HP Universal CMDB Configuration Manager

für Windows- und Linux-Betriebssysteme

Softwareversion: 9.20

Bereitstellungshandbuch

Datum der Dokumentveröffentlichung: Juni 2011
Datum des Software-Release: Juni 2011

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

Aktualisierte Dokumentation

Die Titelseite dieses Handbuchs enthält die folgenden Informationen:

- Software-Versionsnummer zur Angabe der Software-Version.
- Dokument-Releasedatum, das sich mit jeder Aktualisierung des Dokuments ändert.
- Software-Releasedatum zur Angabe des Releasedatums der Software-Version.

Um nach Aktualisierungen des Dokuments zu suchen oder um zu überprüfen, ob Sie die aktuellste Version des Dokuments verwenden, wechseln Sie zu:

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

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport.
Um sich für eine HP Passport-ID zu registrieren, wechseln Sie zu:

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

Alternativ können Sie auf den Link **New user registration** (Neue Benutzer registrieren) auf der HP Passport-Anmeldeseite klicken.

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

TEIL I: INSTALLATION UND KONFIGURATION

TEIL II: ANHÄNGE

Teil I

Installation und Konfiguration

1

Übersicht

Dieses Kapitel umfasst folgende Themen:

Komponenten

HP Universal CMDB Configuration Manager ist ein gemeinsames Release aus mehreren Komponenten:

- **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) ist eine Configuration-Management-Datenbank (CMDB) für IT-Organisationen in Unternehmen, mit der sich Geschäftsservice-Definitionen und zugehörige Infrastrukturbeziehungen dokumentieren, speichern und verwalten lassen.

  UMCDB Foundation implementiert ein Datenmodell, Funktionen für Datenflussverwaltung und Datenmodellierung und stellt außerdem Funktionen für Auswirkungsanalyse, Änderungsverfolgung und Berichterstellung bereit, um CMDB-Daten in verständliche, umsetzbare Informationen umzuwandeln, die bei der Beantwortung kritischer Fragen und Lösung von Geschäftsproblemen helfen.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) verwendet eine neue richtlinienbasierte Topologie- und Inventarkonfigurationssteuerung. Sie wurde speziell für Configuration Manager und Configuration Owner entwickelt und bietet diesen Benutzer neben den in oder durch UCMDB zur Verfügung stehenden CI-Daten und Topologieinhalten die Möglichkeit einer gründlichen Analyse. Configuration Manager stellt die erforderlichen Tools bereit, damit Configuration Manager und Owner mühelos Richtlinien für die Topologie- und Inventarkonfiguration einrichten und ermitteln können, in welchem Maße Organisationsstandards eingehalten werden.

Configuration Manager wird als zusätzlicher Tomcat-basierter Server bereitgestellt. Er kommuniziert mithilfe des umfassenden UCMDB SDK mit dem UCMDB-Server.

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

HP Discovery and Dependency Mapping Advanced Edition (DDMA) ist eine Software mit umfassendem und konstant aktualisiertem Inhalt, die zur bevorzugten Methode für die Beschaffung und Verwaltung von IT-Infrastrukturdaten für UCMDB gehört.

➤ **HP Operations Orchestration**

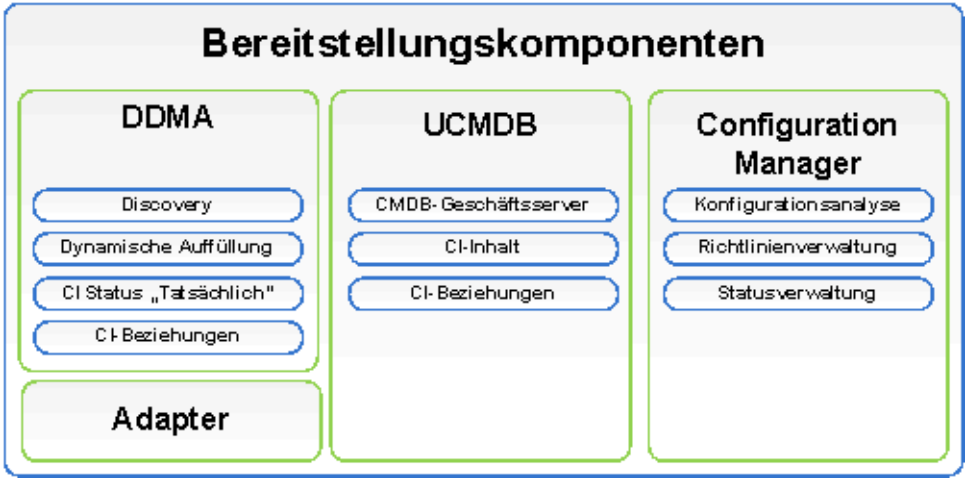
HP Operations Orchestration **(**OO) ist ein Tool für die Erstellung und Bereitstellung von Prozessabläufen (Flows), Durch die intuitiven Funktionen zum Ziehen und Verbinden in OO Studio können Benutzer mit wenigen oder gar keinen Programmierungskenntnissen Flows entwerfen, erstellen, freigeben und anpassen. OO Studio unterstützt die Zusammenarbeit zwischen mehreren Autoren mithilfe von Versionskontrollfunktionen. Der leistungsstarke integrierte Debugger ermöglicht das Testen von Flows in mehreren Umgebungen, beschleunigt die Entwicklung von Inhalten und ermöglicht die Überprüfung von Flows auf ihre stabile, zuverlässige Ausführung.

OOStudio ermöglicht Benutzern auch die einfache Bereitstellung von Flows. Mit OO Studio können Benutzer Flows in mehreren Umgebungen (Entwicklung, Test, Staging und Produktion) vergleichen und höher stufen. Standardprozesse lassen sich mit Studio dokumentieren, um mithilfe einer strukturierten Dokumentation die Einhaltung von Regeln und Standards zu unterstützen.

➤ **Configuration Manager-Integration mit OO**

Configuration Manager bietet die Möglichkeit, OO-Flows aus dem Configuration Manager-Framework auszuführen. Es gibt zwei Hauptmethoden für die Ausführung von OO-Flows:

- ➤ **Prozessintegration** – ermöglicht Ihnen das Öffnen eines Remoteprozeduraufrufs in einer externen Service Desk-Anforderung, die ein bestimmtes CI auf eine bestimmte Konfigurationsrichtlinie abstimmt.
- ➤ **Richtlinienkorrektur** – ermöglicht Ihnen das Auslösen eines OO-Flows, der das Konfigurationsproblem behebt. So können Sie beispielsweise einem virtuellen Hostcomputer zusätzlichen Arbeitsspeicher zuweisen.



Identifizieren der Umgebung

In diesem Handbuch wird der Prozess zur Bereitstellung von HP Universal CMDB Configuration Manager von verschiedenen möglichen Ausgangspunkten beschrieben:

Für Configuration Manager

➤ Wenn Configuration Manager, Version 9.10 installiert ist

Weitere Informationen zum Aktualisieren von Configuration Manager auf die aktuelle Version finden Sie unter "Aktualisieren von Configuration Manager" auf Seite 42.

➤ Wenn keine Configuration Manager-Version installiert ist

Weitere Informationen finden Sie in einem der folgenden Themen:

- ➤ "Installation von HP Universal CMDB Configuration Manager auf einer Windows-Plattform" auf Seite 19
- ➤ "Installation von HP Universal CMDB Configuration Manager auf einer Linux-Plattform" auf Seite 45

Für UCMDB

➤ Wenn eine frühere UCMDB-Version als 9.03 installiert ist

Führen Sie folgende Aktion aus:

➤ Aktualisieren Sie auf UCMDB, Version 9.03. Weitere Informationen finden Sie in der PDF-Datei mit dem *HP Universal CMDB-Bereitstellungshandbuch*. Sie können das Handbuch unter www.hp.com/go/hpsoftwaresupport herunterladen.

➤ Installieren Sie Cumulative Update Pack 2. Sie finden dieses auf dem Configuration Manager-Installationsmedium oder können es unter www.hp.com/go/hpsoftwaresupport herunterladen.

Weitere Informationen zum Konfigurieren der Unternehmensbereitschaft finden Sie unter "Konfigurieren der Datenbank oder des Benutzerschemas" auf Seite 20.

➤ Wenn UCMDB, Version 9.03 installiert ist

Installieren Sie Cumulative Update Pack 2. Sie finden dieses auf dem Configuration Manager-Installationsmedium oder können es unter www.hp.com/go/hpsoftwaresupport herunterladen.

Weitere Informationen zum Konfigurieren der Unternehmensbereitschaft finden Sie unter "Konfigurieren der Datenbank oder des Benutzerschemas" auf Seite 20.

➤ Wenn keine UCMDB-Version installiert ist

Führen Sie eine der folgenden Aktionen aus:

➤ Verwenden Sie den Deployment Manager (nur Windows-Systeme), um UCMDB gleichzeitig mit Configuration Manager zu installieren. Weitere Informationen finden Sie unter "Installation von HP Universal CMDB Configuration Manager auf einer Windows-Plattform" auf Seite 19.

➤ Installieren Sie Configuration Manager auf einem Linux-System, indem Sie den Anweisungen unter "Installation von HP Universal CMDB Configuration Manager auf einer Linux-Plattform" auf Seite 45 folgen.

Allgemeine Informationen

In diesem Handbuch werden auch spezielle UCMDB-Bereitstellungen berücksichtigt, die in Ihrer Umgebung vorhanden sein können (zum Beispiel Hochverfügbarkeitsbereitstellungen), und die entsprechenden Anpassungen an der Bereitstellungsprozedur für diese Bereitstellungen genannt.

Hinweis: Die Installation von UCMDB und Configuration Manager auf einem Server wird unterstützt. Aus Gründen der Skalierung in einer Produktionsumgebung empfiehlt HP Software die Installation dieser Komponenten auf separaten Servern.

Configuration Manager erfordert die Konfiguration von UCMDB mit einem konsolidierten Schemamodus sowie das Erstellen eines neuen UCMDB-Status (autorisierter Status). Diese Konfigurationen werden bei beiden Installationen automatisch von der Bereitstellungsprozedur durchgeführt (unabhängig davon, ob bereits eine UCMDB-Installation vorhanden ist oder ob diese vom Deployment Manager installiert wird).

Wichtig: Wenn Sie auf eine vorhandene UCMDB-Installation verweisen, deren Schema noch nicht konsolidiert ist, kann der Schritt für die Konsolidierung bei stark gefüllten Datenbanken (Datenbanken mit mehr als fünf Millionen CIs) eine lange Zeit in Anspruch nehmen (20 bis 60 Minuten).

Achten Sie darauf, dass der UCMDB-Server ausgeführt werden muss, um die Installation von Configuration Manager abzuschließen, wenn Sie nur Configuration Manager bereitstellen (d. h. eine vorhandene oder aktualisierte UCMDB-Installation verwenden).

