC822 Name =*bobRFC822AltName@example.com*
dNSName	DNS Name=example1.com
x400Address	
directoryName	Directory Address: E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	IP Address=192.168.7.1
registeredID	Registered ID=1.2.3.4

Als u de gebruikers-ID uit de alternatieve naam voor onderwerp wilt ophalen, kunt een van de identiteiten gebruiken.

Configuratie

Configuration Manager gebruikt LW-SSO om de gebruikers-ID van een clientcertificaat op te halen. De volgende attributen worden door de clientcertificaat-handler gebruikt om LW-SSO te configureren om de gebruikers-ID op te halen:

Als u gegevens uit een clientcertificaat wilt ophalen, moet Configuration Manager worden geconfigureerd om aan te geven hoe de gebruikers-ID moet worden verkregen.

Daarbij moet worden beslist over de volgende onderwerpen:

- Welk veld moet worden gebruikt: SubjectDN of alternatieve naam voor onderwerp?
- Moet het volledige veld of slechts een deel van het veld worden gebruikt?
- Als een deel van het invoerveld wordt gebruikt, moet u daar een waarde aan geven: geef het onderwerp-attribuut op voor de SubjectDN of geef de identiteit op voor de alternatieve naam voor het onderwerp.

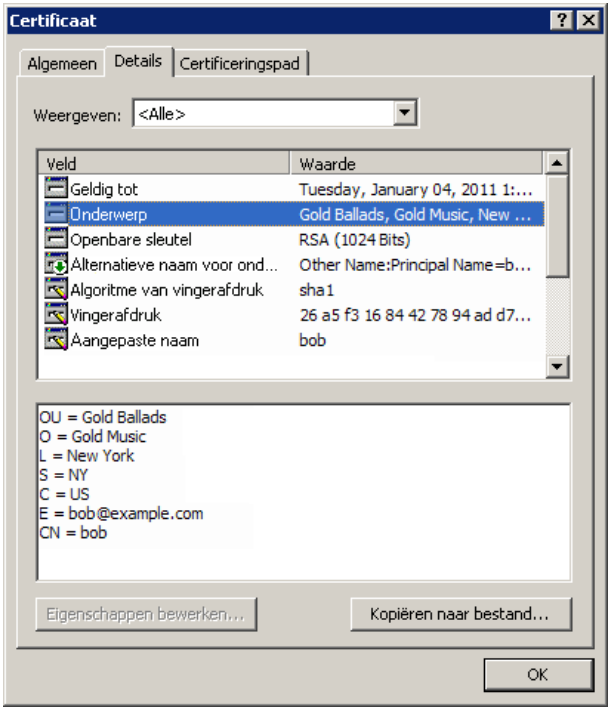
De clientcertificaat-handler gebruikt de volgende attributen om LW-SSO te configureren:

Attribuutnaam	Beschrijving
enabled	Geeft aan of de handler in- of uitgeschakeld is. **Belangrijk**: Het wordt sterk aanbevolen om de waarde expliciet in te stellen op False en de handler alleen in te schakelen als validatie van het clientcertificaat vereist is.
userIdentifierRetrieveField	Deze parameter geeft aan welk certificaatveld de gebruikers-ID bevat. De opties zijn: **SubjectDN** of **SubjectAlternativeName**.
userIdentifierRetrieveMode	De parameter userIdentifierRetrieveMode geeft aan of de gebruikers-ID uit de volledige inhoud van het betreffende veld bestaat of slechts een gedeelte van dat veld. De opties zijn: **EntireField** of **FieldPart**.

Attribuutnaam	Beschrijving
userIdentifierRetrieveFieldPart	Als de waarde van **userIdentifierRetrieveMode FieldPart** is, geeft deze parameter aan welk deel van het betreffende veld de gebruikersnaam is. De waarde is een codeletter gebaseerd op een legenda die in het certificaat zelf is gedefinieerd. **NB**: Dit veld mag niet leeg zijn als **userIdentifierRetrieveMode** is ingesteld op **FieldPart**. Tevens mag dit veld niet leeg zijn als **userIdentifierRetrievField** is ingesteld op **SubjectAlternativeName**.

Voorbeelden

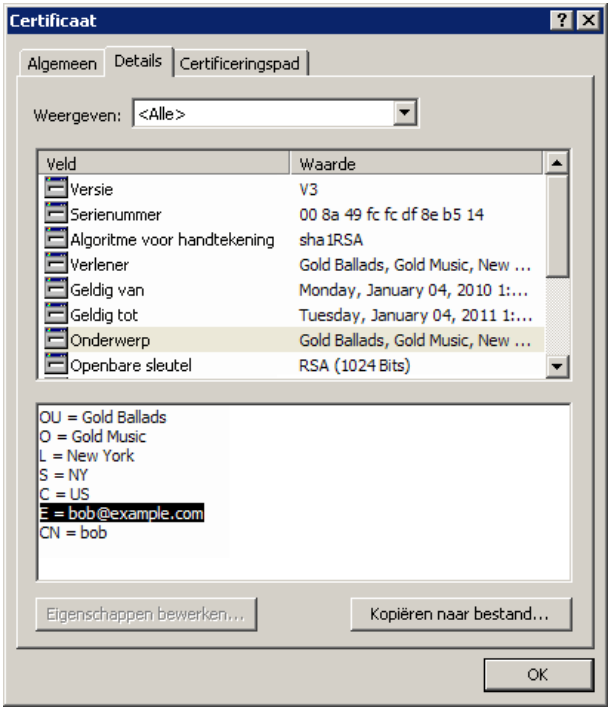
➤ De gebruikers-ID is opgenomen in het veld Onderwerp



