HP Universal CMDB 9.10 Configuration Manager

Für Windows®-Betriebssysteme

Bereitstellungshandbuch

Datum der Dokumentveröffentlichung: November 2010
Datum des Software-Release: November 2010

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212; kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Urheberrechtshinweise

© Copyright 2010 Hewlett-Packard Development Company, L.P.

Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden bezeichnenden Informationen:

- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten:

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

Für diese Website müssen Sie sich für eine HP Passport-Benutzer-ID registrieren und sich anmelden. Hier können Sie sich für eine HP Passport-ID registrieren:

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

Oder klicken Sie auf den Link **Neue Benutzer – bitte jetzt registrieren!** auf der HP Passport-Anmeldeseite.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HP-Kundenbetreuer.

Support

Besuchen Sie die HP Software Support-Website unter:

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

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Supportleistungen von HP Software.

Der Online-Software-Support bietet Kunden mithilfe interaktiver technischer Support-Werkzeuge für die Unternehmensverwaltung die Möglichkeiten, ihre Probleme auf schnelle und effiziente Weise intern zu lösen. Als Valued Support Customer können Sie die Support-Website für folgende Aufgaben nutzen:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Support-Verträgen
- Nachschlagen von HP-Supportkontakten
- Einsehen von Informationen über verfügbare Services
- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Für die meisten Support-Bereiche müssen Sie sich als Benutzer mit einem HP Passport registrieren und anmelden. In vielen Fällen ist zudem ein Support-Vertrag erforderlich. Hier können Sie sich für eine HP Passport-ID registrieren:

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

Weitere Informationen zu Zugriffsebenen finden Sie unter:

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

Inhalt

1

Installation und Konfiguration

Dieses Kapitel umfasst die folgenden Themen:

Configuration Manager – Übersicht

Mit dem HP Universal CMDB Configuration Manager (Configuration Manager) können Sie Daten in Ihrem CMS analysieren und kontrollieren und es steht Ihnen eine Umgebung zur Steuerung der CMS-Infrastruktur zur Verfügung, die zahlreiche Datenquellen umfasst und unterschiedliche Produkte und Applikationen bereitstellt.

Die Bereitstellung von Configuration Manager in einer Unternehmensnetzwerkumgebung ist ein Prozess, der Ressourcenplanung und einen Systemarchitekturentwurf erfordert. Lesen Sie sich vor der Installation von Configuration Manager die Informationen in diesem Abschnitt sorgfältig durch, einschließlich der Informationen zu den Systemanforderungen.

Configuration Manager – Systemanforderungen

Serversystemanforderungen

Die folgende Tabelle beschreibt die Systemanforderungen für den Configuration Manager-Server:

CPU	Mindestens vier Intel Pentium 4-Prozessoren
Arbeitsspeicher (RAM)	Mindestens 4 GB
Plattform	x64
Betriebssystem	Die folgenden 64-Bit Windows-Betriebssysteme werden unterstützt: ➤ Windows 2003 Enterprise SP2 und R2 SP2 ➤ Windows 2008 Enterprise SP2 und R2

Datenbank	➤ Microsoft SQL Server 2005 SP2, 2005 Compatibility Mode 80, (Enterprise Editions) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB, Version 9.02 (Typische CMDB-Installation) Eine vollständige Liste der Systemanforderungen für diese Versionen finden Sie in der HP Universal CMDB-Dokumentation.

Clientanforderungen

Die folgende Tabelle beschreibt die Clientanforderungen zum Anzeigen von Configuration Manager:

Browser	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Flash Player-Browser-Plug-In	Flash Player 9 und höher
Bildschirmauflösung	➤ Mindestens 1024x768 ➤ Empfohlen 1280x1024
Farbqualität	Mindestens 16 Bit

Empfohlene Richtlinien für die Einrichtung

In der folgenden Tabelle sind Richtlinien für Optionen beim Einrichten von Configuration Manager aufgeführt.

LDAP	Die folgenden LDAP-Umgebungen werden unterstützt: ➤ Active Directory ➤ SunONE 6.x
Empfohlene Datenbankschema-Mindestgröße	2 GB

Configuration Manager – Kapazitätenbeschränkungen

In der folgenden Tabelle sind die Kapazitätenbeschränkungen für Configuration Manager aufgeführt.

Empfohlene maximale Anzahl an Ansichten	100
Empfohlene maximale Anzahl an Richtlinien	300
Empfohlene maximale Anzahl an zusammengesetzten CIs pro Ansicht	5000
Empfohlene maximale Anzahl an gleichzeitigen Benutzersitzungen	50

Konfigurieren der Datenbank oder des Benutzerschemas

Für die Verwendung von Configuration Manager müssen Sie ein Datenbankschema bereitstellen. Configuration Manager bietet Unterstützung für Microsoft SQL Server und Oracle Database Server. Im Rahmen dieser Aufgabe wird beschrieben, wie Sie Verbindungseigenschaften für die Configuration Manager-Datenbank oder das Benutzerschema mithilfe des Installationsassistenten konfigurieren.

Hinweis: Informationen zu den Systemanforderungen für Microsoft SQL Server und Oracle Server finden Sie unter "Serversystemanforderungen" auf Seite 8.

So konfigurieren Sie Ihre Datenbank:

1 Weisen Sie eine Microsoft SQL Server-Datenbank oder ein Oracle Server-Benutzerschema zu.

- Für **Microsoft SQL Server 2005**: Aktivieren Sie die Snapshotisolation.

  Führen Sie den folgenden Befehl einmal aus, sobald Sie die Datenbank erstellt haben:

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

  Weitere Informationen zur SQL Server-Snapshotisolationsfunktion finden Sie unter http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

- Für **Oracle**: Weisen Sie Oracle-Benutzern nur Verbindungs- und Ressourcenrollen zu.
  (Durch Erteilen der Berechtigung zur Auswahl aller Tabellen tritt bei der Schemaauffüllungsprozedur ein Fehler auf.)

2 Überprüfen Sie die folgenden Informationen, die Sie während des Konfigurationsprozesses benötigen:

✔	**Erforderliche Informationen**
	DB-Hostname und -Anschluss
	DB-Benutzername und -Kennwort
	Für Microsoft SQL: Datenbankname
	Für Oracle: SID

3 Führen Sie den Configuration Manager-Installationsassistenten aus. Weitere Informationen finden Sie unter "Installieren von Configuration Manager" auf Seite 12.

Installieren von Configuration Manager

Im Rahmen dieser Aufgabe wird beschrieben, wie Sie Configuration Manager auf Ihrem Server installieren und die Datenbankverbindung sowie die UCMDB-Integration konfigurieren. Sie können auf einer beliebigen Seite des Assistenten auf **Hilfe** klicken, um Unterstützung bei der Installation zu erhalten. Detaillierte Beschreibungen der Seiten des Assistenten finden Sie unter "Configuration Manager-Assistent für die Konfiguration nach der Installation" auf Seite 23.

So installieren Sie Configuration Manager:

1 Suchen Sie im Stammverzeichnis der Configuration Manager-DVD nach der folgenden Datei: **install.bat**.

2 Doppelklicken Sie auf die Datei, um den Configuration Manager-Installationsassistenten auszuführen.

3 Klicken Sie auf **Next** um die Seite mit dem Endbenutzer-Lizenzvertrag anzuzeigen.

4 Akzeptieren Sie die Bedingungen der angezeigten Lizenz und klicken Sie auf **Next**, um die Seite für die Produktinstallation zu öffnen.

5. Wählen Sie die zu installierenden Produkte aus (UCMDB und Configuration Manager) und geben Sie den Installationsspeicherort an. Wenn Sie über eine angepasste UCMDB-Lizenz verfügen, aktivieren Sie das entsprechende Kontrollkästchen. Klicken Sie auf **Next**, um die UCMDB-Installation zu starten. Für weitere Informationen zur UCMDB-Installation ziehen Sie die PDF-Datei mit dem *HP Universal CMDB-Bereitstellungshandbuch* heran.
6. Wenn die UCMDB-Installation und der Nachinstallationsprozess abgeschlossen sind, wird automatisch der Configuration Manager-Assistent für die Konfiguration nach der Installation gestartet.
7. Klicken Sie auf der Willkommensseite auf **Next**, um die Seite für die Konfiguration der Datenbankverbindung zu öffnen.
8. Wählen Sie den Datenbanktyp aus (Oracle oder Microsoft SQL Server) und geben Sie den Benutzernamen und das Kennwort ein. Es wird empfohlen, die Verbindung durch Klicken auf die Test-Schaltfläche zu testen. Wenn der Verbindungstest erfolgreich war, klicken Sie auf **Next**, um die Seite für die Konfiguration des Anwendungsservers zu öffnen.

Hinweis: Sie können nach Beendigung des Assistenten erweiterte Datenbankverbindungsoptionen konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren der erweiterten Datenbankverbindungsoptionen" auf Seite 15.

---

9. Geben Sie den Hostnamen ein und klicken Sie auf **Next**, um die Seite für die Windows-Dienstkonfiguration zu öffnen.
10. Wenn Sie Configuration Manager als Windows-Dienst installieren möchten, aktivieren Sie das entsprechende Kontrollkästchen. Klicken Sie auf **Next**, um die Seite für die Benutzeranmeldeinformationen anzuzeigen.
11. Geben Sie den Benutzernamen und das Kennwort für den Administrator und den Integrationsbenutzer ein. Klicken Sie auf **Next**, um die Seite Seite für die Konfiguration der HP UCMDB-Verbindung zu öffnen.

12 Wenn UCMDB bereits auf diesem oder einem anderen Computer installiert ist, stellen Sie sicher, dass der UCMDB-Server ausgeführt wird, bevor Sie fortfahren.

Wenn Sie UCMDB auf einem anderen Computer installieren, stellen Sie sicher, dass das entsprechende Kontrollkästchen aktiviert ist, und geben Sie die erforderlichen Parameter an. Es wird empfohlen, die Verbindung durch Klicken auf die Test-Schaltfläche zu testen. Wenn der Verbindungstest erfolgreich war, klicken Sie auf **Next**, um die Übersichtsseite für Nachinstallationsaktionen zu öffnen.

13 Lesen Sie die Informationen auf Übersichtsseite für Nachinstallationsaktionen. Wenn die Angaben korrekt sind, klicken Sie auf **Next**, um mit dem Nachinstallationsprozess fortzufahren.

14 Klicken Sie auf **Finish** auf der Seite zum Beenden, um die Nachinstallation abzuschließen.

15 Wenn dies nicht der erste Start von UCMDB ist, müssen Sie die Spaltengröße in UCMDB folgendermaßen ändern:

a Wechseln Sie zu **Verwaltung** > **Infrastructure Settings Manager**. Suchen Sie nach der Einstellung **Objektstamm** und ändern Sie sie in **data**. Melden Sie sich von UCMDB ab und melden Sie sich wieder an, damit die Änderungen wirksam werden.

b Wechseln Sie zu **Modellieren** > **CIT Manager**. Wählen Sie den CI-Typ **Data** in der Verzeichnisstruktur aus und wechseln Sie zur Registerkarte **Attribute**. Bearbeiten Sie das Attribut **User Label**, indem Sie **Wertgröße** in **900** ändern.

c Wechseln Sie zurück zu **Infrastructure Settings Manager** und ändern Sie die Einstellung **Objektstamm** wieder in den ursprünglichen Wert. Melden Sie sich ab und wieder an, damit die Änderungen wirksam werden.

16 Wenn Datenflussverwaltung bereits auf dem UCMDB-Server ausgeführt wurde, sind die Verlaufsdaten möglicherweise beschädigt. Führen Sie zum Beheben dieses Problems Folgendes aus:

a Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: http://<UCMDB-Serveradresse>.<Domänenname>:8080/jmx-console.

Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole an. Standardmäßig lauten diese wie folgt:

- Anmeldename = **sysadmin**
- Kennwort = **sysadmin**

b Wählen Sie unter **UCMDB** den Eintrag für die Historien-DB-Dienste aus.

c Wählen Sie die Methode **Fix902EndTimeRecords** aus.

d Geben Sie für den Kunden mit dem Status **Tatsächlich** den Wert **1** als Kunden-ID an und klicken Sie auf **Invoke**.

e Wenn der Vorgang erfolgreich war, wird eine Meldung angezeigt, die besagt, dass die Verlaufsdatenbank erfolgreich aktualisiert wurde.

f Geben Sie für den Kunden mit dem Status **Autorisiert** den Wert **100001** als Kunden-ID an und klicken Sie auf **Invoke**.

g Wenn der Vorgang erfolgreich war, wird eine Meldung angezeigt, die besagt, dass die Verlaufsdatenbank erfolgreich aktualisiert wurde.

Konfigurieren der erweiterten Datenbankverbindungsoptionen

Wenn Sie für Ihre Datenbankbereitstellung erweiterte Datenbankverbindungseigenschaften benötigen, können Sie diese nach Beendigung des Nachinstallationsassistenten festlegen. Configuration Manager unterstützt alle Datenbankverbindungsoptionen, die vom JDBC-Treiber des Herstellers unterstützt werden, und kann mit dem Datenbankverbindungs-URL konfiguriert werden. Um erweiterte Verbindungen zu konfigurieren, bearbeiten Sie die Eigenschaft **jdbc.url** in der Datei **<Configuration Manager-Installationsverzeichnis>\conf\database.properties**.

Im Folgenden werden Beispiele für erweiterte Optionen für Microsoft SQL Server aufgeführt:

- **Windows-Authentifizierung (NTLM).** Fügen Sie zum Anwenden der Windows-Authentifizierung die Domäneneigenschaft Ihrem JTDS-Verbindungs-URL in der Datei **database.properties** hinzu. Geben Sie die zu authentifizierende Windows-Domäne an.

  Beispiel:

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

- **SSL.** Weitere Informationen zum Sichern der Microsoft SQL-Serververbindung mit SSL finden Sie unter http://jtds.sourceforge.net/faq.html.

Im Folgenden werden Beispiele für erweiterte Optionen für Oracle Database Server aufgeführt:

- **Oracle-URL.** Geben Sie der Verbindungs-URL des systemeigenen Oracle-Treibers an. Geben Sie einen gültigen Oracle Server-Namen und eine gültige SID ein. Wenn Sie hingegen **Oracle RAC** verwenden, geben Sie die Oracle RAC-Konfigurationsdetails ein.