Unterstützungsmatrix

Serversystemanforderungen

CPU	Mindestens vier Prozessoren
Arbeitsspeicher (RAM)	Mindestens 4 GB
Plattform	x64
Betriebssystem	Windows (64-Bit) ➤ Windows 2003 Enterprise SP2 und R2 SP2 ➤ Windows 2008 Enterprise SP2 und R2 Linux ➤ Red Hat Enterprise Linux x86 (64-Bit)
Datenbank	➤ Microsoft SQL Server 2005 SP2, 2005 Compatibility Mode 80 (Enterprise Editions) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Webserver	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ HP Universal CMDB, Version 9.03 mit CUP 2 (typische CMDB-Installation) Eine vollständige Liste der Systemanforderungen finden Sie in der PDF-Datei mit dem *HP Universal CMDB-Bereitstellungshandbuch*. **Hinweis:** ➤ Wird der HP Universal CMDB-Server zusammen mit Configuration Manager bereitgestellt, sind die Enterprise Edition von Oracle sowie die Oracle Partitioning-Option erforderlich. ➤ Wenn Sie den HP Universal CMDB-Server vorher mit der Standard Edition von Oracle bereitgestellt haben und Configuration Manager zu Ihrer Installation hinzufügen wollen, müssen Sie zunächst die Standard Edition-Datenbank in eine Enterprise Edition-Datenbank konvertieren und dabei die Partitioning-Option aktivieren.
LDAP (optional)	➤ Active Directory ➤ SunONE 6.x
Empfohlene Datenbankschema-Mindestgröße (optional)	2 GB

Clientanforderungen

Betriebssystem	➤ Windows XP x86 (32-Bit) ➤ Windows Vista x86 (32-Bit und 64-Bit) ➤ Windows 7 x86 (32-Bit und 64-Bit)
Browser	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x, 4
Flash Player-Browser-Plug-In	Flash Player 9 und höher **Hinweis:** Laden Sie Flash Player von folgender Website herunter: http://www.adobe.com/products/flashplayer/.
Bildschirmauflösung	➤ Mindestens 1024x768 ➤ Empfohlen 1280x1024
Farbqualität	Mindestens 16 Bit

HP Operations Orchestration (optional)

HP Operations Orchestration	➤ 7.51, 9.0

2

Installation von HP Universal CMDB Configuration Manager auf einer Windows-Plattform

Wichtig: Lesen Sie die Versionshinweise, um die neusten Installationsanweisungen zu erhalten.

Dieses Kapitel umfasst die folgenden Themen:

Setup vor der Installation

Dieser Abschnitt umfasst die folgenden Themen:

Konfigurieren der Datenbank oder des Benutzerschemas

Hinweis: Diese Aufgabe wird automatisch im Rahmen des Configuration Manager-Installationsprozesses durchgeführt. Sie können sie jedoch auch manuell durchführen.

Sie müssen für die Arbeit mit Configuration Manager ein Datenbankschema bereitstellen. Configuration Manager und UCMDB verwenden unterschiedliche Schemas. Configuration Manager unterstützt Microsoft SQL Server und Oracle Database Server. In dieser Aufgabe wird beschrieben, wie Sie ein Schema für Configuration Manager erstellen. Wenn Sie UCMDB installieren, müssen Sie dafür ebenfalls eine separate Datenbank oder ein Benutzerschema erstellen. Weitere Informationen finden Sie in der PDF-Datei mit dem *HP Universal CMDB-Bereitstellungshandbuch*.

Hinweis: Informationen zu den Systemanforderungen für Microsoft SQL Server und Oracle Server finden Sie unter "Serversystemanforderungen" auf Seite 15.

So konfigurieren Sie Ihre Datenbank:

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

➤ Für **Microsoft SQL Server**: 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 -Port
	DB-Benutzername und -Kennwort
	Für Microsoft SQL: Datenbankname
	Für Oracle: SID

Installieren von Configuration Manager in einer UCMDB-Hochverfügbarkeitsumgebung

Führen Sie die folgenden Schritte aus, um Configuration Manager in einer UCMDB-Hochverfügbarkeitsumgebung zu verwenden:

1 Fahren Sie den Sicherungsserver (passiver Server) herunter. Warten Sie nach dem Herunterfahren zwei Minuten.

2 Installieren Sie Configuration Manager, Version 9.20.

a Verwenden Sie die Load Balancer-Hostdetails.

b Installieren Sie Configuration Manager auf einem dritten Server, nicht auf einem der UCMDB-Server.

3 Stellen Sie sicher, dass UCMDB und Configuration Manager ordnungsgemäß ausgeführt werden.

4 Starten Sie den Sicherungsserver (den passiven Server), um hohe Verfügbarkeit bereitzustellen.

Hinweis: Der Hochverfügbarkeitsmodus wird für HP Universal CMDB Configuration Manager, Version 9.20 selbst nicht unterstützt.

Installieren von Configuration Manager

Der Deployment Manager kann UCMDB, Configuration Manager und DDMA in verschiedenen Konfigurationen (die auf der Produktauswahlseite des Installationsassistenten ausgewählt und konfiguriert wurden) installieren:

- Installieren einer neuen Instanz von UCMDB
- Installieren einer neuen Instanz von Configuration Manager und Verbinden dieser Instanz mit einer neuen oder bestehenden Instanz von UCMDB
- Integrieren einer neuen Instanz von Configuration Manager in eine bestehende Instanz von OO
- Installieren mehrerer Instanzen von DDMA

Hinweis:

- Der Deployment Manager bietet Ihnen die Möglichkeit, Produkte, Komponenten und Integrationen auf einem Zielcomputer zu installieren. Die Deinstallation oder Änderung von Produkten sowie die Installation von Patches auf einem installierten Produkt wird vom Deployment Manager nicht unterstützt und muss manuell durchgeführt werden.
- Sobald Sie auf die Schaltfläche **Next** auf der Seite **Product Selection** geklickt haben, ist es nicht mehr möglich, auf diese Seite zurückzukehren und die Bereitstellungskonfiguration erneut auszuwählen. Wenn Änderungen an der Bereitstellungskonfiguration erforderlich sind, starten Sie den Deployment Manager neu.

So installieren Sie Configuration Manager:

1. Legen Sie zum Starten der Installation das Configuration Manager-Installationsmedium in den Computer ein und suchen Sie nach der Datei **setup.exe**.
2. Doppelklicken Sie auf die Datei **setup.exe**, um den Deployment Manager auszuführen.

3 Deaktivieren Sie die Windows-Firewall auf dem Zielcomputer für die Dauer der Installation. Weitere Informationen zur Firewall finden Sie in Schritt 6 dieses Verfahrens.

4 Akzeptieren Sie die Bedingungen des Endbenutzer-Lizenzvertrags und klicken Sie auf **Next**, um die Seite für die Produktauswahl zu öffnen.

Hinweis: Die Bedingungen des Lizenzvertrags gelten für alle auf der Seite **Product Selection** des Deployment Manager ausgewählten Produkte.

---

5 Wählen Sie die für die Bereitstellung erforderlichen Produkte auf der Seite **Product Selection** aus. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Server Location** fortzufahren.

Auf der Seite **Product Selection** können Sie die Produkte auswählen, die Sie installieren wollen, und die Konfigurationsoptionen angeben, die bei der Bereitstellung durchgeführt werden.

a Wählen Sie eine HP Universal CMDB Foundation-Installationsoption aus.

Es stehen zwei UCMDB Foundation-Installationsoptionen zur Verfügung:

➤ **Connect to an Existing Server** – Ist diese Option ausgewählt, wird Configuration Manager oder DDMA konfiguriert und mit einer bestehenden Instanz eines UCMDB Foundation-Servers verbunden.

Hinweis: Bei der UCMDB-Version auf einem vorhandenen Server muss es sich um Version 9.03 mit CUP 2 oder höher handeln.

- **Install New Server** – Ist diese Option ausgewählt, wird eine neue Instanz eines UCMDB Foundation-Servers installiert, konfiguriert und verbunden und Configuration Manager oder DDMA konfiguriert und mit der neuen Instanz des UCMDB Foundation-Servers verbunden.

b Aktivieren Sie das Kontrollkästchen **Configuration Manager**, um eine neue Instanz von Configuration Manager zu installieren und zu konfigurieren.

Wählen Sie nach Bedarf **Connect to an Existing HP Operation Orchestration instance** aus. Diese Option konfiguriert eine Integration zwischen Configuration Manager und Operations Orchestration, indem Configuration Manager mit Details der OO-Serververbindung aufgefüllt wird.

c **HP Discovery and Dependency Mapping Advanced Edition.** Ist diese Option ausgewählt, werden neue Instanzen von DDMA installiert und konfiguriert.

Mit der Option **Number of DDMA instances** können Sie mehrere DDMA-Instanzen installieren. Die in diesem Eingabefeld angegebene Zahl gibt an, wie viele DDMA-Instanzen mit einer UCMDB-Serverinstanz verbunden sind.

Hinweis: Der Deployment Manager unterstützt mehrere Bereitstellungen von DDMA-Instanzen in derselben DMZ.
Der Deployment Manager unterstützt maximal zehn Instanzen von Discovery-Proben in einer Bereitstellung. Sind zusätzliche Discovery-Proben erforderlich, installieren Sie diese in mehreren Bereitstellungsphasen jeweils in Zehnergruppen.

---

6 Geben Sie den Remoteserverstandort und die Anmeldeinformationen der Zielbereitstellungscomputer für alle Produkte an, die Sie auf der Seite **Server Location** für die Bereitstellung ausgewählt haben. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Connections** fortzufahren.

Bereitstellungsoptionen

Wählen Sie eine Bereitstellungsoption für den Zielstandort aus. Zwei Optionen stehen zur Verfügung:

- **Deploy on the local machine** – Verwenden Sie diese Option, wenn Sie ein Produkt auf demselben Computer wie den Deployment Manager bereitstellen wollen. In diesem Fall sind die Felder für die Remotehostdetails und Anmeldeinformationen deaktiviert.
- **Deploy on the following machine** – Wenn Sie diese Option auswählen, müssen Sie die Adresse des Remotehosts und Betriebssystemdetails bereitstellen. Die bereitgestellten Anmeldeinformationen müssen über Administatorrechte für den Remotehost verfügen.

Hinweis: Achten Sie bei der Angabe des Hostnamens für die Produktbereitstellung darauf, nur Buchstaben (a-z), Ziffern (0-9) und Bindestriche ('-') zu verwenden.