Het volgende voorbeeld geeft aan hoe de handler moet worden geconfigureerd om de gebruikers-ID uit de volledige SubjectDN te halen:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

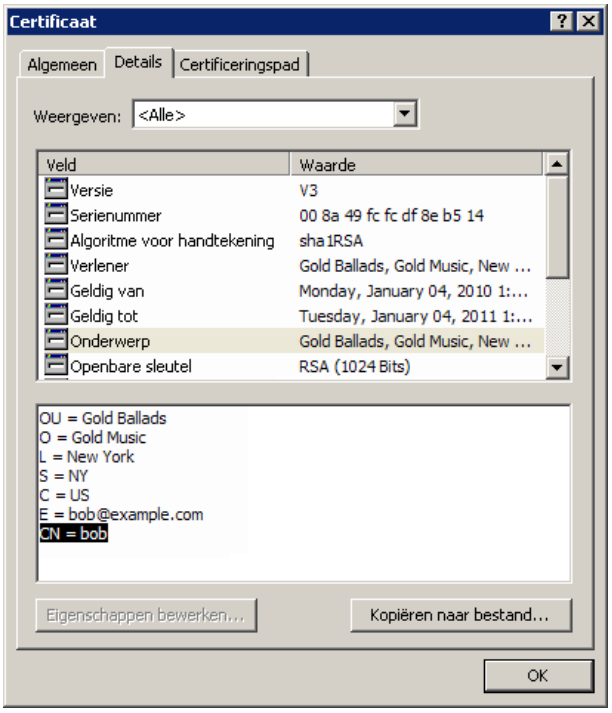
➤ **De gebruikers-ID is opgenomen in het e-mailveld**



Gebruik de namen van velden die zijn weergegeven in de legenda van het clientcertificaat. Het volgende voorbeeld geeft aan hoe de handler moet worden geconfigureerd om de gebruikers-ID uit het e-mailveld van Onderwerp te halen:

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

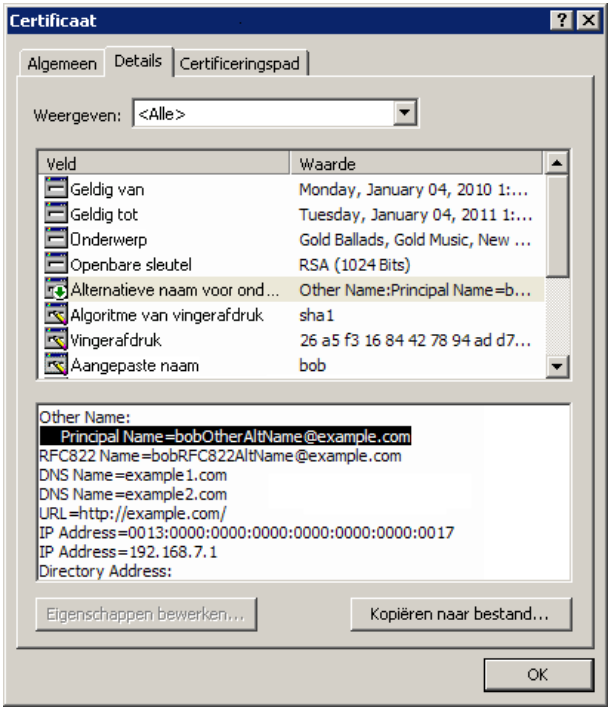
➤ **De gebruikers-ID is opgenomen in het veld Algemene naam**



Gebruik de namen van velden die zijn weergegeven in de legenda van het clientcertificaat. Het volgende voorbeeld geeft aan hoe de handler moet worden geconfigureerd om de gebruikers-ID uit het veld Algemene naam van Onderwerp te halen:

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

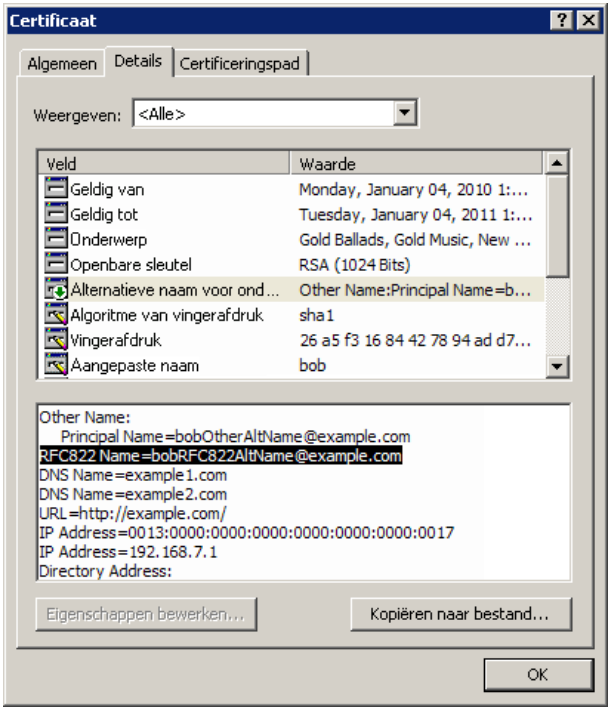
➤ **De gebruikers-ID is opgenomen in identiteit otherName van het veld Alternatieve naam voor onderwerp**



Gebruik de naam van de identiteit die wordt weergegeven in de legenda van het clientcertificaat. Het volgende voorbeeld geeft aan hoe de handler moet worden geconfigureerd om de gebruikers-ID van de identiteit otherName uit de alternatieve naam voor het onderwerp te halen:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **De gebruikers-ID is opgenomen in identiteit rfc822Name van het veld Alternatieve naam voor onderwerp**



Gebruik de naam van de identiteit die wordt weergegeven in de legenda van het clientcertificaat. Het volgende voorbeeld geeft aan hoe de handler moet worden geconfigureerd om de gebruikers-ID van de identiteit rfc822Name uit alternatieve naam voor het onderwerp te halen:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

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.