Hinweis: Detaillierte Informationen zum systemeigenen Oracle JDBC-URL-Format finden Sie unter http://www.orafaq.com/wiki/JDBC#Thin_driver.
Detaillierte Informationen zum Konfigurieren des URL für Oracle RAC finden Sie unter http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Weitere Informationen zum Sichern der Oracle-Verbindung mit SSL erhalten Sie in den folgenden Erläuterungen:
  - 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

Datenbankkonfiguration – MLU-Support (Multi-Lingual Unit)

Im folgenden Abschnitt werden die Datenbankeinstellungen beschrieben, die für die Unterstützung der Lokalisierung erforderlich sind.

Oracle Server-Einstellungen

In der folgenden Tabelle sind die erforderlichen Einstellungen für Oracle Server aufgeführt:

Option	Unterstützt	Empfohlen	Anmerkungen
Zeichensatz	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Microsoft SQL Server-Einstellungen

In der folgenden Tabelle sind die erforderlichen Einstellungen für Microsoft SQL Server aufgeführt:

<table>
<tr><th>Option</th><th>Unterstützt</th><th>Empfohlen</th><th>Anmerkungen</th></tr>
<tr><td>Sortierung</td><td>Groß-/Kleinschreibung wird nicht beachtet. Binäre Sortierreihenfolge und Unterscheidung nach Groß-/Kleinschreibung werden nicht unterstützt. Es wird ausschließlich eine Reihenfolge ohne Unterscheidung nach Groß-/Kleinschreibung mit einer Kombination von Akzent, Kana oder Einstellungen für die Breite unterstützt.</td><td>Verwenden Sie das Dialogfeld für die Sortiereinstellungen, um die Sortierung auszuwählen. Aktivieren Sie nicht das Kontrollkästchen für die Binäreinstellungen. Die Beachtung von Akzenten, Kana und Breite sollte nach den jeweils relevanten Anforderungen für Datensprachen ausgewählt werden. Die ausgewählte Sprache muss mit der Sprache der Ländereinstellungen des Windows-Betriebssystems übereinstimmen.</td><td rowspan="2">Beschränkt auf das Sortierungsgebietsschema und die standardmäßigen englischen Definitionen.</td></tr>
<tr><td>Collation Database-Eigenschaft</td><td colspan="2">Serverstandard</td></tr>
</table>

Hinweis:

Für alle Sprachen gilt Folgendes: **<Sprache>_CI_AS** ist die Mindestanforderung.
Wenn Sie beispielsweise in Japanisch die Optionen für die Berücksichtigung von Kana und Breite auswählen möchten, dann lautet die empfohlene Option: **Japanese_CI_AS_KS_WS** oder **Japanese_90_CI_AS_KS_WS**. Diese Empfehlung gibt an, dass bei den japanischen Zeichen Akzente, Kana und Breite berücksichtigt werden.

- **Unterscheidung nach Akzent (_AS).** Unterscheidet zwischen Zeichen mit und ohne Akzenten. Beispielsweise wird zwischen **a** und **á** unterschieden. Ist diese Option nicht ausgewählt, betrachtet Microsoft SQL Server die Buchstabenversionen mit und ohne Akzent bei der Sortierung als identisch.
- **Unterscheidung nach Kana (_KS).** Unterscheidet zwischen den beiden Typen der japanischen Kana-Zeichen: Hiragana und Katakana. Ist diese Option nicht ausgewählt, betrachtet Microsoft SQL Server Hiragana- und Katakana-Zeichen bei der Sortierung als identisch.
- **Unterscheidung nach Breite (_WS).** Unterscheidet zwischen einem Einzelbyte-Zeichen und demselben Zeichen, wenn es als Doppelbyte-Zeichen dargestellt wird. Ist diese Option nicht ausgewählt, betrachtet Microsoft SQL Server die Darstellung eines Zeichens als Einzelbyte-Zeichen und Doppelbyte-Zeichen bei der Sortierung als identisch.

Aktivieren von Lightweight Single Sign-On

Einige Configuration Manager-Benutzer verfügen zusätzlich über die Berechtigung, sich bei UCMDB anzumelden. Configuration Manager bietet diesen Benutzern einen bequemen, direkten Link zur UCMDB-Benutzeroberfläche (wählen Sie **Verwaltung** > **UCMDB öffnen** aus). Um Single Sign-On verwenden zu können (wodurch eine Anmeldung bei UCMDB nach dem Anmelden bei Configuration Manager nicht mehr erforderlich ist), müssen Sie LW-SSO für Configuration Manager und UCMDB aktivieren und sicherstellen, dass beide denselben initString-Parameter verwenden. Im Rahmen dieser Aufgabe wird beschrieben, wie Sie LW-SSO in Configuration Manager und UCMDB aktivieren.

So aktivieren Sie LW-SSO:

1 Öffnen Sie die folgende Datei im Configuration Manager-Installationsverzeichnis: **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

Hinweis: Diese Datei ist vor dem Starten von Configuration Manager nicht vorhanden.

---

2 Suchen Sie nach dem folgenden Abschnitt:

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

und stellen Sie sicher, dass der Wert **true** ist.

3 Suchen Sie nach dem folgenden Abschnitt:

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

und geben Sie die Configuration Manager-Serverdomäne nach **<Domäne>** ein.

4 Suchen Sie nach dem folgenden Abschnitt:

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

und ersetzen Sie "This string should be replaced" durch eine gemeinsam genutzte Zeichenfolge, die von allen vertrauenswürdigen Applikationen verwendet wird, die eine Integration mit LW-SSO aufweisen.

5 Suchen Sie nach dem folgenden Abschnitt:

```
<!--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-->
```

Entfernen Sie das Kommentarzeichen am Anfang und geben Sie die Configuration Manager-Serverdomänen in die DNSDomain-Elemente ein (anstelle von This value should be replaced by your application domain). Diese Liste sollte die Serverdomäne enthalten, die in Schritt 3 auf Seite 20 eingegeben wurde.

6 Speichern Sie die Datei mit Ihren Änderungen und starten Sie den Server neu.

7 Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: http://<UCMDB-Serveradresse>.<Domänenname>:8080/jmx-console.

Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole an. Standardmäßig lauten diese wie folgt:

- Anmeldename = **sysadmin**
- Kennwort = **sysadmin**

8 Wählen Sie unter **UCMDB-UI** den Eintrag **LW-SSO Configuration** aus, um die Seite **JMX MBEAN View** anzuzeigen.

9 Wählen Sie die Methode **setEnabledForUI** aus, legen Sie den Wert auf **true** fest und klicken Sie auf **Invoke**.

10 Wählen Sie die Methode **setDomain** aus. Geben Sie den Domänennamen des UCMDB-Servers ein und klicken Sie auf **Invoke**.

11 Wählen Sie die Methode **setInitString** aus. Geben Sie denselben initString-Parameter ein, den Sie für Configuration Manager in Schritt 4 auf Seite 21 eingegeben haben, und klicken Sie auf **Invoke**.

12 Wenn sich Configuration Manager und UCMDB in getrennten Domänen befinden, wählen Sie die Methode **addTrustedDomains** aus und geben Sie die Domänennamen der UCMDB- und Configuration Manager-Server ein. Klicken Sie auf **Invoke**.

13 Um die LW-SSO-Konfiguration so anzuzeigen, wie sie im Einstellungsmechanismus gespeichert ist, wählen Sie die Methode **retrieveConfigurationFromSettings** aus und klicken Sie auf **Invoke**.

14 Um die tatsächlich geladene LW-SSO-Konfiguration anzuzeigen, wählen Sie die Methode **retrieveConfiguration** aus und klicken Sie auf **Invoke**.

IPv6-Unterstützung

Configuration Manager unterstützt IPv6-URLs nur im Fall von URLs für Kunden.

So verwenden Sie Configuration Manager mithilfe einer IPv6-Adresse:

1 Stellen Sie sicher, dass Ihr Betriebssystem IPv6 unterstützt. Weitere Informationen finden Sie in der entsprechenden Dokumentation zu Ihrem Betriebssystem.

2 Öffnen Sie die Datei **client-config.properties**, die sich im **conf**-Verzeichnis des <**Configuration Manager-Installationsverzeichnis**> befindet. Ändern Sie den Wert des Parameters **bsf.server.url** in die in eckigen Klammern angegebene IPv6-Adresse. Beispiel:

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

2

Configuration Manager-Assistent für die Konfiguration nach der Installation

Dieses Kapitel umfasst die folgenden Themen:

Configuration Manager-Konfiguration nach der Installation – Übersicht

Dieses Kapitel umfasst detaillierte Beschreibungen der Seiten des Configuration Manager-Assistenten für die Konfiguration nach der Installation sowie Beschreibungen der zugehörigen Konfigurationsaufgaben. Dabei handelt es sich um den Inhalt, der angezeigt wird, wenn Sie auf einer beliebigen Seite des Assistenten auf **Hilfe** klicken.

Datenbankverbindungsseite

Dieser Abschnitt umfasst die folgenden Themen:

Allgemeines

Es muss eine Datenbankverbindung eingerichtet sein, die einer Standard-URL-Verbindung zugeordnet ist. Wenn erweiterte Funktionen erforderlich sind, etwa Oracle Real Application Cluster, richten Sie eine Standardverbindung ein und bearbeiten Sie dann die Datei **database.properties** manuell, um die erweiterten Funktionen zu konfigurieren.

Configuration Manager verwendet systemeigene Treiber für Oracle und Microsoft SQL Server. Das bedeutet, dass im Allgemeinen alle Funktionen für systemeigene Treiber unterstützt werden, sofern diese Funktionen über den Datenbank-URL konfiguriert werden können. Der URL befindet sich in der Datei **database.properties**.

Hinweis: Das Konfigurieren der erweiterten Funktionen sollte im Anschluss an den Nachinstallationsprozess erfolgen, wenn eine funktionierende Konfiguration eingerichtet wurde.

Parameter

Definieren Sie zum Einrichten der Datenbankverbindung die folgenden Parameter:

Parameter	Empfohlener Wert	Beschreibung
Vendor	<Benutzerdefiniert>	Datenbankhersteller Mögliche Werte: **Oracle** oder **Microsoft** HP Universal CMDB kann separat oder mithilfe desselben Installationsprogramms installiert werden wie Configuration Manager. Wenn Configuration Manager und UCMDB auf demselben Computer mithilfe desselben Installationsprogramms installiert werden, entspricht der Standardwert für diesen Parameter dem Datenbankhersteller, der bereits mithilfe des UCMDB-Nachinstallationsassistenten ausgewählt wurde. Nur bei einer Installation der beiden Applikationen mithilfe desselben Installationsprogramms werden die Standardwerte festgelegt. Erfolgt die Installation über separate Installationspakete, werden auch dann in diesem Assistenten keine Standardwerte angezeigt, wenn UCMDB auf demselben Computer installiert ist wie Configuration Manager.

Parameter	Empfohlener Wert	Beschreibung
Hostname	<Benutzerdefiniert>	Hostname des Datenbankservers Wenn Configuration Manager und UCMDB auf demselben Computer installiert werden, entspricht der Standardwert für diesen Parameter dem Datenbankserver, der bereits mithilfe des UCMDB-Nachinstallationsassistenten ausgewählt wurde. **Dieser Wert ist obligatorisch.**
Port	<Benutzerdefiniert>	Port des Datenbank-Listeners Wenn Configuration Manager und UCMDB auf demselben Computer installiert werden, entspricht der Standardwert für diesen Parameter dem Datenbankport, der bereits mithilfe des UCMDB-Nachinstallationsassistenten ausgewählt wurde. Für Oracle lautet der Standardwert **1521**. Für Microsoft SQL Server lautet der Standardwert **1433**. **Dieser Wert ist obligatorisch.**
SID/DB	<Benutzerdefiniert>	Name der Oracle SID oder Name der Microsoft SQL Server-Datenbank Wenn Configuration Manager und UCMDB auf demselben Computer installiert werden, entspricht der Standardwert für diesen Parameter der Datenbank-SID/der Datenbank, die bereits mithilfe des UCMDB-Nachinstallationsassistenten ausgewählt wurde. **Dieser Wert ist obligatorisch.**

Parameter	Empfohlener Wert	Beschreibung
Benutzername	<Benutzerdefiniert>	Benutzernamen für die Anmeldung an der Datenbank. **Dieser Wert ist obligatorisch.**
Kennwort	<Benutzerdefiniert>	Kennwort für die Anmeldung an der Datenbank.

Optionen

Des Weiteren stehen die folgenden Optionen zur Verfügung:

Parameter	Empfohlener Wert	Beschreibung
Encrypt password	<Benutzerdefiniert>	Ist diese Option aktiviert, wird das Kennwort in der Datei **database.properties** verschlüsselt. Aus Sicherheitsgründen empfiehlt es sich, die in Textdateien gespeicherten Kennwörter zu verschlüsseln.
Create schema objects	<Benutzerdefiniert>	Ist diese Option ausgewählt, werden die für die für die Ausführung von Configuration Manager erforderlichen Schema-Objekte erstellt. Heben Sie die Auswahl dieser Option nur auf, wenn für die Installation ein vorhandenes Schema verwendet wird, das zuvor erstellt und mit Configuration Manager-Objekten aufgefüllt wurde.

Test

Hinweis: Es wird dringend empfohlen, die Verbindungseigenschaften zu testen, bevor Sie fortfahren.

Klicken Sie zum Test den Verbindungseigenschaften auf die Test-Schaltfläche. Der Assistent versucht dann, auf die Datenbank zuzugreifen und die Verbindung zu verifizieren. Die Testergebnisse werden rechts neben der Test-Schaltfläche angezeigt.

Die Datenbank generiert unterschiedliche Fehlermeldungen. Diese sind selbsterklärend und beziehen sich normalerweise auf die Eingabe ungültiger Benutzernamen oder Kennwörter. Der Fehler muss vor dem Fortsetzen des Prozesses mit positivem Testergebnis behoben werden.

Anwendungsserverseite

Dieser Abschnitt umfasst die folgenden Themen:

➤ "Allgemeines" auf Seite 30

➤ "Parameter" auf Seite 30

Allgemeines

Richten Sie den Configuration Manager-Anwendungsserver mithilfe der unten angezeigten Portnummern ein.