Die folgenden Informationen sind bei der Angabe von Remotecomputerdetails relevant:

- **WMI and SMB Protocols** – werden für die Verbindung zum Remotecomputer verwendet. Die folgenden Voraussetzungen müssen erfüllt sein, damit der Deployment Manager erfolgreich eine Verbindung zum Remotecomputer herstellen kann.
  - **WMI Service** – der WMI-Dienst muss auf dem Remotecomputer ausgeführt werden.
  - **Server Service** – um das SMB-Protokoll zu aktivieren, muss der Serverdienst auf dem Remotecomputer ausgeführt werden.

➤ **Windows-Firewall** – der Remotecomputer muss Remote-administratorverbindungen zulassen. Führen Sie den entsprechenden Befehl in der Befehlszeilenkonsole auf dem Remotecomputer aus:

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

Verbindung testen

Klicken Sie auf **Test Connection**, um zu überprüfen, ob die Anmelde-informationen und Details für die Verbindung richtig sind und um die lokalen und Remotesystemressourcen zu analysieren.

Wenn beim Testen der Verbindung ein Fehler auftritt, zeigt der Deployment Manager eine Fehlermeldung mit Details zum Fehler an. Wenn Sie auf die Schaltfläche **Next** klicken, wird die Testverbindungs-verifizierung automatisch erzwungen.

Die Validierung der Computerressourcen wird für folgende Bereiche durchgeführt:

➤ **Betriebssystemplattform** – überprüft, ob das Betriebssystem für die Prooduktbereitstellung zertifiziert ist.

➤ **Speicherplatz** – überprüft, ob genügend Speicherplatz vorhanden ist.

➤ **Arbeitsspeicher** – überprüft, ob genügend physischer Speicher vorhanden ist.

➤ **Ports** – überprüft, ob die erforderlichen Anschlüsse verfügbar sind.

Die von der Testverbindung durchgeführten Ressourcenvalidierungen sind von der jeweils unterstützten Produktmatrix abhängig.

Hinweis: Gibt der Test den Fehler **Unknown** unbekannt zurück, überprüfen Sie, ob die folgenden Dienste auf dem Hostcomputer für die Bereitstellung ausgeführt werden:

- Server
- Windows-Verwaltungsinstrumentation

Stellen Sie sicher, dass die Benutzerkontensteuerung (UAC) deaktiviert ist, bevor Sie auf **Next** klicken.
Weitere Informationen zur Benutzerkonten-steuerung finden Sie unter http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Konfigurieren Sie Verbindungen zwischen den ausgewählten Produkten auf der Seite **Connections**. Die auf der Seite **Connections** angezeigten Verbindungsoptionen richten sich nach den Komponenten, die auf der Produktauswahlseite für die Bereitstellung ausgewählt wurden. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Installation Configuration** fortzufahren.

- **UCMDB to Configuration Manager Integration**

  Dieser Abschnitt wird angezeigt, wenn Sie sich entscheiden, Configuration Manager mit der Option **Connect to an Existing Server** zu installieren, und ermöglicht Ihnen das Konfigurieren der Integration von Configuration Manager mit UCMDB.

  Hinweis: Um eine Verbindung mit einer vorhandenen Instanz von UCMDB herzustellen, muss es sich bei der Installation um UCMDB, Version 9.03 mit CUP 2 oder höher handeln.

Stellen Sie die folgenden UCMDB-Details bereit:

Feld	Definition
UCMDB Host Name/IP	Adresse des UCMDB-Bereitstellungsstandorts. ➤ Ist UCMDB im Hochverfügbarkeitsmodus konfiguriert, folgenden Sie den Anweisungen unter "Installieren von Configuration Manager in einer UCMDB-Hochverfügbarkeitsumgebung" auf Seite 21. ➤ Ist UCMDB auf dem lokalen Computer und Configuration Manager auf einem Remotecomputer installiert, muss der Name der lokalen UCMDB-Instanz der vollqualifizierte Domänenname und nicht "localhost" sein. ➤ Wenn UCMDB und Configuration Manager verschiedene DNS-Domänennamen haben und die LW-SSO-Integration erforderlich ist, müssen Sie den vollqualifizierten Domänennamen im vorhandenen UCMDB-Hosteingabefeld angeben.
Protocol	HTTP- oder HTTPS-Protokoll.
UCMDB HTTP(S) Port	Die Standardwerte für den HTTP- oder HTTPS-Port sind **8080** für HTTP und **8443** für HTTPS.
Client Certificate File	Dieses Feld wird angezeigt, wenn das HTTPS-Protokoll ausgewählt ist. Sie müssen die UCMDB-Clientzertifikatsdatei manuell auf dem Configuration Manager-Zielhost platzieren und den vollständigen Dateipfad samt Dateiname im daneben befindlichen Eingabefeld angeben. Wenn UCMDB HTTPS verwendet, ist ein Schlüsselaustausch erforderlich. Der Schlüsselaustausch wird nicht während des Verbindungstests überprüft.

Feld	Definition
Customer Name	Der UCMDB-Standardkundenname ist **Default Client**. Der Kundennamenwert wird während der Konfiguration der UCMDB- und Configuration Manager-Integration verwendet. Dieser Wert wird nicht durch den Verbindungstest überprüft. Wenn Sie einen falschen Wert bereitstellen, schlägt die Bereitstellung fehl.
JMX Port	Der Standardwert ist **29601**.
UCMDB System User (JMX)	Der UCMDB-Systembenutzer (JMX) wird zum Aktivieren von JMX-Funktionen wie das Erstellen eines Configuration Manager-Integrationsbenutzers und Bereitstellen des Configuration Manager-Pakets verwendet. Der Standardwert ist **sysadmin**.
UCMDB System Password	Das Kennwort des UCMDB-Systembenutzers. Der Standardwert ist **sysadmin**.

Hinweis: Configuration Manager wird mit einem internen Benutzerrepository konfiguriert. Wenn Sie ein externes LDAP als Benutzerrepository verwenden wollen, müssen Sie Configuration Manager für dessen Verwendung konfigurieren.
Weitere Informationen finden Sie unter "Systemeinstellungen" im *HP Universal CMDB Configuration Manager-Benutzerhandbuch*.

➤ **Configuration Manager to OO Integration**

Dieser Abschnitt wird angezeigt, wenn Sie die Option **Connect to an Existing HP Operation Orchestration instance** auswählen. Sie können darin eine Configuration Manager-Integration mit OO konfigurieren.

Stellen Sie die folgenden OO-Details bereit:

Feld	Definition
OO Version	Gültig sind die OO-Versionen 7.5 und 9.0.
OO Host Name/IP	Die Host- oder IP-Adresse des OO-Servercomputers.
OO Port Number	Die Standardportnummer ist **8443**.
OO Username	Der OO-Standardbenutzername ist **admin**. Der Benutzer muss in OO als extern konfiguriert sein.
OO Password	Das OO-Standardkennwort ist **admin**.

➤ **DDMA Configuration**

Die folgenden Felder werden angezeigt, wenn Sie die Option **Discovery and Dependency Mapping Advanced Edition instance** auswählen. Sie können damit eine DDMA-Verbindung zu UCMDB konfigurieren.

Stellen Sie die folgenden DDMA-Details bereit:

Feld	Definition
Data Flow Probe Identifier	Der Standardwert ist der Hostname des DDMA-Hostcomputers. Das Feld wird automatisch aufgefüllt. Sie können diesen Wert ändern.
Use Default Domain	Diese Option ist standardmäßig ausgewählt und wirkt sich auf den Domänennamenwert aus. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie den Standardnamen in einen anderen Wert ändern.
Domain Name	Der Standardwert ist auf **DefaultDomain** festgelegt. Deaktivieren Sie das Kontrollkästchen **Use Default Domain**, um dieses Feld zu aktivieren.

Feld	Definition
Initial Heap Size in MB	Die der JVM von DDMA ursprünglich zugewiesene Speichergröße. Der Standardwert ist 256 MB.
Maximum Heap Size in MB	Die der JVM zugewiesene maximale Speichergröße. Der Standardwert ist 512 MB.

8 Legen Sie die Details zum Bereitstellungszielverzeichnis für die Produktbereitstellungen fest, die Sie auf der Seite **Installation Configuration** ausgewählt haben. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Database Configuration** fortzufahren.

Für jedes ausgewählte Produkt wird ein Standardverzeichnispfad bereitgestellt. Wenn Sie eine Bereitstellung auf einem lokalen Rechner durchführen, ist eine Option zum Durchsuchen verfügbar, damit Sie einen anderen Verzeichnispfad auswählen können. Wenn Sie eine Installation auf einem Remotecomputer durchführen, ist diese Option deaktiviert.

Hinweis: Das Installationsverzeichnis darf keine Leerzeichen im Namen enthalten. Außerdem dürfen nur englische Buchstaben (a-z), Ziffern (0-9) sowie Bindestriche ('-') verwendet werden.

---

9 Konfigurieren Sie die Datenbankverbindung und das Datenbankschema der einzelnen Produkte auf der Seite **Database Configuration**. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Ports Configuration** fortzufahren.

Sie können die folgenden Datenbanken (Schemas) konfigurieren:

- UCMDB-CM-Schema
- UCMDB-Schema

➤ UCMDB-Historienschema

Feld	Definition
Database Host Name/IP	Die Adresse des Datenbankserverstandorts.
Port	MSSQL und Oracle verwenden unterschiedliche Standardports. Der Standarddatenbankport für Oracle ist 1521 und der Standarddatenbankport für MSSQL ist 1433.
SID (Oracle)	Der Name der Oracle-Datenbankinstanz.
Admin Username (Oracle)	Geben Sie den Benutzernamen des Oracle-Administrators laut Oracle-Server an.
Admin Password (Oracle)	Geben Sie das Kennwort des Oracle-Administrators laut Oracle-Server ein.
Test Connection	Testen Sie die Verbindung zum Datenbank-zielhost mithilfe der bereitgestellten Anmeldeinformationen.
Schema Name (Oracle)	Geben Sie den Schemanamen ein.
Schema Password (Oracle)	Geben Sie das Schemakennwort ein. Dieses Feld wird angezeigt, wenn Sie ein neues Schema erstellen.
Default Tablespace (Oracle)	Geben Sie den Namen des Standard-Tablespace ein.
Temporary Tablespace (Oracle)	Geben Sie den Namen des vorübergehenden Tablespace ein.
Database Name (MSSQL)	Geben Sie den Namen des Datenbankschemas ein, der auf dem MSSQL-Server verwendet/erstellt werden muss.
Database Username (MSSQL)	Geben Sie den Benutzernamen des MSSQL-Administrators laut MSSQL-Server ein.
Database Password (MSSQL)	Geben Sie das Kennwort des MSSQL-Administrators laut MSSQL-Server ein.