Het servercertificaat exporteren en in de truststore van de client gebruiken

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

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

2. Importeer het certificaat in de truststore van Configuration Manager (de standaard JRE-truststore):

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

3. Stel in Configuration Manager de eigenschappen voor de UCMDB-verbinding in:

   Ga naar **Systeem** > **Instellingen** > **Integraties** > **UCMDB Foundation** > **UCMDB Foundation**. Stel de verbindingsstrategie in op **HTTPS**, de UCMDB-serverpoort op de UCMDB HTTPS-poort en stel de toegangs-URL voor UCMDB in op https://<HostName>:8443.

4. Sla de configuratieset op en activeer hem. Start Configuration Manager opnieuw op.

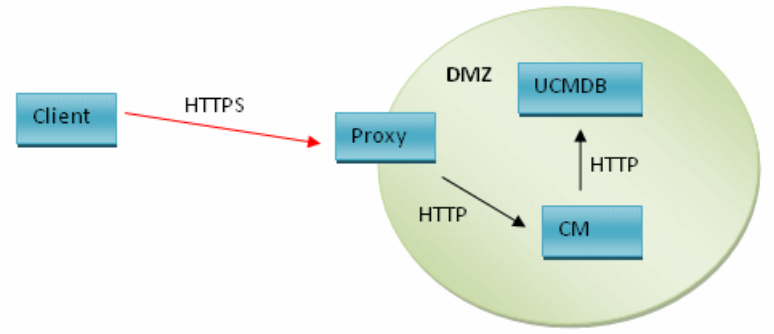
Als u Configuration Manager wilt configureren om via SSL (Secure Sockets Layer) met andere producten te werken (zoals netwerktaakverdelingen), importeert u het beveiligingscertificaat van het product in de truststore van Configuration Manager (standaard JRE-truststore) door de volgende opdracht uit te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

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

Reverse proxy

Als Configuration Manager en UCMDB zich in een DMZ bevinden, wordt aanbevolen om het systeem te configureren voor gebruik met een reverse-proxyserver. De configuratiestappen zijn hetzelfde als bij het configureren van UCMDB voor gebruik met een reverse proxy. Als u toegang tot Configuration Manager wilt inschakelen, moet u de paden **/cnc** en **/bsf** toewijzen aan de URL's van de externe server waarop Configuration Manager is geïnstalleerd.

De onderstaande afbeelding toont het configuratieproces voor een reverse proxy voor Configuration Manager:



Als de reverse proxy bijvoorbeeld Apache-server is, voegt u de volgende regels toe aan het bestand **Apache2.2\conf\extra\httpd-ssl.conf** en start u vervolgens de Apache-server opnieuw:

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
```

Voor verschillende soorten reverse proxy's kunnen verschillende configuratiestappen vereist zijn. Raadpleeg de documentatie van uw proxyserver voor meer informatie.

Een reverse proxy voor Configuration Manager configureren:

Wijzig het bestand **client-config.properties** in de map <**installatiemap van Configuration Manager**>**conf** als volgt:

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

De standaard HTTPS-poort van de Apache-proxy is 443.

Deel II

Bijlagen

A

Capaciteitslimieten

De volgende tabel geeft een overzicht van de capaciteitslimieten voor Configuration Manager:

Maximumaantal weergaven	100
Maximumaantal beleidsregels	300
Maximumaantal samengestelde CI's per weergave	5000
Maximumaantal gelijktijdige gebruikers	50
Maximumaantal samengestelde CI's in de module Configuratie-analyse	1000

B

LW-SSO-verificatie (Lightweight Single Sign-On) – Algemene referentie

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Overzicht LW-SSO-verificatie

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

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

Zie "LW-SSO – probleemoplossing en beperkingen" op pagina 137 voor meer informatie over het oplossen van problemen met LW-SSO.

In dit gedeelte worden de volgende onderwerpen behandeld:

Verloop van het LW-SSO-token

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

Aanbevolen configuratie van de verlooptijd van de LW-SSO

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

GMT-tijd

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

Ondersteuning voor meerdere domeinen

Voor ondersteuning van meerdere domeinen moeten voor alle toepassingen die deel uitmaken van LW-SSO-integratie de trustedHost-instellingen (of de instellingen voor **protectedDomains**) worden geconfigureerd indien deze moeten integreren met toepassingen van andere DNS-domeinen. Bovendien moet in het element **lwsso** van de configuratie het juiste domein worden toegevoegd.

SecurityToken ophalen voor URL-functionaliteit

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

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 toepassing maakt een token aan en elke toepassing 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 alleen worden gedeeld tussen toepassingen die met elkaar integreren met behulp van LW-SSO.
- ➤ De parameter **initString** moet minimaal 12 tekens lang zijn.

➤ **LW-SSO alleen inschakelen indien vereist.** LW-SSO moet uitgeschakeld zijn, behalve indien specifiek vereist.

➤ **Niveau van verificatiebeveiliging.** De toepassing die het zwakste verificatieframework gebruikt en die een LW-SSO-token uitgeeft dat door andere geïntegreerde toepassingen wordt vertrouwd, bepaalt het niveau van beveiligingsinformatie voor alle toepassingen.

Het wordt aanbevolen om alleen toepassingen met sterke en beveiligde verificatieframeworks een LW-SSO-token uit te laten geven.

- **Implicaties van symmetrische codering.** LW-SSO maakt gebruik van symmetrische cryptografie voor het uitgeven en valideren van LW-SSO-tokens. Daarom kan elke toepassing die een LW-SSO gebruikt, een token uitgeven dat wordt vertrouwd door alle andere toepassingen die dezelfde parameter **initString** delen. Dit risico is relevant wanneer een toepassing 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 garandeert geen gebruikerstoewijzing tussen de geïntegreerde toepassingen. Daarom moet de gebruikerstoewijzing worden gecontroleerd door de geïntegreerde toepassing. Wij raden u aan om hetzelfde gebruikersregister (als LDAP/AP) door alle geïntegreerde toepassingen te laten delen.

  Indien gebruikers niet worden toegewezen, kan dat leiden tot beveiligingsinbreuken en kan de toepassing ongewenst gedrag vertonen. Zo kan dezelfde gebruikersnaam worden toegewezen aan verschillende werkelijke gebruikers in de diverse toepassingen.

  In situaties waarin een gebruiker zich bij een toepassing (ToepA) aanmeldt en vervolgens een tweede toepassing (ToepB) opent die container- of toepassingverificatie gebruikt, leidt het niet-toewijzen van gebruikers er bovendien toe dat de gebruiker zich handmatig moet aanmelden bij ToepB en een gebruikersnaam moet invoeren. Indien de gebruiker een andere gebruikersnaam invoert dan de gebruikersnaam die werd gebruikt voor aanmelding bij ToepA, kan het volgende gedrag ontstaan: als de gebruiker vervolgens een derde toepassing (ToepC) toepassing van ToepA of ToepB opent, opent hij deze toepassing met behulp van de gebruikersnamen die werden gebruikt voor aanmelding bij respectievelijk ToepA of ToepB.
- **Identity Manager**. Indien gebruikt ter verificatie, moeten alle onbeschermde bronnen in de Identity Manager worden geconfigureerd met de instelling **nonsecureURLs** in het configuratiebestand LW-SSO.

C

Probleemoplossing

In dit hoofdstuk worden de volgende onderwerpen behandeld:

Probleemoplossing en beperkingen – algemeen

Beperkingen

U kunt een nieuw CI-type dat u in UCMDB hebt gemaakt pas zien nadat u zich bij Configuration Manager hebt afmeld en vervolgens weer hebt aangemeld.

Probleemoplossing

Probleem. Het attribuut **Name** van het knooppunt CI-type heeft niet de kwalificatie Bewaking op wijziging en wordt tijdens CI-autorisatie niet gekopieerd naar de geautoriseerde status. Dit gebeurt als Configuration Manager versie 9.20 is geïnstalleerd zonder Content Pack 9 voor UCMDB.

Oplossing. Voer een van de volgende stappen uit:

- Stel in CI-typebeheer binnen UCMDB het attribuut **Name** handmatig in op de kwalificatie Bewaking op wijziging.
- Installeer Content Pack 9.

Probleem. Als u de Configuration Manager-service start, krijgt u de volgende foutmelding:

> Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

Oplossing. Voer de volgende stappen uit:

1. Ga naar **<installatiemap van Configuration Manager>\cnc\bin** en voer de volgende opdracht uit:

   edit-server-0.bat

2. Selecteer het tabblad Startup. Selecteer in de vervolgkeuzelijst Mode (onderaan) **jvm** in plaats van **exe**.
3. Selecteer het tabblad Shutdown. Wijzig in het veld Class de laatste naam van **Boostrap** in **Bootstrap**.
4. Klik op **OK**.