Parameter

Definieren Sie zum Einrichten des Configuration Manager-Anwendungsservers die folgenden Parameter:

Parameter	Empfohlener Wert	Beschreibung
Hostname	<Benutzerdefiniert>	Externer Name des Anwendungsservers Standardmäßig handelt es sich bei diesem Wert um den vollqualifizierten Hostnamen des Computers, auf dem der Assistent ausgeführt wird (ebenso wie Configuration Manager). Im Falle einiger Bereitstellungen sollte dieser Name abweichen, etwa bei der Bereitstellung eines Webservers vor einem Configuration Manager-Anwendungsserver.
Customize ports	<Benutzerdefiniert>	Diese Option ist standardmäßig nicht ausgewählt. Wenn Sie diese Option auswählen, können Sie die Standardportnummern des Anwendungsservers ändern.
HTTP port	<Benutzerdefiniert>	HTTP-Port des Configuration Manager-Anwendungsservers Standardeinstellung: **8080** Standardwert bei einer Installation auf demselben Computer wie HP Universal CMDB: **8180**

Parameter	Empfohlener Wert	Beschreibung
HTTPS port	<Benutzerdefiniert>	HTTPS-Port des Configuration Manager-Anwendungsservers Standardeinstellung: **8443** Standardwert bei einer Installation auf demselben Computer wie UCMDB: **8143**
Tomcat port	<Benutzerdefiniert>	Port für die Verwaltung des Configuration Manager-Anwendungsservers Standardeinstellung: **8005**
AJP port	<Benutzerdefiniert>	AJP-Port (Apache Java Protocol) des Configuration Manager-Anwendungsservers Standardeinstellung: **8009**
JMX HTTP port	<Benutzerdefiniert>	JMX HTTP-Port für den Configuration Manager-Anwendungsserver Standardeinstellung: **39900**
JMX remote port	<Benutzerdefiniert>	JMX-Remote-Port für den Configuration Manager-Anwendungsserver Standardeinstellung: **39600**

Seite für die Windows-Dienstkonfiguration

Wählen Sie aus, ob Sie Configuration Manager als Windows-Dienst installieren möchten. Die Option steht nur zur Verfügung, wenn die Installation auf einem Computer unter Windows erfolgt.

Der Windows-Dienst kann mithilfe des Dienstprogramms **create-windows-service.bat** im Verzeichnis **cnc-home/bin** manuell eingerichtet werden.

Seite für Benutzeranmeldeinformationen

Dieser Abschnitt umfasst die folgenden Themen:

Allgemeines

Richten Sie die folgenden ersten Configuration Manager-Benutzer ein:

Parameter	Empfohlener Wert	Beschreibung
Admin user	<Benutzerdefiniert>	Administrativer Benutzer von Configuration Manager – der "Super User"
Integration user	<Benutzerdefiniert>	Benutzer, der von Configuration Manager in HP Universal CMDB zu Integrationszwecken erstellt wurde

Hinweis: Sie müssen für Administratoren ebenso wie für Integrationsbenutzer Benutzernamen und Kennwörter angeben.

Seite für die HP Universal CMDB-Verbindung

Dieser Abschnitt umfasst die folgenden Themen:

Allgemeines

Das Einrichten der Verbindung zu HP Universal CMDB ist optional.

Wenn Sie Configuration Manager in Form einer kombinierten Installation auf demselben Computer installieren wie UCMDB, müssen Sie auf dieser Seite nichts angeben.

Wenn Sie UCMDB nicht in Form einer kombinierten Installation installieren oder UCMDB auf einem anderen Computer installieren – auch wenn auf dem Localhost eine Verbindung zu UCMDB hergestellt wird – oder wenn Sie UCMDB vor der Installation von Configuration Manager installieren, dann muss UCMDB ausgeführt werden und Sie müssen die entsprechenden Verbindungseigenschaften angeben.

Hinweis: Bei der Installation mithilfe einer Remote-Instanz von UCMDB ist es erforderlich, dass diese Instanz ausgeführt wird. Werden Configuration Manager und UCMDB auf demselben Computer installiert, darf UCMDB während der Ausführung dieses Assistenten nicht ausgeführt werden.

Parameter

Definieren Sie zum Einrichten der UCMDB-Verbindung die folgenden Parameter:

Parameter	Empfohlener Wert	Beschreibung
Use HP UCMDB on a different host	<Benutzerdefiniert>	Wählen Sie diese Option aus, um alle anderen Eigenschaften bei der Installation von Configuration Manager und UCMDB auf unterschiedlichen Computern zu aktivieren.
Hostname	<Benutzerdefiniert>	Name des Hosts, auf dem UCMDB installiert ist
Anschluss	<Benutzerdefiniert>	Port, der von UCMDB abgehört wird

Parameter	Empfohlener Wert	Beschreibung
Protocol	<Benutzerdefiniert>	HTTP oder HTTPS
Customer	<Benutzerdefiniert>	UCMDB-Kunde
Administrative username	<Benutzerdefiniert>	Benutzername des UCMDB-System-administrators
Administrative password	<Benutzerdefiniert>	Kennwort des UCMDB-System-administrators

Test

Hinweis: Es wird dringend empfohlen, die Verbindungseigenschaften zu testen, bevor Sie fortfahren.

Klicken Sie zum Test den Verbindungseigenschaften auf die Test-Schaltfläche. Der Assistent versucht dann, auf UCMDB zuzugreifen und die Verbindung zu verifizieren. Die Testergebnisse werden rechts neben der Test-Schaltfläche angezeigt.

UCMDB generiert unterschiedliche Fehlermeldungen. Diese sind selbsterklärend und beziehen sich normalerweise auf die Eingabe ungültiger Benutzernamen oder Kennwörter. Der Fehler muss vor dem Fortsetzen des Prozesses mit positivem Testergebnis behoben werden.

Übersichtsseite

Es werden alle Optionen angezeigt, die auf den vorherigen Assistentenseiten ausgewählt wurden. Bestätigen Sie, dass die jeweilige Auswahl richtig ist und nehmen Sie ggf. Änderungen vor. Wenn die Auswahl richtig ist, klicken Sie auf **Next** und der Assistent schließt die Konfigurationsaufgabe ab.

Abschlussseite

Dies ist die letzte Seite des Configuration Manager-Assistenten für die **Konfiguration nach der Installation**. Die Aufgaben für die Konfiguration nach der Installation sind abgeschlossen. Klicken Sie auf **Finish**, um den Assistenten zu schließen.

Hinweis: Auch wenn alle Aufgaben erfolgreich abgeschlossen wurden, empfiehlt es sich, die Protokolle unter **cnc-home/tmp/chp/app.log** zu überprüfen.

3

Konfigurieren von LDAP

HP UCMDB Configuration Manager verwendet LDAP für die Verwaltung von Benutzern, Rollen und Berechtigungen. In diesem Kapitel werden die Schritte für das Konfigurieren von und die Fehlerbehebung für LDAP beschrieben.

Dieses Kapitel umfasst die folgenden Themen:

LDAP – Übersicht

Configuration Manager beinhaltet einen internen LDAP-Server (in der Benutzeroberfläche mit der Bezeichnung **Shared** versehen) und kann ebenso eine Verbindung zu einem Organisations-LDAP-Server herstellen. Configuration Manager verwendet diese Server, um nach Benutzern, Gruppen und Rollen zu suchen, um Personalisierungsdaten zu speichern und um Benutzer zu authentifizieren. Sie können festlegen, wofür jeweils der Organisations-LDAP-Server und der interne LDAP-Server verwendet werden.

In einer typischen Bereitstellung wird der interne (Shared) LDAP-Server zum Speichern von Rollen und der externe (Organisations-)LDAP-Server für alle weiteren Zwecke verwendet.

Auswählen von Providern

1. Melden Sie sich bei **Configuration Manager** als Administrator an.
2. Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung - Konfiguration** und wählen Sie **SHARED** oder **EXTERNAL** für jedes der folgenden Attribute entsprechend Ihren bevorzugten Providern aus (**SHARED** ist die Standardauswahl):
   - Authentifizierungsprovider
   - Gruppenprovider
   - Personalisierungsprovider
   - Rollenprovider
   - Provider von Rollenbeziehungen
3. Speichern Sie den Konfigurationssatz.

Herstellen einer Verbindung zum Organisations-LDAP-Server

HP UCMDB Configuration Manager ist anfänglich mit einem internen (Shared) LDAP-Server konfiguriert. In diesem Abschnitt werden die Schritte zum Herstellen einer Verbindung mit Ihrem Organisations-LDAP-Server beschrieben.

Dieser Abschnitt umfasst die folgenden Themen:

Konfigurieren der LDAP-Verbindung

In diesem Abschnitt wird beschrieben, wie eine Verbindung zwischen Configuration Manager und einem externen LDAP-Server hergestellt wird. Bei dem externen LDAP-Server handelt es sich um den Organisations-LDAP-Server, dieser enthält die Organisationsbenutzer.

1. Melden Sie sich bei **Configuration Manager** als Administrator an.
2. Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository** und aktualisieren Sie die folgenden Attribute entsprechend den Eigenschaften Ihres Organisations-LDAP-Servers:

   Allgemeine LDAP-Verbindung

   ldapHost: <LDAP-Hostname>

   ldapPort: <LDAP-Portnummer>

   enableSSL: <True/False – SSL für die Verbindung zu LDAP verwenden>

   useAdministrator: <True/False – Benutzer für die Verbindung zu LDAP verwenden>

   ldapAdministrator: <LDAP-Benutzername (sollte festgelegt sein, wenn **useAdministrator=true)**>

   ldapAdministratorPassword: <LDAP-Benutzerkennwort (sollte festgelegt sein, wenn **useAdministrator=true**)>
3. Speichern Sie den Konfigurationssatz.

Konfigurieren der Gruppen- und Benutzerprovider

Mit diesem Verfahren wird der Organisations-LDAP-Server (externes Repository) als Provider für die Gruppen und Benutzer festgelegt. Der interne LDAP-Server (freigegebenes Repository) wird weiterhin für die Authentifizierung verwendet, aber die Benutzer und Gruppen werden vom externen LDAP-Server abgerufen. Dieser Modus wird zum Testen der Konfiguration des externen LDAP-Servers und zum Zuweisen von Berechtigungen zu den Organisationsbenutzern verwendet.

So legen Sie die Gruppen- und Benutzerprovider fest:

1. Wechseln Sie (wenn nötig) zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository**. Stellen Sie sicher, dass Sie den Konfigurationssatzentwurf verwenden, den Sie im Abschnitt "Konfigurieren der LDAP-Verbindung" auf Seite 39 gespeichert haben.
2. Aktualisieren Sie die folgenden Attribute entsprechend den Eigenschaften Ihres Organisations-LDAP-Servers:
   a. **Benutzersuche**

      usersBase: <Basis-DN für Benutzersuche>

      usersScope: <Bereich für Benutzersuche>

      usersFilter: <Filter für Benutzersuche>

   b. **Benutzerobjektklasse** (vom LDAP-Provider abhängig)

      usersObjectClass: <LDAP-Benutzerobjektklasse>

      usersUniqueIDAttribute: <LDAP-Attribut für die eindeutige ID der Benutzer>

      Die folgenden Attribute sind optional:

      usersDisplayNameAttribute: <LDAP-Attribut für Benutzeranzeigename>

      usersLoginNameAttribute: <LDAP-Attribut für Benutzeranmeldename>

      usersFirstNameAttribute: <LDAP-Attribut für Benutzervorname>

      usersLastNameAttribute: <LDAP-Attribut für Benutzernachname>

      usersEmailAttribute: <LDAP-Attribut für Benutzer-E-Mail-Adresse>

      usersPreferredLanguageAttribute: <LDAP-Attribut für die bevorzugte Sprache der Benutzer>

      usersPreferredLocationAttribute: <LDAP-Attribut für den bevorzugten Standort der Benutzer>

      usersTimeZoneAttribute: <LDAP-Attribut für die Benutzerzeitzone>

usersDateFormatAttribute: <LDAP-Attribut für das Benutzerdatumsformat>

usersNumberFormatAttribute: <LDAP-Attribut für das Benutzerzahlenformat>

usersWorkWeekAttribute: <LDAP-Attribut für die Benutzerarbeitswoche>

usersTenantIDAttribute: <LDAP-Attribut für die Mandanten-ID der Benutzer>

usersPasswordAttribute: <LDAP-Attribut für das Benutzerkennwort>

c **Gruppensuche**

groupsBase: <Basis-DN für Gruppensuche>

groupsScope: <LDAP-Bereich für Gruppensuche>

groupsFilter: <Filter für Gruppensuche>

rootGroupsBase: <Basis-DN für Stammgruppensuche>

rootGroupsScope: <LDAP-Bereich für Stammgruppensuche>

rootGroupsFilter: <Filter für Gruppensuche>

d **Gruppenobjektklasse** (vom LDAP-Provider abhängig)

groupsObjectClass: <LDAP-Gruppenobjektklasse>

groupsMembersAttribute: <LDAP-Attribut für Gruppenmitglieder>

Die folgenden Attribute sind optional:

groupsNameAttribute: <LDAP-Attribut für eindeutigen Gruppennamen>

groupsDisplayNameAttribute: <LDAP-Attribut für Gruppenanzeigename>

groupsDescriptionAttribute: <LDAP-Attribut für Gruppenbeschreibung>

enableDynamicGroups: <Aktivieren dynamischer Gruppen>

dynamicGroupsClass: <LDAP-Objektklasse für dynamische Gruppen>

dynamicGroupsMemberAttribute: <LDAP-Attribut für Mitglieder dynamischer Gruppen>

dynamicGroupsNameAttribute: <LDAP-Attribut für eindeutigen Namen für dynamische Gruppen>

dynamicGroupsDisplayNameAttribute: <LDAP-Attribut für eindeutigen Anzeigenamen für dynamische Gruppen>

dynamicGroupsDescriptionAttribute: <LDAP-Attribut für die Beschreibung dynamischer Gruppen>

e **Gruppenhierarchie** (wenn der Organisations-LDAP-Server Gruppenhierarchie verwendet)

enableNestedGroups: <Unterstützung verschachtelter Gruppen aktivieren>

maximalAllowedGroupsHierarchyDepth: <Maximal zulässige Gruppenhierarchietiefe>

f **Erweiterte Konfiguration**

ldapVersion: <LDAP-Version>

baseDistinguishNameDelimiter: <Begrenzungszeichen für Basis-DN>

scopeDelimiter: <Bereichsbegrenzungszeichen>

attributeValuesDelimiter: <LDAP-Attribut für Wertbegrenzungszeichen>

3 Speichern Sie den Entwurf des Konfigurationssatzes.

Aktivieren des Konfigurationssatzes

1 Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** und aktualisieren Sie Folgendes:

Externe UUM-Quelle: True.