Hinweis:

- Ist der UCMDB-Tablespace voll, ist die Produktbereitstellung zwar erfolgreich, doch werden die Produkte und Komponenten nicht ordnungsgemäß ausgeführt.
- Das Erstellen eines neuen UCMDB-Schemas und Verbinden mit einem bestehenden UCMDB-Historienschema wird nicht unterstützt.
- Das Verwenden der NTLM-Authentifizierung beim Konfigurieren von UCMDB-Schemas mit einer MSSQL-Datenbank, wenn UCMDB remote installiert wird, wird aus Sicherheitsgründen nicht unterstützt. Ist die NTLM-Authentifizierung erforderlich, stellen Sie UCMDB lokal bereit.

Schemamodus

Configuration Manager erfordert die Konfiguration von UCMDB mit einem konsolidierten Schemamodus sowie das Erstellen eines neuen UCMDB-Status.

Wenn Sie auf eine vorhandene UCMDB-Installation verweisen, deren Schema noch nicht konsolidiert ist, kann der Schritt für die automatische Konsolidierung bei stark gefüllten Datenbanken (Datenbanken mit mehr als fünf Millionen CIs) eine lange Zeit in Anspruch nehmen (20 bis 60 Minuten).

Hinweis: Die Oracle Real Application Cluster (RAC)- und SQL Server NTLM-Verbindungen werden im Rahmen dieser Installation nicht unterstützt. Sind diese Verbindungen erforderlich, installieren Sie Configuration Manager zunächst mit einer einfachen Datenbankverbindung. Ändern Sie nach Abschluss des Installationsprozesses dann die Verbindung aus der jeweiligen Produktkonfiguration. Ändern Sie dazu die Datei **database.properties** nach den Spezifikationen Ihrer Datenbank. Weitere Informationen finden Sie unter "Erweiterte Datenbankkonfiguration (für Configuration Manager)" auf Seite 34.

Datenbankkonfigurationsmodus

Configuration Manager und UCMDB müssen unterschiedliche Schemas verwenden.

Mit Configuration Manager können Benutzer die jeweiligen Datenbanken entweder auf einem Oracle- oder einem MSSQL-Datenbankserver konfigurieren.

Konfigurationstypen

Sie können eine Verbindung zu einem vorhandenen Schema herstellen oder ein neues Schema erstellen. Durch die Verbindung mit einem vorhandenen Schema wird dessen Inhalt überschrieben.

Datenbankkonfiguration

Dieser Schritt wird automatisch vom Deployment Manager durchgeführt. Informationen zur manuellen Ausführung dieses Schritts finden Sie unter "Konfigurieren der Datenbank oder des Benutzerschemas" auf Seite 20.

Erweiterte Datenbankkonfiguration (für Configuration Manager)

Es muss eine Datenbankverbindung konfiguriert 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-Datenbanken. Alle Funktionen für systemeigene werden unterstützt, sofern diese Funktionen über den Datenbank-URL konfiguriert werden können. Der URL befindet sich in der Datei **database.properties**.

Nach Beendigung des Deployment Manager-Assistenten können zusätzliche Datenbank- und Schemakonfigurationen vorgenommen werden.

Datenbankkonfigurationsfelder

Es sind zwei Datenbanktypen verfügbar – Oracle und MSSQL. Die Eingabefelder ändern sich danach, welcher Datenbanktyp ausgewählt wurde.

10 Geben Sie die Configuration Manager-Verbindungsports auf der Seite **Port Configuration** an. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Users Configuration** fortzufahren.

Configuration Manager bietet direkt verwendbare Standardport-einstellungen an, die in den Eingabefeldern auf der Seite **Port Configuration** des Assistenten angezeigt werden.

Liegt ein Port-Nummernkonflikt mit einer bestehenden Installation vor, wenden Sie sich an einen IT-Manager, bevor Sie die Port-Nummer ändern.

Feld	Definition
Application HTTP Port	8180
JMX HTTP Port	39900
Tomcat Port	8005
AJP Port	8009 (Apache Java Protocol)
Application HTTPS Port	8143
JMX Remote Port	39600

Klicken Sie auf die Schaltfläche **Revert to Default Values**, um die Ports auf die vom Deployment Manager bereitgestellten Standardwerte zurückzusetzen.

11 Erstellen Sie auf der Seite **User Configuration** die folgenden Benutzer:

- UCMDB-CM-Benutzerinstanz für die ursprüngliche Anmeldung mit Administratorberechtigungen.
- Integrationsbenutzer in UCMDB – Ein Integrationsbenutzer wird in UCMDB nach Bedarf von Configuration Manager erstellt, um die Integration zwischen den beiden Produkten zu unterstützen.

Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Security Configuration** fortzufahren.

12 Aktivieren Sie globales LW-SSO für eine neue Instanz von UCMDB und Configuration Manager auf der Seite **Security Configuration**. LW-SSO wird nur für neue Instanzen von Configuration Manager oder UCMDB konfiguriert, je nachdem, welche Auswahl auf der Seite **Product Selection** vorgenommen wurde. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Summary** fortzufahren.

LW-SSO ist ein modulares Framework zur Validierung verschiedener Authentifizierungstypen und Sicherheitstoken (wie LW-SSO und SAML2). LW-SSO wird zur Verknüpfung und Nutzung authentifizierter Informationen aus verschiedenen Umgebungen in Applikationssicherheitskontexte innerhalb eines Applikations- oder Sicherheitsframeworks verwendet.

Die LW-SSO-Konfiguration unterscheidet sich je nachdem, welche Produktkomponenten ausgewählt sind.

Wenn Sie Configuration Manager mit einer vorhandenen UCMDB- oder OO-Instanz verbinden, wird LW-SSO nur für Configuration Manager konfiguriert. Sie müssen die LW-SSO-Zeichenfolge aus UCMDB oder OO extrahieren und in das Eingabefeld für die LW-SSO-Zeichenfolge eingeben. Stellen Sie bei einer Verbindung mit UCMDB und OO sicher, dass die in UCMDB und OO definierten LW-SSO-Zeichenfolgen übereinstimmen.

Verwenden Sie bei der Verbindung einer neuen Instanz von Configuration Manager mit einer vorhandenen UCMDB-Instanz den vollqualifizierten Domänennamen als UCMDB-Hostnamen.

So extrahieren Sie die LW-SSO-Zeichenfolge aus UCMDB:

a Öffen Sie UCMDB und wählen Sie **Verwaltung** > **Infrastructure Settings Manager** aus.

b Wählen Sie in der Spalte **Name** das Feld **LW-SSO-Init-Zeichenkette** aus und doppelklicken Sie darauf.

c Kopieren Sie die Zeichenfolge aus dem Eingabefeld **Aktueller Wert**.

d Fügen Sie den Wert in das Eingabefeld **LW-SSO string** auf der Seite **Security Configuration** ein.

Bei der Verbindung von Configuration Manager mit einer neuen UCMDB-Instanz wird LW-SSO automatisch für UCMDB und Configuration Manager konfiguriert.

13 Überprüfen Sie die Installations- und Konfigurationseinstellungen auf der Seite **Summary**. Klicken Sie nach Fertigstellung auf **Next**, um mit der Seite **Validation** fortzufahren.

Auf der Seite **Summary** sind alle Konfigurationsdetails und Benutzereingaben zentral zusammengefasst. Sie können den Inhalt der Zusammenfassung ggf. revidieren, indem Sie auf den Seiten auf die Schaltfläche **Back** klicken, bis Sie zu der gewünschten Seite gelangen, auf der Sie die Bereitstellungseinstellungen anpassen können. Klicken Sie wiederholt auf **Next**, um zur Seite **Summary** zurückzukehren.

14 Der Deployment Manager führt jetzt eine Reihe von Aktionen aus, um sicherzustellen, dass die Systemressourcen der Remotecomputer ausreichend sind, dass die Benutzereingaben richtig sind und um die Datenbankkonfigurationseinstellungen zu überprüfen.
Diese Validierungen zeigen, ob die Benutzerdefinitionseinstellungen den bekannten Umgebungsbeschränkungen entsprechen. Der Validierungsprozess wird automatisch gestartet. Wenn Sie allerdings im Deployment Manager zu einer vorherigen Seite zurückgekehrt sind und Änderungen an der Konfiguration vorgenommen haben, klicken Sie auf **Run Validation**, um den Validierungsprozess zu starten. Klicken Sie nach Fertigstellung auf **Deploy**, um mit der Seite **Deployment** fortzufahren.

15 Auf der Seite **Deployment** wird der jeweilige Status des Bereitstellungsprozesses angezeigt. Der Bereitstellungsprozess beinhaltet Produktinstallationen, die Startprozeduren sowie deren Integration und Verbindung mit anderen Produkten.

Der Bereitstellungsprozess ist abgeschlossen, sobald alle Produkte erfolgreich gestartet wurden.

Klicken Sie auf **Details**, um die Details des Bereitstellungsprozesses anzuzeigen, einschließlich der Schritte, die vom Deployment Manager zur Bereitstellung der einzelnen ausgewählten Produkte durchgeführt wurden.

Klicken Sie auf **Cancel**, um die Bereitstellung so abzubrechen, dass die aktuelle Bereitstellungsaktion fertig gestellt werden kann, bevor die Bereitstellung beendet wird.

Klicken Sie auf **Abort** (nur verfügbar, wenn Sie auf **Cancel** geklickt haben), um einen Abbruch der aktuellen Aktion und der Bereitstellung zu erzwingen. Ein Abbruch der Bereitstellung kann dazu führen, dass die Produkte sich in einem unbestimmten Status befinden.

Validierungen

Die folgende Tabelle enthält eine Liste der vom Deployment Manager durchgeführten Validierungen.

Validierung	Fehlermeldung	Beschreibung
Anmeldeinformationen überprüfen	Credentials verification failed	Die bereitgestellten Benutzeranmelde-informationen sind falsch.
		Die Verbindung konnte nicht hergestellt werden.
Betriebssystem-kompatibilität überprüfen	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	Das eigentliche Zielbetriebssystem entspricht nicht der Liste zertifizierter Betriebssysteme für das Produkt.

Validierung	Fehlermeldung	Beschreibung
Arbeitsspeicher überprüfen	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	Der Zielcomputer verfügt nicht über genügend Arbeitsspeicher für alle zugewiesenen Produkte.
	<Memory> MB of memory are verified to be available on <Target Machine>	Die Validierung war erfolgreich.
Speicherplatz überprüfen	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	Der Zielcomputer verfügt nicht über genügend Speicherplatz für alle zugewiesenen Produkte.
	<Memory> MB of memory are verified to be available on <Target Machine>	Die Validierung war erfolgreich.
Überprüfen, ob alle obligatorischen Eigenschaften bereitgestellt wurden	Missing the target storage device for the product: <Target>	Es ist kein Installations-verzeichnis für das Produkt festgelegt.
Überprüfen, ob ein Bereitstellungs-computer festgelegt ist	No deployment machine is defined for <Product Name>	Das Produkt ist nicht für die Bereitstellung auf einem Computer konfiguriert.
Anmeldeinformationen überprüfen	Credentials verification failed	Falsche Anmelde-informationen.
Überprüfen, ob die Benutzerkontensteuerung deaktiviert ist	The UAC is enabled	Die Benutzerkonten-steuerung ist auf dem Zielcomputer aktiviert.
Freie Ports überprüfen	The required port number <Port> is already in use on <Target>	Der erforderliche Port auf dem Zielcomputer wird bereits verwendet.