5. Voer de service uit.

Deployment Manager – probleemoplossing en beperkingen

Voor het oplossen van problemen met Deployment Manager opent u het sessielogboek van de vorige sessie. Dit sessielogboek bevindt zich in de volgende map:

%temp%\HP\ucmdb-dm\Workspace\Sessions

Algemene richtlijnen voor herimplementatie

Tijdens de installatie dient u de waarschuwingen en fouten te controleren die worden weergegeven op de pagina Validation van Deployment Manager. Hiertoe klikt u op de detailknop naast elk geïmplementeerd onderdeel.

Zodra tijdens de implementatie een probleem is aangetroffen en daarvoor een oplossing is gevonden, voert u de volgende stappen uit:

1. Verwijder de installatie van de geïmplementeerde producten en start de machine opnieuw.
2. Start Deployment Manager opnieuw en voer alle configuraties nogmaals in.

Fouten tijdens de implementatie

Probleem. Machtigingsfout tijdens de implementatie.

Het sessielogboek geeft aan dat er tijdens het maken van een nieuw schema een probleem is opgetreden met de gebruikersmachtigingen voor de database.

Oplossing. Om een nieuwe database te kunnen maken moet u over de juiste machtigingen beschikken. Zorg ervoor dat de gebruikersgegevens die tijdens de implementatie zijn ingevoerd, geschikt zijn voor het maken van tabelruimten en schema's.

Probleem. Fout tijdens het maken van een schema of database in UCMDB.

Het sessielogboek geeft aan dat Deployment Manager een schema of database niet heeft kunnen maken.

Oplossing:

Opmerking: Het is niet mogelijk om een nieuw UCMDB-schema te maken en verbinding te maken met een bestaand UCMDB-geschiedenisschema (ongeacht het type databaseserver).

Controleer of het UCMDB-schema en het UCMDB-geschiedenisschema niet het volgende verbindingstype gebruiken:

- UCMDB-schema – nieuw schema maken
- UCMDB-geschiedenisschema – verbinding maken met een bestaand schema

Probleem. Fout tijdens het maken van een schema of database in UCMDB.

Het sessielogboek geeft aan dat het schema niet kon worden gemaakt.

Oplossing. Open het bestand session.log en zoek de volgende melding:
SQL error executing statement CREATE USER <schemanaam>

Als u in de pagina Database Configuration van Deployment Manager het Oracle-schema een naam geeft, zorg er dan voor dat u alleen letters (a-z), cijfers (0-9) en koppeltekens ('-') gebruikt.

Probleem. Het schema kan niet worden gemaakt omdat er onvoldoende ruimte beschikbaar is.

Oplossing. Vergroot de hoeveelheid vrije ruimte in het schema of de database. Gebruik de standaard beheerinterfaces die door Oracle en Microsoft worden geleverd.

Probleem. Het configureren van de database is mislukt en retourneert de volgende fout:
NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

Als u een MSSQL-server met NTLM-verificatie voor UCMDB-database-configuratie selecteert, mislukt de databaseconfiguratie en wordt een implementatiefout veroorzaakt.

Oplossing. Implementeer UCMDB op een lokale hostmachine (de enige plaats waar NTLM-verificatie wordt ondersteund).

Probleem. Databaseconfiguratiefout in Configuration Manager tijdens het configureren van een nieuwe database.

De volgende fouten kunnen in het detailvenster van Deployment Manager worden weergegeven:

> Failed to create Oracle schema due to error: ORA-01031: insufficient privileges

of

> Failed to create a schema to the database: machineName.
> Reason: ORA-01919: role 'RESOURCE' does not exist

Oplossing. Controleer of de databasegebruiker de volgende rolmachtigingen bezit:

- Connect
- Resource

Probleem. De implementatie kan niet worden uitgevoerd omdat er onvoldoende schijfruimte is op de doelhostmachine.

Oplossing. Meld u aan bij de doelhostmachine en controleer of er voldoende schijfruimte is om de implementatie te kunnen uitvoeren:

- UCMDB vereist 1 GB vrije ruimte
- Configuration Manager vereist 1 GB vrije ruimte
- DDMA vereist 1 GB vrije ruimte

Opmerking: Naast de vereisten voor de specifieke producten is nog 1GB extra vrije ruimte vereist voor het verwerken van tijdelijke bestanden.

Probleem. Pingen naar UCMDB-hulpprogramma mislukt.

Dit hulpprogramma wordt uitgevoerd vanaf de machine Configuration Manager en controleert of de verbinding met het bestaande UCMDB-exemplaar beschikbaar is. Open session.log en zoek het volgende bericht: Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

Oplossing:

- Controleer of poort 8080 op de doel-UCMDB niet wordt geblokkeerd door de Windows-firewall.
- Controleer of de CMDB-server toegankelijk is vanaf de Configuration Manager-machine en of de UCMDB-implementatie voltooid en actief is.

Verbinding met hostmachine niet beschikbaar

Probleem. RPC niet beschikbaar of onbekende fout.

Als u op de knop Test Connection klikt, wordt een fout weergegeven dat RPC niet beschikbaar is.

Oplossing. Corrigeer de hostnaam indien deze onjuist is. Controleer tevens of de WMI-service en de Server-services worden uitgevoerd en of de Windows-firewall de toegang tot de WMI-interface niet blokkeert.

Schakel de Windows-firewall uit of voeg een firewalluitzondering toe waarmee de toegang tot het externe beheer wordt ingeschakeld.

Hiertoe opent u het configuratiescherm **Firewall** en selecteert u **Regels voor binnenkomende verbindingen.** Schakel alle WMI-regels voor bestanden en printers in en schakel poort 8080 in.

Testverbinding mislukt

Probleem. Toegang geweigerd.

De toegang is geweigerd vanwege een onjuiste gebruikersnaam en/of een onjuist wachtwoord, ongeldige DNS-instellingen of omdat de gebruikersnaam die tijdens de implementatie is gebruikt geen beheerdersrechten op de doelhostmachine heeft.

Oplossing. Controleer of de opgegeven gebruikersgegevens correct zijn en of de gebruiker beheerdersrechten op de doelhostmachine heeft.

De toepassing kan niet worden geopend

Probleem. Na implementatie kan de toepassing (UCMDB of Configuration Manager) niet worden geopend.

Oplossing. Controleer of de volgende UCMDB- en Configuration Manager-services bestaan en worden uitgevoerd.

- Service **UCMDB_Server**
- Service **HPUCMDBCMoasisSNAPSHOTserver0**

Controleer de implementatielogboeken in de sessiemap op eventuele fouten.

LW-SSO is uitgeschakeld