Gruppenprovider: EXTERNAL

Benutzerprovider: EXTERNAL

2 Speichern Sie den Konfigurationssatz und aktivieren Sie ihn anschließend.

3 Melden Sie sich ab und starten Sie den **Configuration Manager**-Server neu.

Zuweisen von Berechtigungen zu Benutzern

Mit diesem Verfahren wird Organisationsbenutzern die Rolle des Systemadministrators zugewiesen. Ein Benutzer mit der Rolle **System Administrator** verfügt über die Berechtigungen, allen anderen Organisationsbenutzern die jeweils relevanten Rollen zuzuweisen.

1 Melden Sie sich bei **Configuration Manager** als Administrator an.

2 Öffnen Sie das Modul **Benutzerverwaltung** (**Verwaltung** > **Benutzerverwaltung**).

3 Bestätigen Sie, dass Ihnen die Gruppen und Benutzer von Ihrem Organisations-LDAP-Server angezeigt werden.

4 Wechseln Sie zu **Benutzerverwaltung** > Ausschnitt **Benutzer suchen** und suchen Sie nach den Benutzern, die als Administrator fungieren. Beispielsweise: Vorname = j*, Nachname = Smith.

5 Fügen Sie den Benutzern die Rolle **System Administrator** zu.

Festlegen des externen LDAP-Servers als Authentifizierungsprovider

Mit diesem Verfahren legen Sie den externen Organisations-LDAP-Server als Authentifizierungsprovider fest, sodass die Organisationsbenutzer für die Authentifizierung verwendet werden.

1 Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** und aktualisieren Sie Folgendes:

Authentifizierungsprovider: EXTERNAL

2 Speichern Sie den Konfigurationssatz und aktivieren Sie ihn anschließend.

3 Melden Sie sich ab und starten Sie den **Configuration Manager**-Server neu.

4 Melden Sie sich als einer der Organisationsbenutzer an, denen die Rolle **System Administrator** zugewiesen wurde.

Importieren des LDAP-Zertifikats

Führen Sie die folgenden Schritte aus, wenn für die Verbindung mit dem Organisations-LDAP-Server ein Zertifikat erforderlich ist:

1. Exportieren Sie das Zertifikat in eine Datei.
2. Beenden Sie den Windows-Dienst für Configuration Manager.
3. Führen Sie folgenden Befehl aus:

   <Configuration Manager-Installation>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <Zertifikatsalias> -keystore <Configuration Manager-Installation>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <Zertifikatsdateipfad>

4. Starten Sie den Windows-Dienst für Configuration Manager.

Konfigurieren des internen (Shared) LDAP-Servers

Ändern des internen (Shared) LDAP-Serverkennworts (optional)

Sie können das Kennwort des internen (Shared) LDAP-Servers aus Sicherheitsgründen ändern.

1. Melden Sie sich bei **HP Universal CMDB Configuration Manager** an.
2. Öffnen Sie eine Befehlszeile und navigieren Sie zum Ordner **<Configuration Manager-Installation>\ldap\serverRoot\bat** .
3. Führen Sie **ldappasswordmodify -h localhost -p <LDAP-Port> -D "cn=Directory Manager" -w <LDAP-Administratorkennwort> -c <LDAP-Administratorkennwort> -n <neues LDAP-Administratorkennwort>** aus.
   a. Das standardmäßige LDAP-Administratorkennwort lautet **ldapadmin**.
   b. Der Standardport ist **2389**.
   c. Bestätigen Sie, dass der Befehl erfolgreich ausgeführt wurde, und fahren Sie nur dann mit den folgenden Schritten fort.

4. Wechseln Sie in **UCMDB Configuration Manager** zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Freigegebenes Benutzerrepository**.
5. Aktualisieren Sie das Kennwort im Attribut **ldapAdministratorPassword**.
6. Speichern Sie den Konfigurationssatz und aktivieren Sie ihn anschließend.
7. Melden Sie sich von **UCMDB Configuration Manager** ab.
8. Starten Sie den **UCMDB Configuration Manager**-Server neu.

Konfigurieren des internen (Shared) LDAP-Ports

Der Standardport **2389** wird bereits von einer anderen Applikation verwendet. Verwenden Sie zum Ändern dieses Standardports das folgende Verfahren.

So konfigurieren Sie den internen LDAP-Port:

1. Öffnen Sie eine Befehlszeile und navigieren Sie zum Ordner **<Configuration Manager-Installation>\ldap\serverRoot\bat**.
2. Führen Sie folgenden Befehl aus:
   dsconfig -h localhost -p 2444 -D "cn=directory manager" -w < LDAP-Administratorkennwort> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<Neuer Port>

   Das standardmäßige LDAP-Administratorkennwort lautet **ldapadmin**.
3. Bestätigen Sie, dass keine Fehlermeldung angezeigt wird, und fahren Sie nur dann mit den folgenden Schritten fort.
4. Melden Sie sich an HP Universal CMDB Configuration Manager an.
5. Wechseln Sie in UCMDB Configuration Manager zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Freigegebenes Benutzerrepository** und aktualisieren Sie die Portnummer im Attribut **ldapPort**.
6. Speichern Sie den Konfigurationssatz und aktivieren Sie ihn anschließend.
7. Melden Sie sich von UCMDB Configuration Manager ab.
8. Starten Sie UCMDB Configuration Manager neu.

LDAP-Fehlerbehebung

Problem: Es ist keine Kommunikation mit dem LDAP-Server möglich. In den Protokollen wird eine Kommunikationsausnahme aufgeführt.

Lösung: Überprüfen Sie die Einstellungen für den LDAP-Host und -Port sowie für SSL:

a Überprüfen Sie, ob LDAP-Host und -Port richtig konfiguriert sind: Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository** und überprüfen Sie die Einstellungen **ldapHost, ldapPort**.

b Überprüfen Sie, ob der SSL-Modus richtig konfiguriert ist. Überprüfen Sie mit dem Organisations-LDAP-Administrator, ob für die LDAP-Verbindung Administratorrechte erforderlich sind. Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository** und überprüfen Sie die Einstellung **enableSSL**.

c Überprüfen Sie, ob das entsprechende Serverzertifikat installiert ist. Führen Sie folgenden Befehl aus:

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

d Überprüfen Sie mit dem Organisations-LDAP-Administrator, ob für die LDAP-Verbindung Administratorrechte erforderlich sind. Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository** und überprüfen Sie die folgenden Einstellungen: **useAdministrator, ldapAdministrator, ldapAdministratorPassword**.

Problem: Es werden keine Gruppen auf dem Bildschirm für Benutzer oder Benutzergruppen angezeigt. In den Protokollen wird keine Ausnahme aufgeführt.

Lösung: Überprüfen Sie Folgendes:

a Überprüfen Sie, ob die die Benutzer- und Gruppensuchfilter richtig konfiguriert sind: Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository** und ändern Sie die folgenden Eigenschaften: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter.**

b Öffnen Sie den LDAP-Clientbrowser und suchen Sie unter den Basis-DNs nach den Benutzern.

Problem: Benutzeroberfläche ist zu langsam.

Lösung: Normalerweise liegt dies daran, dass zu viele Gruppen oder Benutzer in Ihrem LDAP-Server konfiguriert sind. Konfigurieren Sie die Basis-DNs und die Filter, um die Anzahl der Gruppen auf die relevanten Untergruppen wie folgt zu reduzieren:

a Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository**.

b Ändern Sie die folgenden Einstellungen: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**.

Problem: Einige vorhandene Benutzer werden nicht auf dem Bildschirm mit den Gruppen oder der Benutzerverwaltung angezeigt.

Lösung: Auf dem Bildschirm mit den Gruppen oder der Benutzerverwaltung werden nur Benutzer angezeigt, die zu einer Gruppe gehören. Fügen Sie die Benutzer zu den entsprechenden Gruppen in LDAP hinzu, damit sie auf dem Hauptbildschirm angezeigt werden.

Problem: Die Anmeldung dauert sehr lange.

Lösung: Der Benutzer gehört möglicherweise zu vielen Gruppen an. Sie können den Startzeitdauer optimieren, indem Sie wie folgt den Gruppensuchfilter ändern, damit weniger Gruppen zurückgegeben werden:

a Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Benutzerverwaltung** > **Benutzerverwaltung – Konfiguration** > **Externes Benutzerrepository**.

b Ändern Sie die Einstellung **groupsFilter**.

4

Lightweight Single Sign-On-Authentifizierung (LW-SSO) – Allgemeine Referenz

Dieses Kapitel umfasst die folgenden Themen:

LW-SSO-Authentifizierung – Übersicht

LW-SSO ist eine Methode zur Zugriffskontrolle, die es einem Benutzer ermöglicht, sich nur einmal anzumelden und auf die Ressourcen mehrerer Softwaresysteme ohne weitere Anmeldeaufforderungen zuzugreifen. Die Applikationen innerhalb der konfigurierten Gruppe von Softwaresystemen vertrauen der Authentifizierung und bei einem Wechsel zwischen den Applikationen ist keine weitere Authentifizierung erforderlich.

Die Informationen in diesem Abschnitt gelten für LW-SSO, Version 2.2 und 2.3.

Dieser Abschnitt umfasst die folgenden Themen:

➤ "URL-Funktion zum Beziehen von SecurityToken" auf Seite 50

Ablauf des LW-SSO-Tokens

Der Ablaufwert für das LW-SSO-Token bestimmt die Gültigkeit der Applikationssitzung. Daher sollte der Ablaufwert mindestens dem Wert für den Ablauf der Applikationssitzung entsprechen.

Empfohlene Konfiguration für den Ablauf des LW-SSO-Tokens

Für jede Applikation, die LW-SSO verwendet, sollte der Token-Ablauf konfiguriert werden. Der empfohlene Wert ist 60 Minuten. Bei einer Applikation, für die keine hohe Sicherheitsstufe erforderlich ist, kann ein Wert von 300 Minuten konfiguriert werden.

GMT-Zeit

Alle Applikationen, die Teil einer LW-SSO-Integration sind, müssen dieselbe GMT-Zeit mit einer maximalen Abweichung von 15 Minuten aufweisen.

Unterstützung für mehrere Domänen

Für die Funktion für mehrere Domänen müssen für alle Applikationen, die Teil einer LW-SSO-Integration sind, die **trustedHosts**-Einstellungen festgelegt werden (oder die **protectedDomains**-Einstellungen), wenn eine Integration mit Applikationen in anderen DNS-Domänen erforderlich ist. Darüber hinaus muss die richtige Domäne im **lwsso**-Element der Konfiguration hinzugefügt werden.

URL-Funktion zum Beziehen von SecurityToken

Um Informationen zu erhalten, die als SecurityToken für URL von anderen Applikationen gesendet wurde, sollte die Hostapplikation die richtige Domäne im **lwsso**-Element der Konfiguration konfigurieren.

LW-SSO-Sicherheitswarnungen

In diesem Abschnitt werden die für die LW-SSO-Konfiguration relevanten Sicherheitswarnungen beschrieben:

➤ **Vertraulicher InitString-Parameter in LW-SSO:** LW-SSO verwendet für die Überprüfung und Erstellung eines LW-SSO-Tokens symmetrische Verschlüsselung. Der **initString**-Parameter in der Konfiguration wird für die Initialisierung des geheimen Schlüssels verwendet. Eine Applikation erstellt ein Token und jede Applikation, die denselben initString-Parameter verwendet, überprüft das Token.

Achtung:

- ➤ Es ist nicht möglich, LW-SSO zu verwenden, ohne den **initString**-Parameter festzulegen.
- ➤ Bei dem **initString**-Parameter handelt es sich um vertrauliche Informationen. Dies sollte hinsichtlich der Veröffentlichung, des Transports und der Persistenz berücksichtigt werden.
- ➤ Der **initString**-Parameter sollte nur zwischen Applikationen freigegeben werden, die eine gegenseitige Integration mithilfe von LW-SSO aufweisen.
- ➤ Der Parameter sollte mindestens 12 Zeichen umfassen.

➤ **Aktivieren Sie LW-SSO nur, wenn dies erforderlich ist.** LW-SSO sollte deaktiviert werden, sofern es nicht benötigt wird.

➤ **Ebene der Authentifizierungssicherheit.** Die Applikation, die das schwächste Authentifizierungsframework verwendet und ein LW-SSO-Token ausgibt, dem von anderen integrierten Applikationen vertraut wird, bestimmt die Ebene Authentifizierungssicherheit für alle Applikationen.

Nur Applikationen, die starke und sichere Authentifizierungsframeworks verwenden, sollten ein LW-SSO-Token ausgeben.

- **Auswirkungen der symmetrischen Verschlüsselung.** LW-SSO verwendet symmetrische Kryptographie, um LW-SSO-Tokens auszugeben und zu validieren. Aus diesem Grund kann jede Applikation, die LW-SSO verwendet, ein Token ausgeben, dem alle anderen Applikationen vertrauen, die denselben **initString**-Parameter aufweisen. Dieses potenzielle Risiko spielt eine Rolle, wenn sich eine Applikation, die einen gemeinsamen initString-Parameter verwendet, an einem nicht vertrauenswürdigen Speicherort befindet oder von dort darauf zugegriffen werden kann.

- **Benutzerzuordnung (Synchronisation).** Das LW-SSO-Framework stellt nicht sicher, dass die Benutzerzuordnung zwischen den integrierten Applikationen erfolgt. Aus diesem Grund muss die integrierte Applikation die Benutzerzuordnung überwachen. Es empfiehlt sich, für alle integrierten Applikationen denselben Benutzerregistrierungseintrag (wie LDAP/AD) freizugeben.

  Ein Fehler bei der Zuordnung der Benutzer kann zu Sicherheitsverletzung und einem fehlerhaften Applikationsverhalten führen. Beispielsweise kann in den verschiedenen Applikationen ein Benutzername unterschiedlichen physischen Benutzern zugeordnet werden.

  Darüber hinaus kann in Fällen, in denen sich ein Benutzer bei einer Annwendung (AppA) anmeldet und auf eine zweite Applikation (AppB) zugreift, die Benutzercontainer oder Applikationsauthentifizierung verwendet, der Benutzer durch den Fehler bei der Zuordnung gezwungen werden, sich manuell bei AppB anzumelden und einen Benutzernamen einzugeben. Wenn der Benutzer einen anderen Benutzernamen verwendet, als den, mit dem er sich bei AppA angemeldet hat, kann es zu dem folgenden Verhalten kommen: Wenn der Benutzer im Anschluss auf eine dritte Applikation (AppC) von AppA oder AppB zugreift, dann erfolgt der Zugriff unter Verwendung der Benutzernamen die für die Anmeldung bei AppA bzw. AppB verwendet wurden.