Validierung	Fehlermeldung	Beschreibung
Vorhandensein des Zielspeichergeräts überprüfen	The target storage device <Device> does not exist on <Target>	Das ausgewählte Ziel-speichergerät ist auf dem Zielcomputer nicht vorhanden.
Vorhandensein des Schemas überprüfen	Schema <Name> does not exist/ already exist	Das Schema auf dem Zielcomputer ist vorhanden/ist nicht vorhanden.
Vorhandensein der Schemaberechtigung überprüfen	Validate <Permissions> schema tables user permissions existence	Der Datenbankbenutzer verfügt nicht über ausreichend Berechtigungen.
Vorhandensein der Schematabellen überprüfen	Schema Tables <Tables> on the database: <Tables> already exist	Die Schematabellen in der Datenbank sind bereits vorhanden.
Vorhandensein der Schematabellen-Benutzer-berechtigungen überprüfen	The database user does not have the correct permissions	Der Datenbankbenutzer verfügt nicht über die richtigen Berechtigungen.
UCMDB-Verbindung überprüfen	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	Fehler bei der Testverbindung mit UCMDB ist mit den vorliegenden Verbindungseinstellungen.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	Bei der vorhandenen UCMDB-Version muss es sich um Version 9.03 mit CUP 2 oder höher handeln.

Validierung	Fehlermeldung	Beschreibung
Datenbankverbindung überprüfen	The host name/IP address validation failed	Der angegebene Datenbank-Hostname bzw. die IP-Adresse ist nicht erreichbar
	The username or password validation failed	Die angegebenen Benutzeranmelde-informationen sind nicht gültig.
	The port validation failed	Der angegebene Daten-bankport ist nicht erreichbar.
	The SID validation failed	Die angegebene Daten-bank-SID ist in der Datenbank nicht vorhanden.
Installations-überprüfung	The product is already installed	Das Produkt ist bereits auf dem Zielhost installiert.

Aktualisieren von Configuration Manager

Die Aktualisierungsprozedur überprüft zunächst automatisch, ob folgende Voraussetzungen erfüllt sind:

- Es besteht eine funktionierende Verbindung zum UCMDB-Server.
- Der CUP 2-Patch wurde für UCMDB installiert.
- Der JMX-Port ist richtig.

Wurden einige dieser Elemente nicht ordnungsgemäß installiert oder konfiguriert, werden Sie durch eine Fehlermeldung darüber informiert. Sie können das jeweilige Problem beheben und dann die Aktualisierung durchführen.

- Schlägt die Aktualisierung fehl, weil Sie keine Verbindung zu UCMDB herstellen können, überprüfen Sie, ob der UCMDB-Server ordnungsgemäß ausgeführt wird.
- Schlägt die Aktualisierung fehl, weil das Patch nicht installiert ist, installieren Sie CUP 2 gemäß den Anweisungen unter: http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- Schlägt die Aktualisierung fehl wegen eines falschen UCMDB-JMX-Ports, wählen Sie den richtigen JMX-Port aus. Ändern Sie dazu die Eigenschaft **ucmdb.jmx.port** in der Datei **upgrade.properties**, die sich im Ordner **<Configuration Manager-Installationsverzeichnis>\utilities\Upgrade** befindet.

Führen Sie für die Aktualisierung folgende Schritte durch:

Hinweis: Stellen Sie sicher, dass der UCMDB-Server ordnungsgemäß ausgeführt wird, bevor Sie mit der Aktualisierungsprozedur beginnen.

---

1. Sichern Sie Configuration Manager- und UCMDB-Schemas.
2. Suchen Sie die Datei **setup-win64.msi** im Windows-Unterordner des Configuration Manager-Installationsmediums.

3. Doppelklicken Sie auf die Datei, um den Configuration Manager-Installationsassistenten auszuführen.
4. Klicken Sie auf **Next**, um die Seite mit dem Endbenutzer-Lizenzvertrag anzuzeigen.
5. Akzeptieren Sie die Bedingungen der angezeigten Lizenz und klicken Sie auf **Next**, um die Seite **Customer Information** zu öffnen.
6. Geben Sie Ihre Informationen ein und klicken Sie auf **Next**, um die Seite **Setup Type** zu öffnen.
7. Wählen Sie den Ordner aus, in dem Configuration Manager installiert werden soll. Stellen Sie sicher, dass Sie einen anderen Speicherort als für die vorherige Version auswählen.

   Standardmäßig wird Configuration Manager im folgenden Verzeichnis installiert: **c:\hp\cnc920**. Klicken Sie auf **Next**, um den Standardspeicherort zu akzeptieren, oder auf **Browse**, um einen anderen Speicherort auszuwählen. Klicken Sie dann auf **Next**.

   Hinweis: Der Name des Installationsverzeichnisses darf keine Leerzeichen enthalten.

   ---

8. Klicken Sie auf **Next**, um die Installation zu starten.

   Nach Beenden des Installationsassistenten wird automatisch der Configuration Manager-Nachinstallationsassistent gestartet.
9. Klicken Sie auf **Next**, bis Sie gefragt werden, ob Sie eine neue Installation von Configuration Manager oder eine Aktualisierung durchführen wollen.
10. Wählen Sie **Upgrade** aus und klicken Sie auf **Next**.

11 Überprüfen Sie nach Beenden der Installation die Datei **post_installation.log** (im Ordner **<Configuration Manager-Installationsverzeichnis/tmp/log**), um sicherzustellen, dass die Installation fehlerfrei fertig gestellt wurde.

Wenn es während der Aktualisierung zu einem Fehler kommt, wird eine Meldung angezeigt und Sie können den Assistenten schließen. Wenden Sie sich in diesem Fall an den HP Support.

12 Starten Sie den Configuration Manager-Dienst.

Hinweis: Nach der Aktualisierung müssen Sie die SSL-Konfiguration erneut durchführen. Weitere Informationen finden Sie unter "Härten" auf Seite 93.

3

Installation von HP Universal CMDB Configuration Manager auf einer Linux-Plattform

Wichtig: Lesen Sie die Versionshinweise, um die neusten Installationsanweisungen zu erhalten.

Dieses Kapitel umfasst die folgenden Themen:

Setup vor der Installation

Dieser Abschnitt umfasst auch Folgendes:

Voraussetzungen

- Mindestens 400 MB freier Speicherplatz
- X-Display empfohlen

Abrufen der Datei "setup.bin"

Die Linux-Installationsdatei (**setup.bin**) befindet sich auf dem Installationsmedium oder dem ISO-Abbild, das Sie von der HP-Website herunterladen können. Greifen Sie über eine der folgenden Methoden auf die Datei zu:

➤ Bereitstellen einer DVD auf dem Linux-Computer:

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

➤ Bereitstellen eines ISO-Abbilds als Loopback-Blockgeräts:

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

➤ Kopieren Sie die Datei **setup.bin** an einen temporären Speicherort auf dem Linux-Computer.

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.

Wenn Sie über ein X-Display verfügen, wird der Nachinstallationsassistent in der Benutzeroberfläche angezeigt. Ansonsten werden die Informationen des Assistenten im Konsolenmodus angezeigt.

Hinweis: In diesem Handbuch werden die Schritte für den Konsolenmodus erläutert. Bei Verwenden des Assistenten in der Benutzeroberfläche werden jedoch vergleichbare Schritte angezeigt.

So installieren Sie Configuration Manager:

1 Geben Sie folgenden Befehl aus, um Configuration Manager an der aktuellen Position zu installieren:

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

2 Es wird ein Endbenutzer-Lizenzvertrag (EULA) angezeigt, dem Sie zustimmen müssen. Führen Sie einen Bildlauf ans Ende des Endbenutzer-Lizenzvertrags durch, indem Sie wiederholt auf die Leertaste klicken. Geben Sie **Yes** ein und drücken Sie die **Eingabetaste**, um zuzustimmen und mit der Installation fortzufahren.

HP Universal CMDB Configuration Manager wird an der aktuellen Position im Unterordner **cnc** installiert.

Willkommensseite

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

Drücken Sie die **Eingabetaste**, um mit der nächsten Seite fortzufahren.

Auswahl des Datenbankherstellers

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

Drücken Sie die **Eingabetaste**, um Oracle auszuwählen, oder geben Sie **2** ein und drücken Sie dann die **Eingabetaste**, um Microsoft auszuwählen.

Datenbankhostname

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

Geben Sie den Hostnamen Ihrer Datenbank ein und drücken Sie die **Eingabetaste**. Für den Hostnamen wird der Standardwert **localhost** bereitgestellt.

Datenbank-Port

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

Der Standardport für Oracle ist 1521 und der Standardport für Microsoft 1433. Wenn Sie eine andere Portnummer verwenden wollen, geben Sie sie hier ein und drücken die **Eingabetaste**.

SID/Datenbankname

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

Bei Oracle gibt dieses Feld die Datenbank-SID an, bei Microsoft den Datenbanknamen. Geben Sie einen gültigen Wert ein und drücken Sie die **Eingabetaste**.

Benutzer-/Schemaname und Kennwort

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

Geben Sie Ihren Datenbankbenutzernamen ein und drücken Sie die **Eingabetaste**.

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

Geben Sie Ihr Schemakennwort ein und drücken Sie die **Eingabetaste**.

Testen der Datenbankverbindung

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

Drücken Sie die **Eingabetaste**, um die Datenbankverbindung zu testen.

Da dieser Assistent versucht, Tabellen im Datenbankschema zu erstellen, sollten Sie die Datenbankverbindung unbedingt testen. Wenn Sie die Verbindung nicht testen wollen, geben Sie **No** ein und drücken Sie die **Eingabetaste**.

Wurde der Test der Datenbankverbindung erfolgreich abgeschlossen, wird folgende Meldung angezeigt:

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

Drücken Sie die **Eingabetaste**, um fortzufahren. Wenn beim Testen der Verbindung ein Fehler auftritt, wird eine Fehlermeldung angezeigt und Sie werden aufgefordert, den Test erneut auszuführen. Beheben Sie das Verbindungsproblem, führen Sie den Test erneut aus und setzen Sie die Installation fort.

Anwendungsserver-Hostname

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

Der Standardwert für den Hostnamen ist der eigentliche Hostname des Computers. Wenn Sie eine Installation hinter einem Load Balancer oder Reverse-Proxy durchführen, geben Sie hier den externen Namen ein.