Probleem. Implementatie geslaagd, LW-SSO-functionaliteit is uitgeschakeld.

Oplossing. Controleer of de initialisatiereeks en het domein voor LW-SSO op UCMDB en Configuration Manager (en OO, indien van toepassing) identiek zijn.

Controleer de configuratie-instellingen voor LW-SSO in de producten aan de hand van de volgende methoden:

- Configuration Manager – open het bestand **lwssofmconf.xml** en controleer de definities van het domein en de initialisatiereeks.
  Het bestand bevindt zich in de map **<installatiemap van Configuration Manager>\conf**.

➤ UCMDB – open UCMDB en selecteer **Managers** > **Beheer** > **Beheer infrastructuurinstellingen**.

Als Configuration Manager en UCMDB geïnstalleerd zijn op hostmachines met verschillende DNS-domeinen, controleer dan of de instellingen voor **Vertrouwde domeinen** beide DNS-domeinen bevatten en in beide producten zijn ingeschakeld.

Als u extra informatie over de implementatie wilt zien, kunt u Deployment Manager activeren in foutopsporingsmodus. De foutopsporingsmodus geeft aanvullende informatie over de implementatie.

U schakelt de foutopsporingsmodus als volgt in:

1. Voer Deployment Manager uit en open vervolgens een browservenster. Voer in de adresbalk %temp% in.
2. Navigeer naar de map **hp\ucmdb-dm**.
3. Open het **ini**-bestand in een teksteditor en voeg de volgende eigenschap toe aan de laatste regel van het bestand:

   –Ddebug.mode=true

4. Gebruik **%temp%\HP\ucmdb-dm\ucmdb-dm.exe** om Deployment Manager uit te voeren.

Configuration Manager openen – probleemoplossing en beperkingen

Beperkingen

➤ Telkens als de tijd op de Tomcat-server van Configuration Manager wordt gewijzigd, moet de server opnieuw worden gestart om de tijd op de server bij te werken.

Probleemoplossing

Probleem. Nadat de configuratieset in **Systeem** > **Instellingen** is gewijzigd, kan de server niet meer worden gestart.

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

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

   ```
   <installatiemap van Configuration Manager>\bin\export-cs.bat <database-eigenschappen> --history
   ```

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

   ```
   cd <installatiemap van Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties --history
   ```

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

   ```
   <installatiemap van Configuration Manager>\bin\export-cs.bat <database-eigenschappen> <configuratieset-ID> <naam dumpbestand>
   ```

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

   ```
   cd <installatiemap van Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
   ```

3. Stop de Configuration Manager-service.

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

   ```
   <installatiemap van Configuration Manager>\bin\import-cs.bat <database-eigenschappen> -i <naam dumpbestand > --activate
   ```

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

Oplossing. Een van de volgende fouten is mogelijk de oorzaak:

- De UCMDB-server is uitgevallen. Start Configuration Manager opnieuw op nadat UCMDB weer helemaal hersteld is (controleer of de status van de UCMDB-server inderdaad **Up** is).
- De UCMDB-server is actief maar de verbindingsreferenties of URL van Configuration Manager zijn onjuist. Start Configuration Manager. Ga naar **Systeem** > **Instellingen** > **Integraties** >**UCMDB Foundation** > **UCMDB Foundation**, wijzig de instellingen en sla de nieuwe configuratieset op. Activeer de configuratieset en start de server opnieuw op.

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

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

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

Oplossing. Start de Configuration Manager-server opnieuw op.

Probleem. Het Configuration Manager-logboek bevat de fout dat er een time-out is opgetreden bij de uitvoering van UCMDB.

Oplossing. Deze fout treedt op wanneer de UCMDB-database overbelast is. Om deze fout te corrigeren, kunt u de time-out van de verbinding als volgt verlengen:

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

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

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

- Max. aantal actieve server-TQL's
- Max. aantal actieve klanten-TQL's

Probleem. Het HTTPS-servercertificaat is niet geldig.

Oplossing. Een van de volgende fouten is mogelijk de oorzaak:

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

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

Oplossing. Een van de volgende fouten is mogelijk de oorzaak:

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

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

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

1. Open een opdrachtregel en voer de volgende opdracht uit om het bijgewerkte databasewachtwoord te coderen:

   <installatiemap van Configuration Manager>\bin\encrypt-password.bat –p <wachtwoord>

   waarbij het resultaat een gecodeerd wachtwoord is.

2. Kopieer het gecodeerde wachtwoord (inclusief het voorvoegsel {ENCRYPTED}) naar de parameter **db.password** in <**installatiemap van Configuration Manager**>**conf****database.properties**.

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

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

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

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

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

en kunt u de toepassing opnieuw starten in de browser.

Probleem. De Configuration Manager tomcat-server start niet.

Oplossing. Voer een van de volgende oplossingen uit:

- Start de wizard voor voltooiing van de installatie en vervang de serverpoorten van Configuration Manager.
- Breek het andere proces af dat de Configuration Manager-poorten bezet.
- Wijzig de poorten handmatig in de configuratiebestanden van Configuration Manager, door het volgende bestand te bewerken: **<installatiemap van Configuration Manager>\servers\server-0\conf\server.xml** en de betreffende poorten bij te werken:
  - HTTP (8180): regel 69
  - HTTPS (8443): regels 71, 90

Probleem. U ontvangt een melding dat er onvoldoende geheugen is.