- **Identitätsmanager**. Da sie für Authentifizierungszwecke verwendet werden, müssen alle ungeschützten Ressourcen im Identitätsmanager mit der **nonsecureURLs**-Einstellung in der LW-SSO-Konfigurationsdatei konfiguriert werden.

Fehlerbehebung und Einschränkungen

Bekannte Fehler

In diesem Abschnitt werden die bekannten Fehler im Zusammenhang mit LW-SSO-Authentifizierung beschrieben.

- **Sicherheitskontext.** Der LW-SSO-Sicherheitskontext unterstützt nur einen Attributwert pro Attributnamen.

  Aus diesem Grund wird vom LW-SSO-Framework nur ein Wert akzeptiert, wenn das SAML2-Token mehr als einen Wert für denselben Attributnamen sendet.

  Ähnlich wird vom LW-SSO-Framework nur ein Wert akzeptiert, wenn das IdM-Token so konfiguriert ist, dass es mehr als einen Wert für denselben Attributnamen sendet.

- **Abmeldefunktion für mehrere Domänen bei Verwendung von Internet Explorer 7**. Bei der Abmeldefunktion für mehrere Domänen können unter folgenden Umständen Fehler auftreten:

  - Der verwendete Browser ist Internet Explorer 7 und die Applikation ruft mehr als drei aufeinanderfolgende HTTP 302-Umleitungsbefehle beim Abmeldeverfahren auf.

  In diesem Fall verarbeitet Internet Explorer 7 die HTTP 302-Umleitungsantwort möglicherweise nicht ordnungsgemäß und zeigt stattdessen die Fehlerseite **Die Webseite kann nicht angezeigt werden** an.

  Als Problemumgehung empfiehlt es sich, die Anzahl der Applikationsumleitungsbefehle beim Abmeldeverfahren zu verringern, sofern möglich.

Einschränkungen

Beachten Sie bei der Verwendung der LW-SSO-Authentifizierung die folgenden Einschränkungen:

- **Clientzugriff auf die Applikation**.

  Wenn in der LW-SSO-Konfiguration eine Domäne definiert ist:

  - Der Applikationsclient muss auf die Applikation mit dem vollqualifizierten Domänennamen im Anmelde-URL zugreifen. Beispiel: http://myserver.**Unternehmensdomäne**.com/WebApp.
  - LW-SSO bietet keine Unterstützung für URLs mit einer IP-Adresse. Beispiel: http://192.168.12.13/WebApp.
  - LW-SSO bietet keine Unterstützung für URLs ohne eine Domäne. Beispiel: http://myserver/WebApp.

  Wenn in der LW-SSO-Konfiguration keine Domäne definiert ist: Der Client kann auf die Applikation ohne den vollqualifizierten Domänennamen im Anmelde-URL zugreifen. In diesem Fall wird speziell für einen einzelnen Computer ohne Domäneninformationen ein LW-SSO-Sitzungscookie erstellt. Aus diesem Grund wird das Cookie nicht vom Browser an andere delegiert und es wird nicht an andere Computer in derselben DNS-Domäne weitergegeben. Das bedeutet, dass LW-SSO nicht innerhalb derselben Domäne funktioniert.

- **LW-SSO-Framework-Integration.** Applikationen können die LW-SSO-Funktionen nur dann nutzen, wenn sie vorab ins LW-SSO-Framework integriert wurden.

- **Unterstützung für mehrere Domänen**.

  - Die Funktion für mehrere Domänen basiert auf dem HTTP-Referrer. Aus diesem Grund unterstützt LW-SSO Links zwischen Applikationen und bietet keine Unterstützung für die Eingabe eines URLs in ein Browserfenster, sofern sich nicht beide Applikationen in derselben Domäne befinden.
  - Der erste domänenübergreifende Link, der die **HTTP POST**-Methode verwendet, wird nicht unterstützt.

Die Funktion für mehrere Domänen unterstützt die erste **HTTP POST**-Anforderung an eine zweite Applikation nicht (nur die **HTTP GET**-Anforderung wird unterstützt). Wenn Ihre Applikation beispielsweise einen HTTP-Link zu einer zweiten Applikation aufweist, wird eine **HTTP GET**-Anforderung unterstützt, eine **HTTP FORM**-Anforderung wird jedoch nicht unterstützt. Bei allen Anforderungen nach der ersten kann es sich um **HTTP POST**- oder **HTTP GET**-Anforderungen handeln.

- Größe des LW-SSO-Tokens:

  Der Umfang der Informationen, die LW-SSO von einer Applikation in einer Domäne in eine andere Applikation in einer anderen Domäne übertragen kann, ist auf 15 Gruppen/Rollen/Attribute begrenzt (beachten Sie, dass jedes Element durchschnittlich nur 15 Zeichen umfassen darf).

- Links zwischen geschützten (HTTPS) und nicht geschützten Seiten (HTTP) in einem Szenario mit mehreren Domänen:

  Die Funktion für mehrere Domänen kann bei einem Link von einer geschützten (HTTPS) zu einer nicht geschützten Seite (HTTP) nicht ordnungsgemäß ausgeführt werden. Hierbei handelt es sich im eine Browserbeschränkung, aufgrund welcher im Falle einer Verlinkung von einer geschützten zu einer nicht geschützten Ressource die Referrerkopfzeile nicht gesendet wird. Beispiel: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- **SAML2-Token.**

  - Die Abmeldefunktion wird bei Verwendung des SAML2-Tokens nicht unterstützt.

    Aus diesem Grund wird ein Benutzer unter Verwendung des SAML2-Tokens zum Zugriff auf eine zweite Applikation bei der Abmeldung von der ersten Applikation nicht von der zweiten Applikation abgemeldet.

  - Der Ablauf des SAML2-Tokens spiegelt sich nicht in der Sitzungsverwaltung der Applikation wider.

    Entsprechend erfolgt, wenn das SAML2-Token für den Zugriff auf eine zweite Applikation verwendet wird, die Sitzungsverwaltung für jede Applikation separat.

- **JAAS Realm.** JAAS Realm in Tomcat wird nicht unterstützt.
- **Verwenden von Leerzeichen in Tomcat-Verzeichnissen.** Verwenden von Leerzeichen in Tomcat-Verzeichnissen.

  Die Verwendung von LW-SSO ist nicht möglich, wenn ein Tomcat-Installationspfad (Ordner) Leerzeichen enthält (beispielsweise "Program Files") und die LW-SSO-Konfigurationsdatei sich im Tomcat-Ordner **common\classes** befindet.
- **Load Balancer-Konfiguration.** Ein mit LW-SSO bereitgestellter Load Balancer muss für den Einsatz von Sticky Sessions konfiguriert sein.

5

Identitätsmanagerauthentifizierung

Dieses Kapitel umfasst folgende Themen:

Akzeptieren von Identitätsmanagerauthentifizierung

Wenn Sie einen Identitätsmanager verwenden und HP Universal CMDB Configuration Manager hinzufügen möchten, müssen Sie diese Aufgabe durchführen.

Im Rahmen dieser Aufgabe wird beschrieben, wie Sie HP Universal CMDB Configuration Manager so konfigurieren, dass die Identitätsmanager-authentifizierung akzeptiert wird.

Diese Aufgabe umfasst folgende Schritte:

Voraussetzungen

Der Configuration Manager-Tomcat-Server sollte mit Ihrem Webserver (IIS oder Apache) verbunden und durch Ihren Identitätsmanager über einen Tomcat Java-Connector (AJP13) geschützt sein.

Anweisungen zur Verwendung eines Tomcat Java-Connectors (AJP13) finden Sie in der Dokumentation zu Tomcat Java (AJP13).

Konfigurieren von HP Universal CMDB Configuration Manager, sodass Identitätsmanager akzeptiert wird

So konfigurieren Sie Tomcat Java (AJP13) mit IIS6:

1. Konfigurieren Sie den Identitätsmanager zum Senden einer Personalisierungskopfzeile/Rückmeldung, die den Benutzernamen enthält, sowie einer Anforderung des Kopfzeilennamens.
2. Öffnen Sie die Datei <**Configuration Manager-Installationsverzeichnis**>**conf****lwssofmconf.xml** und suchen Sie nach dem Abschnitt, der mit **in-ui-identity-management** beginnt.

   Beispiel:

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

   a Aktivieren Sie die Funktion, indem Sie das Kommentarzeichen entfernen.

   b Ersetzen Sie **enabled**="**false**" durch **enabled**="**true**".

   c Ersetzen Sie **sm-user** durch den Kopfzeilennamen, den Sie in Schritt 1 angefordert haben.

3 Öffnen Sie die Datei <**Configuration Manager-Installationsverzeichnis**>**conf****client-config.properties** und bearbeiten Sie die folgenden Eigenschaften:

   a Ändern Sie **bsf.server.url** in den Identitätsmanager-URL und ändern Sie den Port in den Identitätsmanagerport:

   bsf.server.url=http://<Identitätsmanager-URL>:< Identitätsmanagerport >/bsf

   b Ändern Sie **bsf.server.services.url** in das HTTP-Protokoll und ändern Sie den Port in den ursprünglichen Configuration Manager-Port:

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

Beispiel für die Verwendung eines Java-Connectors für die Konfiguration von Identitätsmanagement für Configuration Manager mit IIS6 auf einem Windows 2003-Betriebssystem

Im Rahmen dieser Beispielaufgabe wird beschreiben, wie Sie den Java-Connector für die Konfiguration von Identitätsmanagement für die Verwendung mit Configuration Manager mit IIS6 unter Windows 2003 verwenden.

So installieren Sie den Java-Connector und konfigurieren ihn für IIS6 auf einem Computer unter Windows 2003:

1 Laden Sie die aktuellste Version des Java-Connectors von der Apache-Website herunter (beispielsweise **djk-1.2.21**).

   a Klicken Sie auf **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.

   b Wählen Sie die aktuellste Version aus.

   c Laden Sie die Datei **isapi_redirect.dll** aus dem Verzeichnis **amd64** herunter.

2 Speichen Sie die Datei unter <**Configuration Manager-Installationsverzeichnis**>**tomcat****bin****win32**.

3 Erstellen Sie eine neue Textdatei mit dem Namen **isapi_redirect.properties** im selben Verzeichnis wie **isapi_redirect.dll**.

Diese Datei umfasst Folgendes:

```
# Configuration file for the Jakarta ISAPI Redirector

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

# This must be in a virtual directory with execute privileges

extension_uri=/jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector

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

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

log_level=info

# Full path to the workers.properties file

worker_file==<Configuration Manager-Installationsverzeichnis>\tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager-Installationsverzeichnis>\tomcat\conf\uriworkermap.properties
```

4 Erstellen Sie eine neue Textdatei mit dem Namen **workers.properties.minimal** unter <**Configuration Manager-Installationsverzeichnis**>**tomcat****conf**.

Diese Datei umfasst Folgendes:

```
# 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 Erstellen Sie eine neue Textdatei mit dem Namen **uriworkermap.properties** unter <**Configuration Manager-Installationsverzeichnis**>**\tomcat\conf**.

Diese Datei umfasst Folgendes:

```
# 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
```

Wichtig: Beachten Sie, dass Configuration Manager zwei Regeln aufweisen muss. Die neue Syntax ermöglicht es, diese in einer Regel zu vereinen, beispielsweise:

/cnc|/*=ajp13w

---

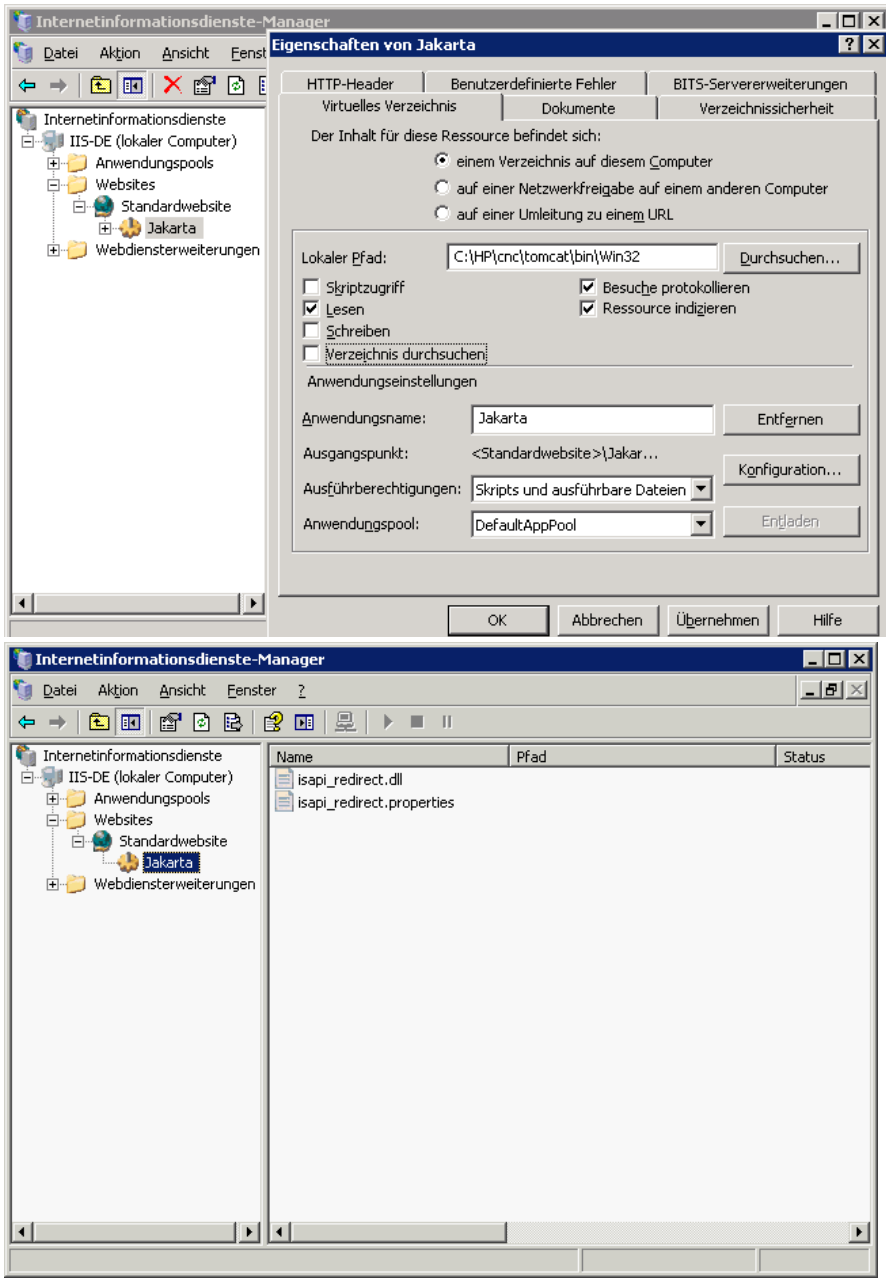
6 Erstellen Sie das virtuelle Verzeichnis im entsprechenden Website-Objekt in der IIS-Konfiguration.

a Öffnen Sie im Windows-Startmenü **Einstellungen\Systemsteuerung\Verwaltung\Internetinformationsdienste-Manager**.

b Klicken Sie im rechten Ausschnitt auf **<Name des lokalen Computers>\Websites\<Name Ihrer Website>** und wählen Sie **Neu\Virtuelles Verzeichnis** aus.

c Versehen Sie das Verzeichnis mit dem Aliasnamen **Jakarta** und legen Sie den lokalen Pfad so fest, dass er auf das Verzeichnis mit **isapi_redirect.dll** verweist.

Im Manager-Fenster wird Folgendes angezeigt:



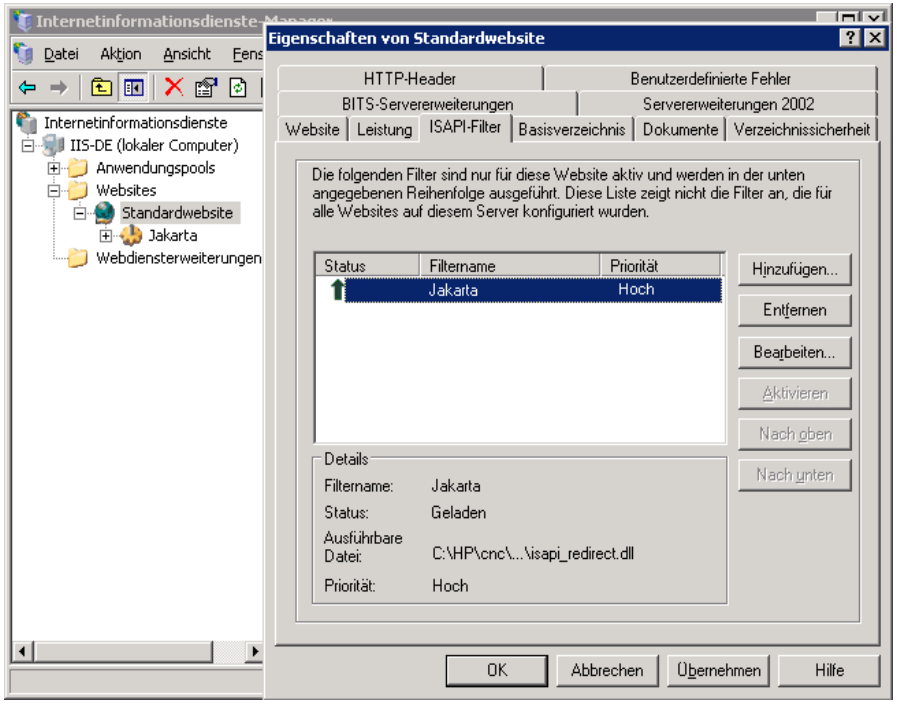
7 Fügen Sie **isapi_redirect.dll** als ISAPI-Filter hinzu.

a Klicken Sie mit der rechten Maustaste auf **<Name Ihrer Website>** und wählen Sie **Eigenschaften** aus.

b Wechseln Sie zur Registerkarte **ISAPI-Filter** und klicken Sie auf die Schaltfläche zum Hinzufügen.

c Wählen Sie den Filternamen **Jakarta** aus und suchen Sie **isapi_redirect.dll**. Der Filter wurde hinzugefügt, aber noch nicht aktiviert.

Im Konfigurationsfenster wird Folgendes angezeigt:



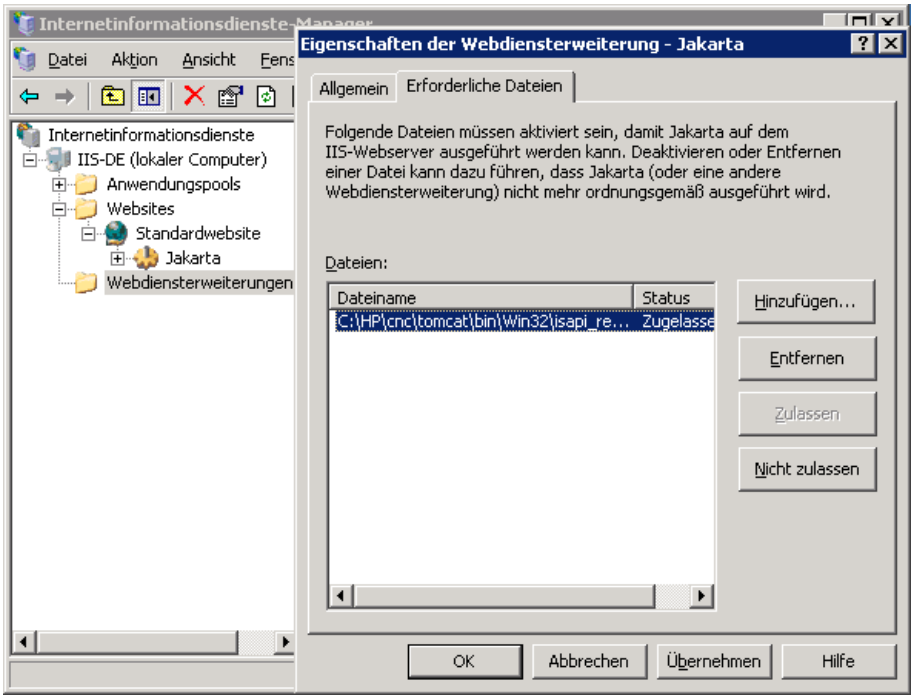
d Klicken Sie auf die Schaltfläche zum Anwenden.

8 Definieren Sie eine neue Webdiensterweiterung und lassen Sie sie zu.

a Klicken Sie mit der rechten Maustaste auf den Eintrag **<Name des lokalen Computers>\Webdiensterweiterungen** und wählen Sie den Menübefehl zum Hinzufügen einer neuen Webdiensterweiterung aus.

b Versehen Sie die neue Webdiensterweiterung mit dem Namen **Jakarta** und suchen Sie die Datei **isapi_redirect.dll**.

Hinweis: Aktivieren Sie vor dem Klicken auf **OK** das Kontrollkästchen **Erweiterungsstatus auf "Zugelassen" setzen**.



9 Starten Sie den IIS-Webserver neu und greifen Sie über den Webdienst auf die Applikation zu.

6

Anmelden bei Configuration Manager

Dieses Kapitel umfasst die folgenden Themen:

Configuration Manager-Zugriff

Sie greifen auf Configuration Manager mithilfe eines unterstützten Webbrowsers von einem beliebigen Computer mit einer Netzwerkverbindung (Intranet oder Internet) mit dem Configuration Manager-Server zu. Die jeweilige Zugriffsebene für einen Benutzer hängt von seinen Berechtigungen ab. Weitere Informationen zum Erteilen von Benutzerberechtigungen finden Sie unter "Benutzerverwaltung" im *Configuration Manager-Benutzerhandbuch* zu *HP Universal CMDB*.

Weitere Informationen zu den Webbrowseranforderungen sowie den Mindestanforderungen zum Anzeigen von Configuration Manager finden Sie unter "Configuration Manager – Systemanforderungen" auf Seite 8.

Weitere Informationen zum sicheren Zugriff auf Configuration Manager finden Sie unter "Härten" auf Seite 77.

Zugreifen auf Configuration Manager

Geben Sie im Webbrowser den URL des Configuration Manager-Servers ein, beispielsweise **http://<Servername oder IP-Adresse>.<Domänenname>:<Port>**, wobei **<Servername oder IP-Adresse>.<Domänenname>** für den vollqualifizierten Domänennamen (FQDN) des Configuration Manager-Servers steht und **<Port>** für den während der Installation ausgewählten Port.

Anmelden bei Configuration Manager

1. Geben Sie den Benutzernamen und das Kennwort an, die Sie im Configuration Manager-Nachinstallationsassistenten festgelegt haben.
2. Klicken Sie auf **Anmelden**. Nach der Anmeldung wird der Benutzername oben rechts auf dem Bildschirm angezeigt.
3. (Empfohlen) Stellen Sie eine Verbindung zum Organisations-LDAP-Server her und weisen Sie den LDAP-Benutzern Administratorrollen zu, um den Configuration Manager-Administratoren den Zugriff auf das System zu ermöglichen. Weitere Informationen zum Zuweisen von Rollen zu Benutzern im Configuration Manager-System finden Sie unter "Benutzerverwaltung" im *HP Universal CMDB Configuration Manager-Benutzerhandbuch*.

Abmelden

Wenn Sie Ihre Sitzung beendet haben, sollten Sie sich von der Website abmelden, um nicht autorisierte Zugriffe zu verhindern.

So melden Sie sich ab:

Klicken Sie oben auf der Seite auf **Abmelden**.

Hinweis: Standardmäßig läuft eine Sitzung nach 30 Minuten ab.

Zugreifen auf die JMX Console für Configuration Manager

Möglicherweise müssen Sie zur Fehlerbehebung oder zum Ändern bestimmter Konfigurationen auf die JMX Console zugreifen.

So greifen Sie auf die JMX Console zu:

1. Öffnen Sie die JMX Console unter http://<Servername oder IP-Adresse>:<Port>/cnc/jmx-console. Bei dem Port handelt es sich um den während der Installation von Configuration Manager konfigurierten Port.
2. Geben Sie die standardmäßigen Benutzeranmeldeinformationen ein. Dabei handelt es sich um dieselben Daten, die auch für die Anmeldung bei Configuration Manager erforderlich sind.

Fehlerbehebung und Einschränkungen

Problem. Nach dem Ändern des Konfigurationssatzes in der Serververwaltung kann der Server nicht mehr gestartet werden.

Lösung. Stellen Sie den vorherigen Konfigurationssatz wieder her. Gehen Sie dabei folgendermaßen vor:

1. Führen Sie den folgenden Befehl aus, um die ID des zuletzt aktivierten Konfigurationssatzes zu finden:

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

   wobei <**Datenbankeigenschaften**> durch einen Verweis auf den Speicherort der Datei <**Configuration Manager-Installationsverzeichnis**>**conf\database.properties** oder durch Angabe aller Datenbankeigenschaften angegeben werden kann. Beispiel:

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

2. Führen Sie den folgenden Befehls aus, um den letzten Konfigurationssatz zu exportieren:

   ```
   < HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <Datenbankeigenschaften> <Konfigurationssatz-ID> <Name der
   Sicherungsdatei>
   ```

wobei <**Konfigurationssatz-ID**> die Konfigurationssatz-ID aus dem vorherigen Schritt und <**Sicherungsdatei**> der Name der temporären Datei ist, die zum Speichern des Konfigurationssatzes verwendet wird. Geben Sie beispielsweise zum Exportieren eines Konfigurationssatzes mit der ID **491520** in die Datei **mydump.zip** Folgendes ein:

```
cd <HP Universal CMDB Configuration-Stammverzeichnis>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
```

3. Halten Sie den HP Universal CMDB Configuration Manager-Dienst an.
4. Führen Sie den folgenden Befehl aus, um den vorherigen Konfigurationssatz zu importieren und aktivieren:

```
< HP Universal CMDB Configuration Manager>\bin\import-cs.bat <Datenbankeigenschaften> <Name der Sicherungsdatei> --activate
```

Problem. Es tritt ein Fehler bei der UCMDB-Verbindung auf.

Lösung. Dies kann eine der folgenden Ursachen haben:

- Der UCMDB-Server steht nicht zur Verfügung. Starten Sie Configuration Manager neu, nachdem UCMDB wieder vollständig verfügbar ist (stellen Sie sicher, dass der Status des UCMDB-Servers die Verfügbarkeit angibt).
- Der UCMDB-Server ist verfügbar, aber die Anmeldeinformationen für die Configuration Manager-Verbindung sind nicht korrekt oder der URL stimmt nicht. Starten Sie Configuration Manager. Wechseln Sie zu **Serververwaltung**, ändern Sie die Verbindungseinstellungen für UCMDB und speichern Sie den neuen Konfigurationssatz. Aktivieren Sie den Konfigurationssatz und starten Sie den Server neu.

Problem. Die LDAP-Verbindungseinstellungen sind falsch.

Lösung. Stellen Sie den vorherigen Konfigurationssatz wieder her. Legen Sie die richtigen LDAP-Verbindungseinstellungen fest und aktivieren Sie den neune Konfigurationssatz.

Problem. Änderungen am UCMDB-Klassenmodell werden in Configuration Manager nicht erkannt.

Lösung. Starten Sie den Configuration Manager-Server neu.

Problem. Das Configuration Manager-Protokoll weist eine Fehlermeldung zu einer Überschreitung des Zeitlimits bei der Ausführung von UCMDB auf.

Lösung. Dieser Fehler tritt auf, wenn die UCMDB-Datenbank überlastest ist. Verlängern Sie die Zeit für den Verbindungstimeout, um diesen Fehler zu beheben:

1 Erstellen Sie eine Datei **jdbc.properties** im Ordner **UCMDBServer\conf**.

2 Geben Sie Folgendes ein: QueryTimeout=<Anzahl in Sekunden>.

3 Starten Sie den UCMDB-Server neu.

Problem. Sie können in Configuration Manager keine zu verwaltende Ansicht hinzufügen.

Lösung. Wenn Sie eine zu verwaltende Ansicht hinzufügen, wird eine neue TQL in UCMDB erstellt. Wenn die maximale Anzahl an aktiven TQLs erreicht wurde, kann keine Ansicht hinzugefügt werden. Erhöhen Sie die zulässige Anzahl an aktiven TQLs in UCMDB, indem Sie die folgenden Einstellungen im Infrastructure Settings Manager ändern:

- Maximale Anzahl an TQLs auf dem Server
- Maximale Anzahl an aktiven benutzerdefinierten TQLs

Problem. Das HTTPS-Serverzertifikat ist ungültig.

Lösung. Dies kann eine der folgenden Ursachen haben:

- Das Datum für die Zertifikatverifizierung wurde überschritten. Sie benötigen ein neues Zertifikat.
- Bei der Zertifizierungsstelle des Zertifikats handelt es sich nicht um eine vertrauenswürdige Stelle. Fügen Sie die Zertifizierungsstelle zu Ihrer Liste mit vertrauenswürdigen Stammzertifizierungsstellen hinzu.

Problem. Beim Anmelden über die Configuration Manager-Anmeldeseite wird Ihnen eine Fehlermeldung oder eine Seite mit dem Hinweis angezeigt, dass der Zugriff verweigert wurde.

Lösung. Dies kann eine der folgenden Ursachen haben:

- Der Benutzername wurde möglicherweise nicht im Authentifizierungsprovider definiert (externer/freigegebener LDAP-Server). Fügen Sie den Benutzer im Authentifizierungsprovidersystem hinzu.
- Der Benutzer wurde definiert, verfügt aber nicht über die Anmeldeberechtigung für Configuration Manager. Erteilen Sie ihm die Anmeldeberechtigung. Als Best Practice wird empfohlen, der Stammgruppe aller Configuration Manager-Benutzer die Anmeldeberechtigung zu erteilen.
- Diese Lösungen greifen auch, wenn die Anmeldung fehlschlägt, nachdem eine IDM-Systemanmeldung erfolgt ist.

Problem. Der Configuration Manager-Server wird nicht gestartet, weil falsche Datenbank-Anmeldeinformationen eingegeben wurden.

Lösung. Wenn Sie die Datenbank-Anmeldeinformationen geändert haben und der Server nicht gestartet wird, sind die Anmeldeinformationen möglicherweise falsch. (**Hinweis**: Der Nachinstallationsassistent testet die eingegebenen Anmeldeinformationen nicht automatisch. Sie müssen im Assistenten auf die Test-Schaltfläche klicken.) Das Datenbankkennwort muss erneut verschlüsselt werden und die neuen Anmeldeinformationen müssen in der Konfigurationsdatei eingegeben werden. Gehen Sie dabei folgendermaßen vor:

1. Geben Sie an einer Befehlszeile den folgenden Befehl ein, um das aktualisierte Datenbankkennwort zu verschlüsseln:

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

   Hierdurch wird ein verschlüsseltes Kennwort zurückgegeben.

2. Kopieren Sie das verschlüsselte Kennwort (einschließlich des verschlüsselten Präfixes) in den Parameter **db.password** im **<CnC-Installationsordner>\conf\database.properties**.

Problem. Wenn der DNS-Server nicht richtig konfiguriert ist, müssen Sie sich möglicherweise mithilfe der Server-IP-Adresse anmelden. Beim Eingeben der IP-Adresse tritt ein zweiter DNS-Fehler auf.

Lösung. Ersetzten Sie den Namen des Computers erneut durch die IP-Adresse. Beispiel:

Wenn Sie sich unter Verwendung der folgenden IP-Adresse anmelden:
http://16.55.245.240:8180/cnc/

und Ihnen eine Adresse mit dem Namen des Computers mit einem DNS-Fehler angezeigt wird, beispielsweise:
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

ersetzen Sie die Angabe durch:
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

und starten Sie die Applikation erneut im Browser.

Problem. Der Configuration Manager-Tomcat-Server startet nicht.

Lösung. Führen Sie eine der folgenden Aktionen aus:

- Führen Sie den Nachinstallationsassistenten aus und ersetzen Sie die Configuration Manager-Serverports.
- Beenden Sie den anderen Prozess, der die Configuration Manager-Ports belegt.
- Ändern Sie die Ports in den Configuration Manager-Konfigurationsdateien manuell, indem Sie die folgende Datei bearbeiten: **<CnC-Installationsordner>\servers\server-0\conf\server.xml**. Aktualisieren Sie außerdem die relevanten Ports:
  - HTTP (8080): Zeile 69
  - HTTPS (8443): Zeilen 71, 90

Problem. Im Configuration Manager-Protokoll ist eine Fehlermeldung aufgeführt, die besagt, dass nicht genügend Speicher verfügbar ist.

Lösung. Erhöhen Sie die maximale Java-Arbeitsspeichergröße wie erforderlich.

So ändern Sie die Speichergröße im Configuration Manager-Dienst:

1. Wechseln Sie zum Verzeichnis **<CnC-Installationsordner>\cnc\bin** und führen Sie den folgenden Befehl aus: edit-server-0.bat.

2. Wechseln Sie zur Registerkarte **Java**.
3. Aktualisieren Sie die Parameter **Initial memory pool** und **Maximum memory pool**.

So ändern Sie die Speichergröße in der Batchdatei:

1. Wechseln Sie zum Verzeichnis <**CnC-Installationsordner**>**cnc** und öffnen Sie die Datei **start-server-0.bat**, um sie zu bearbeiten.
2. Suchen Sie nach der Zeile, die mit **SET JAVA_OPTS=-Dcnc.home** beginnt.
3. Suchen Sie nach den Befehlen **-Xms** und **-Xmx** und ändern Sie sie entsprechend Ihren Anforderungen:

   -Xms<anfängliche Speicherpoolgröße> -Xmx<maximale Speicherpoolgröße>

   Beispiel: Geben Sie zum Festlegen der anfänglichen Größe des Speicherpools auf 100 MB und der maximalen Größe des Speicherpools auf 800 MB Folgendes ein:

   -Xms100m -Xmx800m

Problem. Der Nachinstallationsassistent benötigt für den Abschluss nach Klicken auf **Finish** sehr viel Zeit.

Lösung. Für ein UCMDB-System, dass nicht für den konsolidierten Modus vorkonfiguriert war, kann der Vorgang der Schemakonsolidierung viel Zeit in Anspruch nehmen (abhängig von der Datenmenge). Warten Sie 15 Minuten. Wenn kein Fortschritt erkennbar ist, beenden Sie den Assistenten und starten Sie den Prozess neu.

Problem. Änderungen an CIs in UCMDB werden in Configuration Manager nicht angezeigt.

Lösung. Configuration Manager führt einen asynchronen Offline-Analyseprozess aus. Der Prozess hat die letzten Änderungen in UCMDB möglicherweise noch nicht verarbeitet. Versuchen Sie eine der folgenden Aktionen, um das Problem zu beheben:

- Warten Sie ein paar Minuten. Das Standardintervall zwischen den Ausführungen des Analyseprozesses beträgt zehn Minuten. Es kann im Serververwaltungsmodul konfiguriert werden.
- Führen Sie einen JMX-Aufruf aus, um die Offline-Analyseberechnung in der relevanten Ansicht auszuführen.
- Wechseln Sie zur Richtlinienverwaltung. Klicken Sie auf die Schaltfläche **Richtlinienanalyse neu berechnen**. Dadurch wird der Offline-Analyseprozess für alle Ansichten aufgerufen (was einige Zeit in Anspruch nehmen kann). Außerdem müssen Sie möglicherweise eine künstliche Änderung an einer Richtlinie vornehmen und diese speichern.

Problem. Wenn Sie auf **Verwaltung** > **UCMDB öffnen** klicken, wird die UCMDB-Anmeldeseite angezeigt.

Lösung. Sie müssen Single Sign-on aktivieren, um ohne erneute Anmeldung auf UCMDB zugreifen zu können. Weitere Informationen finden Sie unter "Aktivieren von Lightweight Single Sign-On" auf Seite 20. Stellen Sie außerdem sicher, dass der angemeldete Configuration Manager-Benutzer im UCMDB-Benutzerverwaltungssystem festgelegt ist.

Problem. Wenn eines der folgenden Verhalten auftritt:

- Nach dem Löschen eines CIs aus dem Status "Tatsächlich" in UCMDB ist die Bezeichnung (der Name) des CI in Configuration Manager nicht verfügbar.
- Nach der Autorisierung ist ein CI als geändert gekennzeichnet.
- Daten zu zusammengesetzten CIs entsprechen den vorherigen Daten, obwohl auf den Registerkarten mit den CI-Details und den geänderten Attributen die aktualisierten Daten angezeigt werden.
- Beim Ausführen von UCMDB, aktualisiert auf Version 9.02:

- Änderungen werden in den tatsächlichen und den autorisierten Status nicht erkannt.
- In der Statusverwaltung werden keine CI-Details angezeigt.

Lösung. Stellen Sie sicher, dass die UCMDB-Patches installiert wurden. Führen Sie zum Installieren der Patches die Schritte der Installationsaufgabe durch, beginnend mit Schritt 15 auf Seite 14.

Problem. Im Nachinstallationsassistenten funktioniert beim Konfigurieren einer UCMDB-Verbindung zu einer IPv6-Adresse das Menüelement **Verwaltung** > **UCMDB öffnen** nicht.

Lösung. Gehen Sie in diesem Fall folgendermaßen vor:

1. Wechseln Sie zu **Verwaltung** > **Serververwaltung** > **Configuration Manager** > **UCMDB-Verbindung**.
2. Fügen Sie um die IP-Adresse um den URL für den UCMDB-Zugriff eckige Klammern ein. Der URL sollte folgendermaßen aussehen: http://[x:x:x:x:x:x:x:x]:8080/.
3. Speichern Sie den Konfigurationssatz und aktivieren Sie ihn.
4. Starten Sie Configuration Manager neu.

Für die Verwendung von Configuration Manager gelten folgende Einschränkungen:

- Jedes Mal, wenn auf dem Configuration Manager-Tomcat-Server die Zeit geändert wird, muss der Server neu gestartet werden, um die Zeit auf dem Server zu aktualisieren.

7

Härten

Dieses Kapitel umfasst die folgenden Themen:

Härten von Configuration Manager

In diesem Abschnitt wird das Konzept sicherer Configuration Manager-Applikationen vorgestellt. Darüber hinaus werden die für die Implementierung der Sicherheit erforderliche Planung und Architektur erörtert. Es wird dringend empfohlen, diesen Abschnitt zu lesen, bevor Sie sich dem Thema in den folgenden Abschnitten zuwenden.

Configuration Manager ist als Teil einer sicheren Architektur konzipiert und daher für die Herausforderung gerüstet, die die Sicherheitsbedrohungen darstellen, denen das Programm ausgesetzt ist.

Mit den Richtlinien zum Härten wird auf die Konfiguration eingegangen, die für eine sicherere (gehärtete) Configuration Manager-Implementierung erforderlich sind.

Die Informationen zum Härten sind vorrangig für Configuration Manager-Administratoren vorgesehen, die sich vor Beginn der Prozeduren mit den entsprechenden Einstellungen und Empfehlungen vertraut machen sollten.

Im Folgenden sind die empfohlenen Vorbereitung zum Härten Ihres Systems aufgeführt:

- Evaluieren Sie die Sicherheitsrisiken/den Sicherstatus Ihres allgemeinen Netzwerks und nutzen Sie diese Kenntnisse, wenn Sie entscheiden, wie Configuration Manager optimal in Ihr Netzwerk integriert werden kann.
- Eignen Sie sich umfassende Kenntnisse des technischen Configuration Manager-Frameworks sowie der Configuration Manager-Sicherheitsfunktionen an.
- Lesen Sie sämtliche Richtlinien für das Härten.
- Stellen Sie sicher, dass Configuration Manager uneingeschränkt funktionsfähig ist, bevor Sie mit den Prozeduren beginnen.
- Befolgen Sie die Schritte der Prozeduren in jedem Abschnitt in chronologischer Reihenfolge.

Wichtig:

- Für die Prozeduren ist Voraussetzung, dass Sie nur die jeweils in den Abschnitten vorgegebenen Anweisungen umsetzen und keine sonstigen, anderweitig dokumentierten Schritte durchführen.
- Sind die Prozeduren auf eine bestimmte verteilte Architektur ausgerichtet, bedeutet dies nicht, dass es sich dabei um die am besten für Ihr Unternehmen geeignete Architektur handelt.
- Für die Prozeduren in den folgenden Abschnitten wird vorausgesetzt, dass die Durchführung auf dedizierten Computern für Configuration Manager erfolgt. Bei paralleler Verwendung der Computer für andere Zwecke können Probleme auftreten.
- Die in diesem Abschnitt bereitgestellten Informationen zum Härten stellen keine Anleitung für eine Risikobewertung Ihrer Computersysteme dar.

Verschlüsseln des Datenbankkennworts

Das Datenbankkennwort ist in der Datei **<Configuration Manager-Installationsverzeichnis>\conf\database.properties** gespeichert. Unser Verschlüsselungsalgorithmus entspricht den FIPS 140-2-Standards, wenn Sie das Kennwort verschlüsseln möchten. Aktivieren Sie zum Verschlüsseln des Datenbankkennworts das Kontrollkästchen für die Kennwortverschlüsselung auf der Datenbankkonfigurationsseite des Configuration Manager-Nachinstallationsassistenten.

Die Verschlüsselung erfolgt anhand eines Schlüssels, durch den das Kennwort verschlüsselt wird. Der Schlüssel selbst wird dann anhand eines weiteren Schlüssels verschlüsselt, auch als Hauptschlüssel bezeichnet. Beide Schlüssel werden mithilfe desselben Algorithmus verschlüsselt. Weitere Informationen zu den im Verschlüsselungsprozess verwendeten Parametern finden Sie unter "Kennwortverschlüsselung" auf Seite 88.

Achtung: Wenn Sie den Verschlüsselungsalgorithmus ändern, werden die zuvor verschlüsselten Kennwörter unbrauchbar.

So ändern Sie die Verschlüsselung Ihres Datenbankkennworts:

1. Öffnen Sie die Datei **<Configuration Manager-Installationsverzeichnis>\conf\encryption.properties** und bearbeiten Se die folgenden Felder:
   - **engineName.** Geben Sie den Namen des Verschlüsselungsalgorithmus ein.
   - **keySize.** Geben Sie die Größe des Hauptschlüssels für den ausgewählten Algorithmus ein.
2. Führen Sie das Skript **generate-keys.bat** aus, um das Verzeichnis **cnc\security\encrypt_repository** und den Verschlüsselungsschlüssel zu erstellen.
3. Führen Sie den Nachinstallationsassistenten erneut aus.

Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat

In diesem Abschnitt wird erläutert, wie Sie Configuration Manager für die Unterstützung von Authentifizierung und Verschlüsselung mithilfe des Secure Sockets Layer-Kanals (SSL) konfigurieren.

Configuration Manager verwendet Tomcat 6.0 als Anwendungsserver.

Hinweis: Die Verzeichnis- und Dateispeicherorte sind von Ihren spezifischen Plattform-, Betriebssystem- und Installationseinstellungen abhängig.

---

1 Voraussetzungen

Bevor Sie mit der folgenden Prozedur beginnen, entfernen Sie die alte Datei **tomcat.keystore** unter **<Configuration Manager-Installationsverzeichnis>\java\lib\security\tomcat.keystore**.

2 Erstellen eines Serverschlüsselspeichers

Erstellen Sie einen Schlüsselspeicher (JKS-Typ) mit einem selbstsignierten Zertifikat und einem übereinstimmenden privaten Schlüssel:

➤ Führen Sie im bin-Verzeichnis der Java-Installation im **<Configuration Manager-Installationsverzeichnis>** den folgenden Befehl aus:

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

Das Konsolendialogfeld wird geöffnet.

➤ Geben Sie das Schlüsselspeicherkennwort ein. Wenn das Kennwort geändert wurde, ändern Sie es manuell in der Datei.

➤ Beantworten Sie die Frage nach Ihrem Vor- und Nachnamen. Geben Sie den Configuration Manager-Webservernamen ein. Geben Sie alle weiteren unternehmensspezifischen Informationen wie gefordert an.

➤ Geben Sie ein Schlüsselkennwort ein. Das Schlüsselkennwort MUSS mit dem Schlüsselspeicherkennwort übereinstimmen.

Es wird ein JKS-Schlüsselspeicher namens **tomcat.keystore** mit einem Serverzertifikat mit der Bezeichnung **hpcert** erstellt.

3 Platzieren des Zertifikats im vertrauenswürdigen Speicher des Clients

Nach dem Erstellen von **tomcat.keystore** und Exportieren des Serverzertifikats platzieren Sie dieses Zertifikat für jeden Client, der mit Configuration Manager über SSL mithilfe dieses selbstsignierten Zertifikats kommunizieren muss, in die vertrauenswürdigen Speicher des Clients.

Einschränkung: In **tomcat.keystore** kann nur ein Serverzertifikat vorhanden sein.

---

4 Verifizieren der Clientkonfigurationseinstellungen

Öffnen Sie die Datei **client-config.properties**, die sich im **conf**-Verzeichnis des <**Configuration Manager-Installationsverzeichnis**> befindet. Legen Sie die Einstellung des Protokolls auf **https** und den Port auf **8443** fest.

5 Ändern der Datei "server.xml"

Öffnen Sie die Datei **server.xml**, die sich im **conf**-Verzeichnis des <**Configuration Manager-Installationsverzeichnis**> befindet. Suchen Sie nach der Einstellung, die mit

Connector port="8443"

beginnt (in den Kommentaren). Aktivieren Sie das Skript, indem Sie das Kommentarzeichen entfernen und die folgenden beiden Zeilen hinzufügen:

keystoreFile="<tomcat.keystore-Dateispeicherort>" (siehe Schritt 2 auf Seite 81)

keystorePass="<Kennwort>"

6 Neustarten des Servers

7 Verifizieren der Serversicherheit

Um zu verifizieren, dass der Configuration Manager-Server sicher ist, geben Sie den folgenden URL in den Webbrowser ein: **https://<Configuration Manager-Servername oder IP-Adresse>:8443/cnc**.

Tipp: Wenn Sie keine Verbindung herstellen können, verwenden Sie einen anderen Browser oder eine neuere Version des Browsers.

Aktivieren von SSL auf dem Servercomputer mit einem Zertifikat von einer Zertifizierungsstelle

Um ein von einer Zertifizierungsstelle ausgegebenes Zertifikat zu verwenden, muss der Schlüsselspeicher das Java-Format aufweisen. Das folgende Beispiel veranschaulicht, wie der Schlüsselspeicher für einen Windows-Computer formatiert wird.

1 Voraussetzungen

Bevor Sie mit der folgenden Prozedur beginnen, entfernen Sie die alte Datei **tomcat.keystore** unter **<Configuration Manager-Installationsverzeichnis>\java\lib\security\tomcat.keystore**.

2 Erstellen eines Serverschlüsselspeichers

a Erstellen sie ein von einer Zertifizierungsstelle signiertes Zertifikat und installieren Sie es unter Windows.

b Exportieren Sie mithilfe von Microsoft Management Console (**mmc.exe**) das Zertifikat in eine PFX-Datei (einschließlich privater Schlüssel).

➤ Geben Sie eine Zeichenfolge als Kennwort für die PFX-Datei ein. (Sie werden aufgefordert, dieses Kennwort anzugeben, wenn Sie den Schlüsselspeichertyp in einen JAVA-Schlüsselspeicher konvertieren.) Die PFX-Datei enthält nun ein öffentliches Zertifikat und einen privaten Schlüssel und ist kennwortgeschützt.

c Kopieren Sie die von Ihnen erstellte PFX-Datei in den folgenden Ordner: <**Configuration Manager-Installationsverzeichnis**>**\java\lib\security**.

d Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis in <**Configuration Manager-Installationsverzeichnis**>**\bin\jre\bin**.

➤ Ändern Sie den Schlüsselspeichertyp von **PKCS12** in einen **JAVA**-Schlüsselspeicher, indem Sie den folgenden Befehl ausführen:

```
keytool -importkeystore -srckeystore <Configuration Manager-
Installationsverzeichnis>\conf\security\<Name der PFX-Datei> -srcstoretype
PKCS12 -destkeystore tomcat.keystore
```

Sie werden aufgefordert, das Kennwort für den Quellschlüsselspeicher (**.pfx**) einzugeben. Es handelt sich um das Kennwort, dass Sie beim Erstellen der PFX-Datei in Schritt b angegeben haben.

3 Verifizieren der Clientkonfigurationseinstellungen

Öffnen Sie folgende Datei: <**Configuration Manager-Installationsverzeichnis**>**\cnc\conf\client-config.properties** und verifizieren Sie, dass die Eigenschaft **bsf.server.url** auf **https** und der Port auf **8443** festgelegt ist.

4 Ändern der Datei "server.xml"

Öffnen Sie folgende Datei: <**Configuration Manager-Installationsverzeichnis**>**\conf\server.xml**. Suchen Sie nach der Einstellung, die mit

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

beginnt (in den Kommentaren). Aktivieren Sie das Skript, indem Sie das Kommentarzeichen entfernen und die folgenden beiden Zeilen hinzufügen:

```
keystoreFile="../../java/lib/security/tomcat.keystore"

keystorePass="password" />
```

5 Neustarten des Servers

6 Verifizieren der Serversicherheit

Um zu verifizieren, dass der Configuration Manager-Server sicher ist, geben Sie den folgenden URL in den Webbrowser ein: **https://<Configuration Manager-Servername oder IP-Adresse>:8443/cnc**.

Einschränkung: In **tomcat.keystore** kann nur ein Serverzertifikat vorhanden sein.

Aktivieren von SSL mit einem Clientzertifikat

Wenn das vom Configuration Manager-Webserver verwendete Zertifikat von einer bekannten Zertifizierungsstelle ausgegeben wird, kann Ihr Webbrowser das Zertifikat höchstwahrscheinlich validieren, ohne das weitere Aktionen erforderlich sind.

Wenn der Serververtrauensspeicher der Zertifizierungsstelle nicht vertraut, importieren Sie das Zertifikat in den Serververtrauensspeicher.

Mit dem folgenden Beispiel wird veranschaulicht, wie das selbstsignierte **hpcert**-Zertifikat in den Serververtrauensspeicher (cacerts) importiert wird.

So importieren Sie ein Zertifikat in den Serververtrauensspeicher:

1. Suchen Sie auf dem Clientcomputer nach dem Zertifikat **hpcert** und benennen Sie es in **hpcert.cer** um.

   Im Windows-Explorer wird anhand des Symbols angezeigt, dass es sich um ein Sicherheitszertifikat handelt.

2. Doppelklicken Sie auf **hpcert.cer**, um das Zertifikatsdialogfeld von Internet Explorer zu öffnen und die Datei zu importieren.

3. Importieren Sie auf dem Servercomputer das Zertifikat in den Vertrauensspeicher (cacerts). Verwenden Sie hierzu das keytool-Dienstprogramm mithilfe des folgenden Befehls:

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

4. Ändern Sie die Datei "server.xml" wie folgt:

   a. Nehmen Sie die in Schritt 5 auf Seite 82 beschriebenen Änderungen vor.

   b. Fügen Sie direkt im Anschluss die folgenden Zeilen hinzu:

   ```
   truststoreFile="../../java/lib/security/cacerts"

   truststorePass="changeit" />
   ```

   c. Legen Sie clientAuth="true" fest.

5. Verifizieren Sie die Serversicherheit, wie in Schritt 7 auf Seite 83 beschrieben.

Aktivieren von SSL ausschließlich für die Authentifizierung

Im Rahmen dieser Aufgabe wird beschrieben, wie Sie Configuration Manager konfigurieren, um ausschließlich die Authentifizierung zu unterstützen. Dabei handelt es sich um die Mindestsicherheitsebene die für die Verwendung von Configuration Manager erforderlich ist.

So aktivieren Sie SSL für die Authentifizierung:

1. Führen Sie eine der folgende Prozeduren zum Aktivieren von SSL auf dem Servercomputer durch, wie unter "Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat" auf Seite 80 bis Schritt 6 auf Seite 83 oder unter "Aktivieren von SSL auf dem Servercomputer mit einem Zertifikat von einer Zertifizierungsstelle" auf Seite 83 bis Schritt 5 auf Seite 85 beschrieben.

2. Geben Sie den folgenden URL in den Webbrowser ein: **http://<Configuration Manager-Servername oder IP-Adresse>:8080/cnc**.

Aktivieren der Clientzertifikatsauthentifizierung

Im Rahmen dieser Aufgabe wird beschrieben, wie Sie Configuration Manager einrichten, um die Authentifizierung mit clientseitigen Zertifikaten zu akzeptieren.

So aktivieren Sie die Clientzertifikatsauthentifizierung:

1. Führen Sie die Prozedur zum Aktivieren von SSL auf dem Servercomputer durch, wie unter "Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat" auf Seite 80 beschrieben.
2. Öffnen Sie folgende Datei: <**Configuration Manager-Installationsverzeichnis**>**\conf\lwssofmconf.xml.** Suchen Sie nach dem Abschnitt, der mit in-client certificate beginnt. Beispiel:

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

   Aktivieren Sie die Clientzertifikatsfunktion, indem Sie das Kommentarzeichen entfernen.
3. Extrahieren Sie entsprechend der folgenden Prozedur den Benutzernamen aus dem Zertifikat:
   a. Der Parameter **userIdentifierRetrieveField** gibt an, welches Zertifikatsfeld den Benutzernamen enthält. Folgende Optionen stehen zur Verfügung:
      - **SubjectDN**
      - **SubjectAlternativeName**

   b. Der Parameter **userIdentifierRetrieveMode** gibt an, ob der Benutzername aus dem gesamten Inhalt des relevanten Felds besteht oder nur aus einem Teil. Folgende Optionen stehen zur Verfügung:
      - **EntireField**
      - **FieldPart**

   c. Ist **FieldPart** der Wert von **userIdentifierRetrieveMode**, dann gibt der Parameter **userIdentifierRetrieveFieldPart** an, welcher Teil des relevanten Feld den Benutzernamen darstellt. Bei dem Wert handelt es sich um einen Codebuchstaben, der auf einer im Zertifikat definierten Legende basiert.

4 Öffnen Sie folgende Datei: **<Configuration Manager-Installationsverzeichnis>\conf\client-config.properties** und bearbeiten Sie die folgenden Eigenschaften:

- Ändern Sie **bsf.server.url**, um das HTTPS-Protokoll zu verwenden, und ändern Sie den HTTPS-Port in den unter "Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat" auf Seite 80 beschriebenen Port.
- Ändern Sie **bsf.server.services.url**, um das HTTPS-Protokoll zu verwenden, und ändern Sie den Port in den ursprünglichen Port.

Kennwortverschlüsselung

In der folgenden Tabelle sind die in der Datei **encryption.properties** enthaltenen Parameter aufgeführt, die für die Kennwortverschlüsselung verwendet werden. Weitere Informationen zum Verschlüsseln des Datenbankkennworts finden Sie unter "Verschlüsseln des Datenbankkennworts" auf Seite 79.

Parameter	Beschreibung
cryptoSource	Gibt die Infrastruktur an, in der der Verschlüsselungsalgorithmus implementiert wird. Folgende Optionen stehen zur Verfügung: ➤ **lw.** Verwendet Bouncy Castle-Lightweight-Implementierung (Standardoption) ➤ **jce.** Java Cryptography Enhancement (standardmäßige Java-Kryptographie-Infrastruktur)
storageType	Gibt den Typ des Schlüsselspeichers an. Derzeit wird nur der Binärdateityp unterstützt.
binaryFileStorageName	Gibt an, an welcher Stelle der Hauptschlüssel in der Datei gespeichert ist.
cipherType	Der Typ der Verschlüsselung. Derzeit wird nur **symmetricBlockCipher** unterstützt.

Parameter	Beschreibung
engineName	Der Name des Verschlüsselungs-algorithmus. Folgende Optionen stehen zur Verfügung: ➤ **AES.** American Encryption Standard. Diese Verschlüsselung ist FIPS 140-2-konform. (Standardoption) ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (FIPS 140-2-konform) ➤ **Null**. Keine Verschlüsselung
keySize	Die Größe des Hauptschlüssels. Die Größe wird von dem folgenden Algorithmus bestimmt: ➤ **AES.** 128, 192, oder 256 (Standardoption ist 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156
encodingMode	Die ASCII-Verschlüsselung der binären Verschlüsselungsergebnisse. Folgende Optionen stehen zur Verfügung: ➤ **Base64** (Standardoption) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	Der Modus des Algorithmus. Derzeit wird nur **CBC** unterstützt.

Parameter	Beschreibung
algorithmPaddingName	Der verwendete Auffüllalgorithmus. Folgende Optionen stehen zur Verfügung: ➤ **PKCS7Padding** (Standardoption) ➤ **PKCS5Padding**
jceProviderName	Der Name des JCE-Verschlüsselungs-algorithmus. **Hinweis:** Nur relevant, wenn **crytpSource** auf **jce** festgelegt ist. Für **lw** wird **engineName** verwendet.