Anpassen von Applikationsserver-Ports

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

Wenn Sie Standardports für Configuration Manager verwenden wollen, drücken Sie die **Eingabetaste**. Wenn Sie benutzerdefinierte Ports verwenden wollen, geben Sie **Yes** ein und drücken Sie die **Eingabetaste**. Die Standardportnummern sind:

Portname	Portnummer
HTTP	8180
HTTPS	8443
Tomcat management	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

Wenn Sie sich entschieden haben, die Ports anzupassen, werden Sie aufgefordert, für jeden der oben genannten Ports einen Wert einzugeben. Geben Sie den neuen Wert ein und drücken Sie für jeden die **Eingabetaste**:

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

Ursprünglicher administrativer Benutzer

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

Ein ursprünglicher administrativer Benutzer wird als Administrator oder Super-User des Systems für die Erstanmeldung erstellt. Geben Sie den Administrator-Benutzernamen ein, den Sie verwenden wollen, und drücken Sie die **Eingabetaste**.

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

Geben Sie das Kennwort für den Administratorbenutzer ein und drücken Sie die **Eingabetaste**.

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

Geben Sie das Kennwort für den Administratorbenutzer zur Bestätigung erneut ein und drücken Sie die **Eingabetaste**.

Integrationsbenutzer

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

Wählen Sie den Benutzernamen für die UCMDB-Integration aus. Dieser Benutzer wird während dieses Nachinstallationsprozesses in UCMDB erstellt. HP empfiehlt, einen Benutzernamen zu verwenden, aus dem eindeutig hervorgeht, dass er für Integrationszwecke bestimmt ist (z. B. "cm_integration"). Geben Sie den ausgewählten Benutzernamen ein und drücken Sie die **Eingabetaste**.

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

Geben Sie das Kennwort für den Integrationsbenutzer ein und drücken Sie die **Eingabetaste**.

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

Geben Sie das Kennwort für den Integrationsbenutzer zur Bestätigung erneut ein und drücken Sie die **Eingabetaste**.

Hostname des HP Universal CMDB-Servers

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

Geben Sie den Hostnamen für den UCMDB-Server ein und drücken Sie die **Eingabetaste**. Dieser weicht voraussichtlich vom lokalen Standardhost ab, da davon abgeraten wird, UCMDB und Configuration Manager in einer Produktionsumgebung auf demselben Computer zu installieren.

Port des HP Universal CMDB-Servers

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

Drücken Sie die **Eingabetaste**, um die Standardportnummer 8080 für den UCMDB-Server anzunehmen, oder geben Sie eine Portnummer ein und drücken Sie die **Eingabetaste**.

Protokoll des HP Universal CMDB-Servers

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

Drücken Sie die **Eingabetaste**, um HTTP zu verwenden, oder geben Sie 2 ein und drücken Sie die **Eingabetaste**, um HTTPS zu verwenden.

Hinweis: Wenn Sie HTTPS auswählen, müssen Sie Schlüssel mit UCMDB austauschen. Weitere Informationen finden Sie unter "Härten" auf Seite 93. Bei diesem Verfahren wird HTTPS mit einem nicht gesicherten selbstsignierten Zertifikat eingerichtet.

Kunde des HP Universal CMDB-Servers

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

Drücken Sie die **Eingabetaste**, um den Standardkundennamen für den UCMDB-Server anzunehmen, oder geben Sie einen Kundennamen ein und drücken Sie die **Eingabetaste**.

Systemadministrator-Anmeldeinformationen für den HP Universal CMDB-Server

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

Geben Sie den Systemadministrator-Benutzernamen für den UCMDB-Server ein. Dabei handelt es sich um einen Benutzer, der JMX-Methoden auf dem UCMDB-Server ausführen kann. Der Benutzer ist bereits vorhanden und wird nicht bei der Installation erstellt. Die Anmeldeinformationen für den Systemadministratorbenutzer erhalten Sie beim Administrator des UCMDB-Servers.

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

Geben Sie das Kennwort des Systemadministratorbenutzers für den UCMDB-Server ein und drücken Sie die **Eingabetaste**.

Testen der Verbindung mit dem HP Universal CMDB-Server

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

Drücken Sie die **Eingabetaste**, um die Verbindung mit dem UCMDB-Server zu testen. Da dieser Assistent versucht, Pakete bereitzustellen und den UCMDB-Server zu konfigurieren, sollten Sie die Serververbindung unbedingt testen. Wenn Sie die Verbindung nicht testen wollen, geben Sie **No** ein und drücken Sie die **Eingabetaste**.

Wurde der Test der Serververbindung erfolgreich abgeschlossen, wird folgende Meldung angezeigt:

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

Drücken Sie die **Eingabetaste**, um fortzufahren. Wenn beim Testen der Verbindung ein Fehler auftritt, wird eine Fehlermeldung angezeigt und Sie werden aufgefordert, den Test erneut auszuführen. Beheben Sie das Verbindungsproblem, führen Sie den Test erneut aus und setzen Sie die Installation fort.

Zusammenfassung

Der Assistent zeigt eine Zusammenfassung der von Ihnen jeweils getroffenen Auswahl an, bevor er diese ausführt:

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

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

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

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

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

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

Drücken Sie die **Eingabetaste**, um mit der Konfigurationsphase fortzufahren. Während der Konfiguration wird ein Fortschrittsbalken angezeigt. Der Assistent führt die folgenden Aufgaben durch:

1. Er erstellt die Datenbanktabellen und -objekte.
2. Er füllt die Datenbank mit Standard- und Anfangswerten auf.
3. Er erstellt den ursprünglichen administrativen Benutzer.
4. Er erstellt den Integrationsbenutzer auf dem UCMDB-Server.
5. Er konsolidiert den UCMDB-Server.
6. Er erstellt den autorisierten Status auf dem UCMDB-Server.
7. Er stellt Configuration Manager-Pakete an den UCMDB-Server bereit.

Nach Beenden der Konfiguration wird folgende Meldung angezeigt:

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

Drücken Sie die **Eingabetaste**, um den Assistenten zu beenden.

Option für die unbeaufsichtigte Installation

Sie können Configuration Manager im unbeaufsichtigten Modus installieren. Dabei werden nur die Dateien aus dem Installationspaket extrahiert und es wird keine Konfiguration nach der Installation durchgeführt. Führen Sie den folgenden Befehl aus, um die Installation im unbeaufsichtigten Modus auszuführen:

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

Ausführen des Configuration Manager-Anwendungsservers

Führen Sie die folgenden Befehle aus, um Configuration Manager auszuführen:

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

Sie können ein Skript im Verzeichnis **/etc/init.d** erstellen, um Configuration Manager automatisch beim Start des Computers zu starten.

4

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 "Unterstützungsmatrix" auf Seite 15.

Weitere Informationen zum sicheren Zugriff auf Configuration Manager finden Sie unter "Härten" auf Seite 93.

Weitere Fehlerbehebungsinformationen zum Zugriff auf Configuration Manager finden Sie unter "Fehlerbehebung" auf Seite 129.

Anmelden bei Configuration Manager

1. Geben Sie im Webbrowser den URL des Configuration Manager-Servers ein, beispielsweise http://<Servername oder IP-Adresse>.<Domänenname>:<Port>/cnc, 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.
2. Geben Sie den Benutzernamen und das Kennwort an, die Sie im Configuration Manager-Nachinstallationsassistenten festgelegt haben.
3. Klicken Sie auf **Anmelden**. Nach der Anmeldung wird der Benutzername oben rechts auf dem Bildschirm angezeigt.
4. (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.

Klicken Sie oben auf der Seite auf **Abmelden**, um sich abzumelden.

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.

5

Zusätzliche Verwendungsszenarien

Dieses Kapitel umfasst die folgenden Themen:

Portieren einer Configuration Manager-Installation zwischen Computern

Verwenden Sie dieses Verfahren, wenn Sie eine Installation von Configuration Manager von einem Computer auf einen anderen verschieben wollen, das Datenbankschema dabei intakt bleiben soll und Sie eine Verbindung zum selben UCMDB-Server herstellen wollen.

1. Führen Sie im Ordner <**Configuration Manager-Installationsverzeichnis**>**cnc****bin** den folgenden Befehl aus: edit-server-0.bat.
2. Protokollieren Sie alle Parameter, die Sie finden, einschließlich Ports (z. B. den JMX-Port).
3. Halten Sie den Configuration Manager-Server auf dem Quellcomputer an. (Ist auf dem Quellcomputer ein Windows-System installiert, halten Sie dazu den Configuration Manager-Dienst an).

4 Installieren Sie Configuration Manager auf dem Zielcomputer:

- ➤ Unter Windows: Führen Sie die Datei **setup-win64.msi** aus (sie befindet sich im Ordner **\windows** des Installationsmediums).
- ➤ Unter Linux: Folgen Sie den Anweisungen in "Installieren von Configuration Manager" auf Seite 46.

5 Brechen Sie den Nachinstallationsassistenten ab, wenn dieser gestartet wird.

6 Kopieren Sie alle Dateien aus dem vorherigen Installationsverzeichnis auf dem Quellcomputer an den Speicherort der neuen Installation auf dem Zielcomputer.

7 Ändern Sie auf dem Zielcomputer in **client-config.properties** und **resources.properties** (im Ordner **\conf**) den Hostnamen in den Zielcomputernamen.

Hinweis: Wenn sich der Zielcomputer in einer anderen Domäne befindet als der Quellcomputer, ändern Sie auch den alten Domänenverweis in der Datei **lwssofmconf.xml**.

---

8 Führen Sie die Datei **bin/create-windows-service.bat** auf dem Zielcomputer aus, um den Windows-Dienst zu erstellen. Legen Sie das Flag **-h** fest, um ggf. alle verfügbaren Optionen anzuzeigen und die protokollierten Parameter des Dienstes auf dem Quellcomputer (den Sie in Schritt 2 aufgezeichnet haben) zu verwenden. Verwenden Sie als Domänennamenparameter server-0. Bei Verwendung von Standardwerten sieht der Befehl so aus:

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

9 Starten Sie den Configuration Manager-Server auf dem Zielcomputer.

Ändern von Port-Nummern nach der Installation

1. Halten Sie den Configuration Manager-Server an.
2. Sichern Sie den Inhalt des Ordners **<Configuration Manager-Installationsverzeichnis>\servers\server-0**.
3. Löschen Sie den Ordner **<Configuration Manager-Installationsverzeichnis>\servers\server-0**.
4. Führen Sie das Skript **create-node.bat** mit dem Flag **-h** aus, um die verfügbaren Optionen anzuzeigen. Übergeben Sie alle erforderlichen Port-Nummern an das Dienstprogramm.
5. Ändern Sie den Port auf dem Zielcomputer in **client-config.properties** und **resources.properties** (im Ordner **\conf**) in die neue HTTP-Port-Nummer.
6. Führen Sie das Skript **edit-server-0.bat** aus, das sich im Ordner **<Configuration Manager-Installationsverzeichnis>\bin** befindet.
7. (Für Windows-Systeme) Klicken Sie im angezeigten Fenster mit den Eigenschaften von HP Universal CMDB Configuration Manager auf die Registerkarte **Java** und ändern Sie die Einstellungen **jmx.http.port** und **com.sun.management.jmxremote.port** in die neuen Port-Nummern.
8. Starten Sie den Configuration Manager-Dienst auf dem Zielcomputer.