Oplossing. Ga als volgt te werk om de opstartparameters van de server te wijzigen:

1. Voer het volgende batchbestand uit:

   <installatiemap van Configuration Manager>/bin/edit-server-0.bat

2. Wijzig de volgende instellingen:

   -Dapplication.ms=<oorspronkelijke grootte geheugengroep>
   -Dapplication.mx=<maximumgrootte geheugengroep>

Probleem. Nadat u op **Finish** hebt geklikt, duurt het lang voordat de wizard voor voltooiing van de installatie is afgesloten.

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

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

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

- Wacht enkele minuten. Standaard worden uitvoeringen van analyseprocessen elke 10 minuten herhaald. Deze waarde kunt u instellen in **Systeem** > **Instellingen**.
- Voer een JMX-aanroep uit om de offline-analysebewerking op de betreffende weergave uit te voeren.
- Ga naar **Beheer** > **Beleidsregels** > **Beleidsregels configuratie**. Klik op de knop **Beleidsanalyse herberekenen**. Hiermee wordt het offline-analyseproces voor alle weergaven geopend (dit kan enige tijd duren). Mogelijk moet u tevens een kunstmatige wijziging in een beleidsregel aanbrengen en deze opslaan.

Probleem. Als u klikt op **Beheer** > **UCMDB Foundation** wordt de aanmeldingspagina van UCMDB weergegeven.

Oplossing. Om toegang te krijgen tot UCMDB zonder u opnieuw aan te melden, moet u Single Sign-On inschakelen. Raadpleeg "Single Sign-On (SSO)" op pagina 74 voor meer informatie. Controleer tevens of de aangemelde gebruiker van Configuration Manager is gedefinieerd in het gebruikersbeheersysteem van UCMDB.

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

Oplossing. Ga als volgt te werk:

1. Ga naar **Systeem** > **Instellingen** > **Integraties** > **UCMDB Foundation** > **UCMDB Foundation**.
2. Voeg vierkante haken toe aan het IP-adres in de URL van UCMDB-toegang. De URL moet er zo uitzien: http://[x:x:x:x:x:x:x:x]:8080/.

3 Sla de configuratieset op en activeer hem.

4 Start Configuration Manager opnieuw op.

LW-SSO – probleemoplossing en beperkingen

Bekende problemen

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

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

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

Tevens 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 toepassing roept tijdens de afmeldingsprocedure meer dan drie opeenvolgende HTPP 302-omleidingsbewerkingen aan.

In dit geval is het mogelijk dat Internet Explorer 7 de HTTP 302-omleidingsreactie verkeerd verwerkt en dat in plaats daarvan een foutpagina **Internet Explorer cannot display the webpage** verschijnt.

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

Beperkingen

Bij het werken met LW-SSO-verificatie zijn de volgende beperkingen van toepassing:

- **Clienttoegang tot de toepassing**.

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

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

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

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

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

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

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

    De functionaliteit voor meerdere domeinen werkt niet wanneer u een koppeling maakt van een beveiligde pagina (HTTPS) naar een niet-beveiligde pagina (HTTP). Dit is een browserbeperking waarbij de referrerheader niet wordt verzonden wanneer een koppeling wordt gemaakt van een beveiligde naar een niet-beveiligde bron. Zie http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP voor een voorbeeld.

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

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

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

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

Probleemoplossing

Probleem: Na aanmelding is er geen LW-SSO-cookie gemaakt.

- **Mogelijke oorzaak:** In het LW-SSO-element van de configuratie is een niet-leeg domein onjuist gedefinieerd.
- **Mogelijke oplossing**: Zorg ervoor dat het domein dat in het LW-SSO-element van de configuratie is gedefinieerd, overeenkomt met het domein van de toepassing.
- **Mogelijke oorzaak:** Een niet-leeg domein dat als een parameter is doorgegeven aan de functie enableSSO, is onjuist.
- **Mogelijke oplossing**: Zorg ervoor dat het domein dat als een parameter is doorgegeven aan de functie enableSSO overeenkomt met het domein van de toepassing.
- **Mogelijke oorzaak:** U hebt de toepassing niet geopend met de volledig gekwalificeerde domeinnaam (FQDN) in de aanmeldings-URL toen een domein werd gedefinieerd in de LW-SSO-configuratie (bijvoorbeeld: http://192.168.12.13/WebApp).
- **Mogelijke oplossing**: Zorg ervoor dat u de toepassing opent met de volledig gekwalificeerde domeinnaam (FQDN) in de aanmeldings-URL (bijvoorbeeld: http://mijnserver.bedrijfsdomein.com/WebApp).

Probleem: LW-SSO kan geen cookie maken voor de functie AutoCookieCreation.

- **Mogelijke oorzaak:** In het LW-SSO-element van de configuratie is een onjuist domein gedefinieerd.
- **Mogelijke oplossing**: Zorg ervoor dat het domein dat in het LW-SSO-element van de configuratie is gedefinieerd, overeenkomt met het domein van de toepassing.

Probleem: Het LW-SSO-token is niet gevalideerd.

- **Mogelijke oorzaak:** De twee toepassingen hebben verschillende initString-parameters in het crypto-element van de configuratie (of andere crypto-parameters).

- **Mogelijke oplossing**: Gebruik in beide toepassingen dezelfde initString (naast alle overige crypto-parameters in het element voor het maken van LW-SSO).
- **Mogelijke oorzaak:** Het GMT-tijdsverschil tussen de twee toepassingen is meer dan 15 minuten.
- **Mogelijke oplossing**: Zorg ervoor dat alle toepassingen die deel uitmaken van een LW-SSO-integratie op dezelfde GMT-tijd zijn ingesteld, met een verschil van maximaal 15 minuten.
- **Mogelijke oorzaak:** In het LW-SSO-element van de configuratie is een domein leeg en u opent een tweede toepassing op een andere computer met hetzelfde DNS-domein.
- **Mogelijke oplossing**: Zorg ervoor dat het domein dat in het LW-SSO-element van de configuratie is gedefinieerd, overeenkomt met het domein van de toepassing.
- **Mogelijke oorzaak:** In het LW-SSO-element van de configuratie is een domein niet gedefinieerd en u opent een tweede toepassing op een andere computer met hetzelfde DNS-domein.
- **Mogelijke oplossing**: Voeg een domein toe aan het LW-SSO-element en zorg ervoor dat het domein zo is gedefinieerd dat het overeenkomt met het domein van de toepassing.

Probleem: LW-SSO kan het LW-SSO-token niet valideren in een omgeving met meerdere domeinen

- **Mogelijke oorzaak:** In de configuratie van een van de toepassingen is een domein in het LW-SSO-element onjuist gedefinieerd.
- **Mogelijke oplossing**: Het domein dat in het LW-SSO-element van de toepassingsconfiguratie is gedefinieerd, moet overeenkomen met het domein van de toepassing volgens de werkelijk gebruikte domeinen.
- **Mogelijke oorzaak:** In de configuratie van een van de toepassingen is een domein in de trustedHosts-instellingen (of de protectedDomains-instellingen) onjuist gedefinieerd.
- **Mogelijke oplossing**: Zorg ervoor dat de domeinen in de trustedHosts-instellingen (of de protectedDomains-instellingen) van alle configuraties van de toepassing correct zijn gedefinieerd.

- **Mogelijke oorzaak:** Internet Explorer 6.x, 7.x of 8.x wordt gebruikt en de cookie van de LW-SSO-sessie wordt geblokkeerd of geweigerd.
- **Mogelijke oplossing**: Voeg alle LW-SSO-servers toe aan de zone "Intranet"/"Vertrouwd" in de beveiligingszones van Internet Explorer op uw computer (Extra > Internetopties > Beveiliging > Lokaal intranet > Websites > Geavanceerd). Hierdoor worden alle cookies geaccepteerd.
- **Mogelijke oorzaak:** Sommige toepassingen hebben verschillende initString-parameters in het crypto-element van de configuratie (of andere crypto-parameters).
- **Mogelijke oplossing**: Gebruik dezelfde initString in alle toepassingen (naast alle overige crypto-parameters in het element voor het maken van LW-SSO).
- **Mogelijke oorzaak:** Sommige toepassingen hebben een GMT-tijdsverschil van meer dan 15 minuten.
- **Mogelijke oplossing**: Zorg ervoor dat alle toepassingen die deel uitmaken van een LW-SSO-integratie op dezelfde GMT-tijd zijn ingesteld, met een verschil van maximaal 15 minuten.
- **Mogelijke oorzaak:** Er loopt een koppeling voor meerdere domeinen van de beveiligde (HTTPS) naar de niet-beveiligde (HTTP) bron.
- **Mogelijke oplossing**: Als u een koppeling of kruisverbinding tussen domeinen maakt, controleer dan of de eerste koppelings- of kruisings-aanvraag van de ene beveiligde bron (HTTPS) naar een andere beveiligde bron (HTTPS) loopt.

IPv6-ondersteuning – probleemoplossing en beperkingen

Beperkingen

- De URL mag geen IP-adres bevatten.
- Het besturingssysteem moet zowel IPv6 als IPv4 ondersteunen. U kunt zich niet bij de Configuration Manager-server aanmelden als het IPv4-adres niet is gesloten of niet wordt ondersteund.
- Telkens als de tijd op de Tomcat-server van Configuration Manager wordt gewijzigd, moet de server opnieuw worden gestart om de tijd op de server bij te werken.

Probleemoplossing

Probleem. Nadat tijdens de installatie een UCMDB-verbinding met een IPv6-adres is geconfigureerd, werkt de menu-optie **Beheer** > **UCMDB Foundation** niet.

Oplossing. Ga als volgt te werk:

1. Ga naar **Systeem** > **Instellingen** > **Integraties** > **UCMDB Foundation** > **UCMDB Foundation**.
2. Voeg vierkante haken toe aan het IP-adres in het veld URL UCMDB-toegang. De URL moet er als volgt uitzien: http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Sla de configuratieset op en activeer hem.
4. Start Configuration Manager opnieuw op.

Verificatie – probleemoplossing en beperkingen

In dit hoofdstuk worden de bekende problemen met verificatie beschreven.

Probleem: Tijdens verificatie voor een toepassing na omleiding naar een verificatiepunt, ontvangt u fout 500.

- **Mogelijke oorzaak:** De .WAR en BSF.WAR van Configuration Manager hebben verschillende initString-parameters in het crypto-element van de configuratie (of andere crypto-parameters).
- **Mogelijke oplossing:** Gebruik in beide toepassingen dezelfde initString (naast alle overige crypto-parameters in het element voor het maken van LW-SSO).

Probleem: Tijdens verificatie voor een toepassing na omleiding naar een verificatiepunt, kunt u het aanmeldingsformulier niet zien.

Oplossing: De cookie van de Configuration Manager-verificatiesessie wordt bij gebruik van Internet Explorer versie 6.0, 7.0 of 8.0 geblokkeerd of geweigerd. Voeg de Configuration Manager-server toe aan de zone **Intranet/Vertrouwd** in de beveiligingszones van Internet Explorer op uw computer (**Extra** > **Internetopties** > **Beveiliging** > **Lokaal intranet** > **Websites** > **Geavanceerd**). Hierdoor worden alle cookies geaccepteerd.

Probleem: Na verificatie ontvangt u fout 403.

- **Mogelijke oorzaak:** In het LW-SSO-element van de toepassingsconfiguratie is een domein onjuist gedefinieerd.
- **Mogelijke oplossing:** Zorg ervoor dat het domein dat in het LW-SSO-element van de toepassingsconfiguratie is gedefinieerd, overeenkomt met het domein van de toepassing.
- **Mogelijke oorzaak:** U hebt de toepassing niet geopend met de volledig gekwalificeerde domeinnaam (FQDN) in de aanmeldings-URL toen een domein werd gedefinieerd in de LW-SSO-configuratie (bijvoorbeeld: http://192.168.12.13/WebApp).
- **Mogelijke oplossing:** Zorg ervoor dat u de toepassing opent met de volledig gekwalificeerde domeinnaam (FQDN) in de aanmeldings-URL (bijvoorbeeld: http://mijnserver.bedrijfsdomein.com/WebApp).

Probleem: Na verificatie verschijnt de pagina **Get Acegi User Details**.

Oplossing: De cookie van de Configuration Manager-verificatiesessie wordt bij gebruik van Internet Explorer versie 6.0, 7.0 of 8.0 geblokkeerd of geweigerd. Voeg de Configuration Manager-server toe aan de zone **Intranet/Vertrouwd** in de beveiligingszones van Internet Explorer op uw computer (**Extra** > **Internetopties** > **Beveiliging** > **Lokaal intranet** > **Websites** > **Geavanceerd**). Hierdoor worden alle cookies geaccepteerd.