Kopieren von Systemeinstellungen zwischen Systemen

1. Öffnen Sie Configuration Manager auf dem Quellcomputer. Wechseln Sie zu **System** > **Systemeinstellungen** und klicken Sie auf die Schaltfläche **Konfigurationssatz in eine Zip-Datei exportieren**.

   Vor dem Exportieren können Sie bestimmte Teile der Konfiguration ausschließen, indem Sie das Kontrollkästchen neben den entsprechenden Konfigurationselementen deaktivieren.
2. Kopieren Sie die exportierte Konfiguration auf den Zielcomputer.
3. Öffnen Sie Configuration Manager auf dem Zielcomputer. Wechseln Sie zu **System** > **Systemeinstellungen** und klicken Sie auf die Schaltfläche **Konfigurationssatz importieren**.

Sichern und Wiederherstellen

Sie können eine Installation von Configuration Manager sichern, um bei jedem Fehlertyp, der ansonsten eine vollständig neue Installation erfordern würde, eine Wiederherstellung durchführen zu können.

Sichern

Sichern Sie die folgenden Informationen:

- die Unterordner **conf** und **security** im Configuration Manager-Installationsverzeichnis. Dies kann bei laufendem System erfolgen, ohne dass der Betrieb gestört wird.
- das Datenbankschema

Wiederherstellen (auf einem Windows-System)

Dieses Verfahren sollte nur auf einem neuen System ausgeführt werden, auf dem sich noch keine Configuration Manager-Installation befindet.

1. Installieren Sie Configuration Manager auf dem Zielcomputer, indem Sie die Datei **setup-win64.msi** (die sich im Ordner **\windows** des Installationsmediums befindet) wie folgt im unbeaufsichtigten Modus ausführen:

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

2. Stellen Sie die Verzeichnisse **conf** und **security** wieder her. Verwenden Sie für die Wiederherstellung dieselbe Methode wie für die Sicherung. Überschreiben Sie die Verzeichnisse, die bei der in Schritt 1 durchgeführten Installation erstellt wurden.
3. Stellen Sie das Datenbankschema wieder her. Wenn Sie eine Wiederherstellung auf einem anderen Datenbankserver durchführen, müssen Sie die Eigenschaft **url** in der Datei **database.properties** (im Verzeichnis **conf**) dem neuen Datenbankservernamen entsprechend ändern.

4 Verwenden Sie das Dienstprogramm **create-windows-service** (mit dem Flag **-h**), um die verfügbaren Optionen anzuzeigen), um einen Windows-Dienst zu erstellen.

5 Starten Sie den Configuration Manager-Server.

Wiederherstellen (auf einem Linux-System)

1 Installieren Sie Configuration Manager auf dem Zielcomputer, indem Sie die Datei **setup.bin** ausführen (die sich auf dem Installationsmedium befindet). Weitere Informationen finden Sie unter "Installieren von Configuration Manager" auf Seite 46. Sie müssen die Installation allerdings im ersten Schritt des Nachinstallationsassistenten abbrechen. Alle Dateien werden bereitgestellt, das System wird jedoch nicht konfiguriert.

2 Stellen Sie die Verzeichnisse **conf** und **security** wieder her. Verwenden Sie für die Wiederherstellung dieselbe Methode wie für die Sicherung. Überschreiben Sie die Verzeichnisse, die bei der in Schritt 1 durchgeführten Installation erstellt wurden.

3 Stellen Sie das Datenbankschema wieder her. Wenn Sie eine Wiederherstellung auf einem anderen Datenbankserver durchführen, müssen Sie die Eigenschaft **url** in der Datei **database.properties** (im Verzeichnis **conf**) dem neuen Datenbankservernamen entsprechend ändern.

4 Starten Sie den Configuration Manager-Server.

6

Erweiterte Konfiguration

Dieses Kapitel umfasst die folgenden Themen:

Erweiterte 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**.

Hinweis: Gehen Sie bei der Durchführung einer erweiterten Konfiguration auf einem Linux-System wie folgt vor:

- Ändern Sie umgekehrte Schrägstriche in den Anweisungen in Schrägstriche (/).
- Ersetzen Sie **.bat** in Skriptausführungen durch **.sh**.

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=myDomain
  ```

- **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:

Option	Unterstützt	Empfohlen	Anmerkungen
Sortierung	Groß-/Kleinschreibung wird nicht beachtet. HP Universal CMDB 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.	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.	Beschränkt auf das Sortierungsgebietsschema und die standardmäßigen englischen Definitionen.
Collation Database-Eigenschaft	Serverstandard		

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.

Single Sign-On (SSO)

Single Sign-On zwischen Configuration Manager und UCMDB erfolgt über die LWSSO-Technologie von HP. Weitere Informationen finden Sie unter "Lightweight Single Sign-On- Authentifizierung (LW-SSO) – Allgemeine Referenz" auf Seite 125.

Dieser Abschnitt umfasst die folgenden Themen:

Aktivieren von LW-SSO zwischen Configuration Manager und UCMDB

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 Foundation** 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. Diese Aufgabe sollte manuell ausgeführt werden, sofern sie nicht bereits im Rahmen der Deployment Manager-Installation durchgeführt wurde.

So aktivieren Sie LW-SSO:

1. Bearbeiten Sie im Configuration Manager-Installationsverzeichnis die Datei **\conf\lwssofmconf.xml**.
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 gemeinsame Zeichenfolge, die von allen vertrauenswürdige Applikationen verwendet wird, die mit LW-SSO integriert sind.

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-->
```

Hinweis: Die zweite DNS-Domäne sollte nur hinzugefügt werden, wenn sich Configuration Manager und eine andere Applikation in unterschiedlichen Domänen befinden.

Entfernen Sie das Kommentarzeichen am Anfang und geben Sie ggf. alle Serverdomänen in die DNSDomain-Elemente ein (anstelle von This value should be replaced by your application domain oder This value should be replaced by domain of other application). Diese Liste sollte die Serverdomäne enthalten, die in Schritt 3 auf Seite 78 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 78 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**.

Konfigurieren von LW-SSO in Operations Orchestration

Wird LW-SSO in Configuration Manager und in Operations Orchestration (OO) aktiviert, können bei Configuration Manager angemeldete Benutzer sich über die Webebene bei Operations Orchestration anmelden, ohne einen Benutzernamen und ein Kennwort (für Systemadministratoren) angeben zu müssen.

Hinweis:

- Im folgenden Verfahren stellt <OO_HOME> das Operations Orchestration-Basisverzeichnis dar.
- Bei LW-SSO müssen die zur Anmeldung an Operations Orchestration und Configuration Manager verwendeten Konten denselben Kontonamen haben (unterschiedliche Kennwörter sind jedoch zulässig).
- Für LW-SSO darf das Konto in Operations Orchestration nicht intern sein.

So konfigurieren Sie LW-SSO in Operations Orchestration:

1. Beenden Sie den RSCentral-Dienst.
2. Aktivieren Sie in **<OO_HOME>\Central\WEB-INF\applicationContext.xml** den Import zwischen LWSSO_SECTION_BEGIN und LWSSO_SECTION_END, wie unten dargestellt:

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

3 Aktivieren Sie in <**OO_HOME**>**Central****WEB-INF****web.xml** alle Filter und Zuordnungen zwischen LWSSO_SECTION_BEGIN und LWSSO_SECTION_END, wie unten dargestellt:

```
<!--  LWSSO_SECTION_BEGIN-->

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

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

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

4 Bearbeiten Sie in <**OO_HOME**>**Central****conf****lwssofmconf.xml** die beiden folgenden Parameter:

- domain: Domänenname des OO-Servers.
- initString: Muss identisch sein mit dem initString-Wert in der OO-LW-SSO-Konfiguration (Mindestlänge: 12 Zeichen). Beispiel: smintegrationlwsso.

Beispiel:

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

5 Starten Sie den RSCentral-Dienst neu, damit die Konfiguration wirksam wird.

Durchführen der Identity Manager-Authentifizierung

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

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

Diese Aufgabe umfasst folgende Schritte:

➤ "Voraussetzungen" auf Seite 83

➤ "Konfigurieren von HP Universal CMDB Configuration Manager, sodass der Identity Manager akzeptiert wird" auf Seite 83

Voraussetzungen

Der Configuration Manager-Tomcat-Server sollte mit Ihrem Webserver (IIS oder Apache) verbunden und durch Ihren Identity Manager 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 der Identity Manager akzeptiert wird

So konfigurieren Sie Tomcat Java (AJP13) mit IIS6:

1. Konfigurieren Sie den Identity Manager zum Senden einer Personalisierungskopfzeile/Rückmeldung, die den Benutzernamen enthält, sowie einer Anforderung des Kopfzeilennamens.
2. Öffnen Sie die Datei **<Configuration Manager-Installationsverzeichnis>\conf\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 Identity Manager-URL und ändern Sie den Port in den Identitätsmanagerport:

   bsf.server.url=http://<Identity Manager-URL>:< Identity Manager_port>/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 beschrieben, 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

---

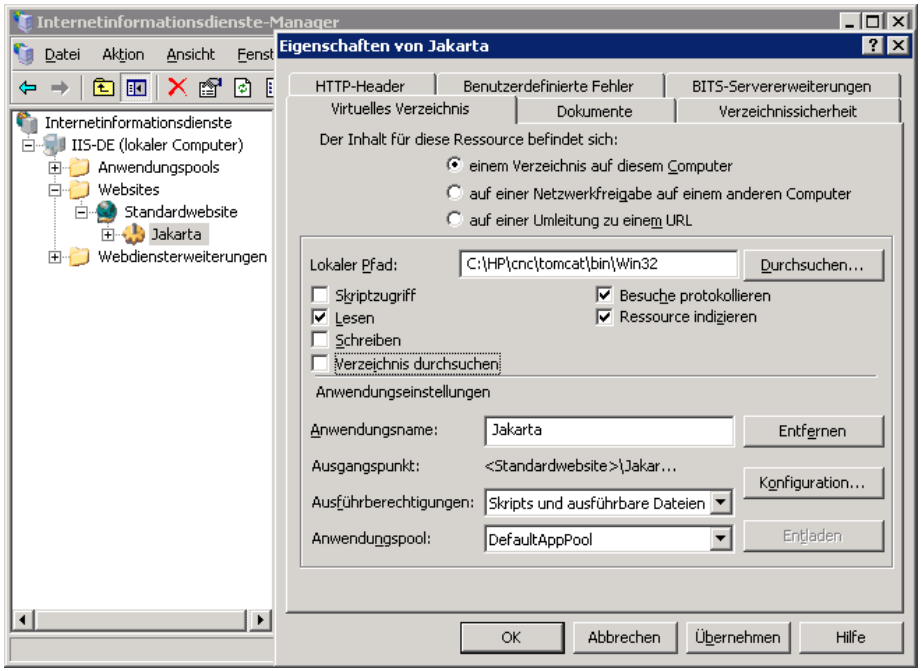
6 Erstellen Sie das virtuelle Verzeichnis im entsprechenden Website-Objekt in der IIS-Konfiguration.

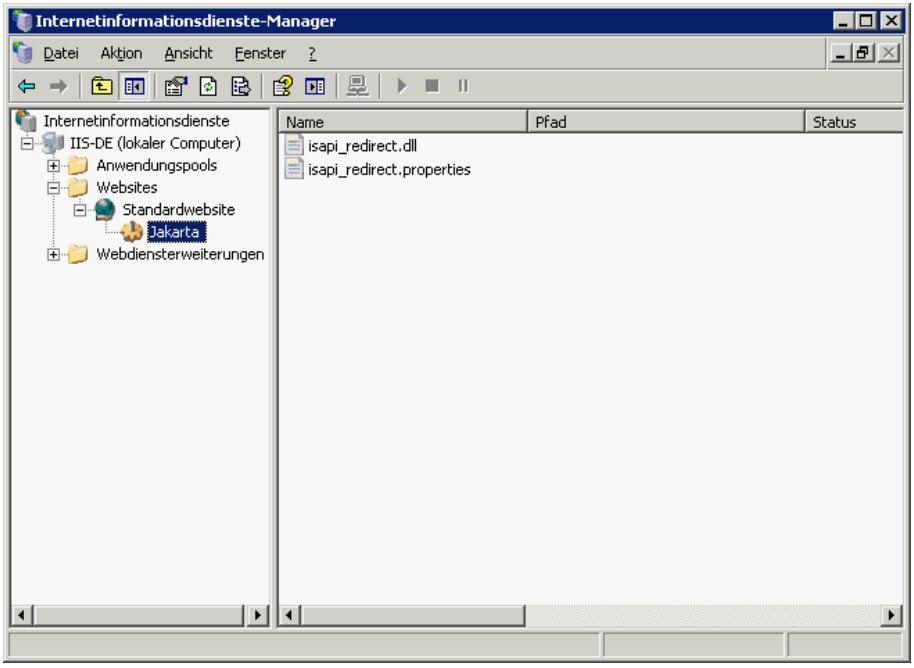
a Öffnen Sie im Windows-Startmenü **Einstellungen** > **Systemsteuerung** > **Verwaltung** >**Internetinformationsdienste-Manager**.

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:





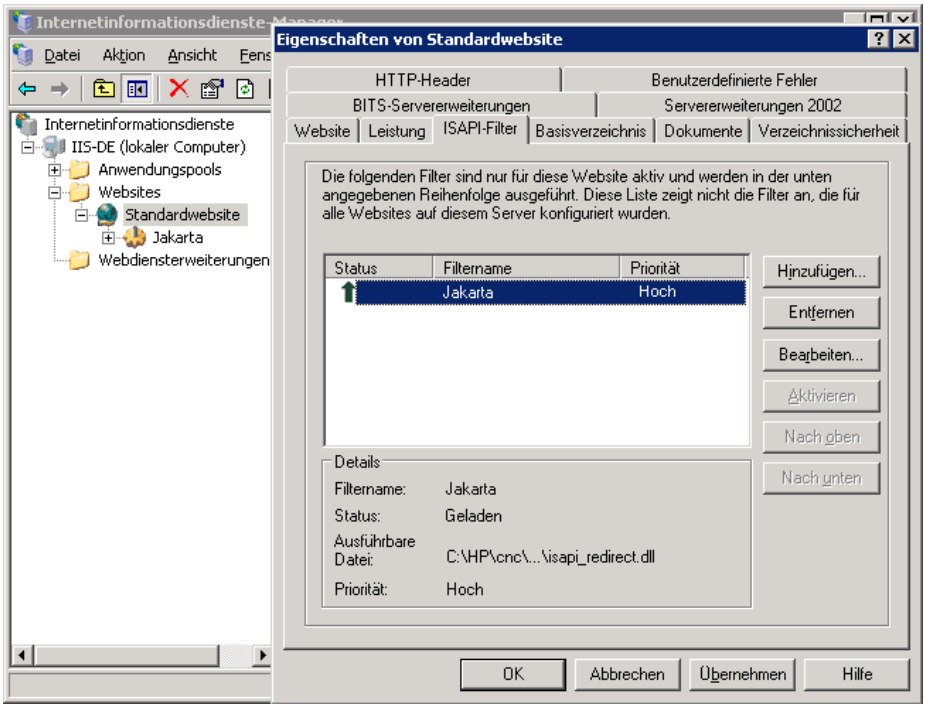
7 Fügen Sie **isapi_redirect.dll** als ISAPI-Filter hinzu.

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

b Wechseln Sie zum Register **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:



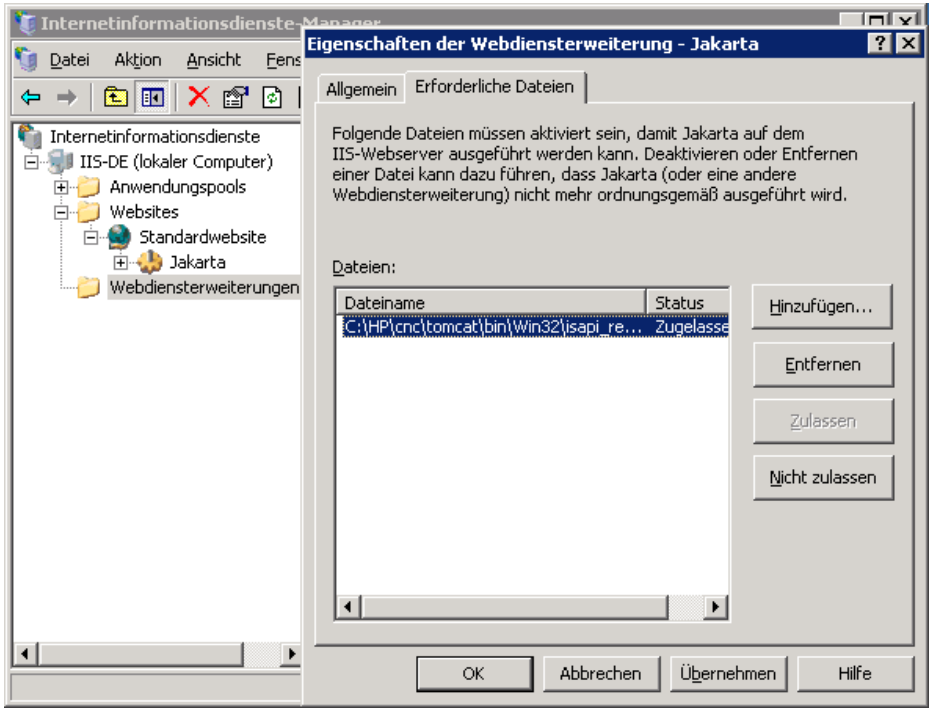
d Klicken Sie auf die Schaltfläche zum Anwenden.

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.

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 IPv4 und IPv6 unterstützt. Weitere Informationen finden Sie in der entsprechenden Dokumentation zu Ihrem Betriebssystem.
2. Öffnen Sie die Datei **client-config.properties**, die sich im Ordner <**Configuration Manager-Installationsverzeichnis**>/**conf** befindet und bearbeiten Sie die folgenden Werte:
   - Ändern Sie den Wert des Parameters **bsf.server.url** und stellen Sie sicher, dass er den Hostnamen verwendet. Beispiel:

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

   - Ändern Sie den Wert des Parameters **bsf.server.services.url** und stellen Sie sicher, dass es sich bei der Configuration Manager-URL um die Hostnamenadresse handelt. Beispiel:

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

3 Öffnen Sie die Tomcat-Datei **servers\server-0\conf\server.xml** und bearbeiten Sie die folgenden Werte:

➤ Fügen Sie die IPv6-Adresse zum SHUTDOWN-Hook hinzu, indem Sie **address="[::]"** zum folgenden Tag hinzufügen:

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

➤ Duplizieren Sie den HTTP-Connector. Fügen Sie für den zweiten Connector die IPv6-Adresse [::] hinzu. Beispiel:

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

➤ Duplizieren Sie den AJP-Connector. Fügen Sie für den zweiten Connector die IPv6-Adresse [::] hinzu. Beispiel:

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

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

4 Fügen Sie die Umgebungsvariable zum Server hinzu: useIPv6="true":

Öffnen Sie die Datei **edit_server-0.bat**, die sich im Ordner <**Configuration Manager-Installationsverzeichnis**>**bin** befindet. Fügen Sie im Register **Java** die folgende Eigenschaft zu den Java-Optionen hinzu: -DuseIPv6.

5 Starten Sie den Server neu.

LDAP

LDAP kann in Configuration Manager konfiguriert werden. Weitere Informationen finden Sie unter "Systemeinstellungen" im *HP Universal CMDB Configuration Manager-Benutzerhandbuch*.

Härten

Dieser Abschnitt umfasst die folgenden Themen:

Hinweis: Nach der Aktualisierung müssen Sie die SSL-Konfiguration erneut durchführen. Weitere Informationen finden Sie unter "Aktualisieren von Configuration Manager" auf Seite 42.

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.

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 97.

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 Sie 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 **cnc920\security\encrypt_repository** zu erstellen und den Verschlüsselungsschlüssel zu erzeugen.
3. Führen Sie das Dienstprogramm **bin\encrypt-password** aus, um das Kennwort zu verschlüsseln. Setzen Sie das Flag **-h**, um die verfügbaren Optionen anzuzeigen.
4. Kopieren Sie das Ergebnis des Dienstprogramms für die Kennwortverschlüsselung und fügen Sie das Verschlüsselungsergebnis in die Datei **conf\database.properties** ein.

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 95.

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.
engineName	Der Name des Verschlüsselungsalgorithmus. 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

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

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 7,0 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

Fügen Sie das Zertifikat den vertrauenswürdigen Speichern des Clients in Internet Explorer auf dem Computer hinzu (**Extras** > **Internetoptionen** > **Inhalt** > **Zertifikate**). Falls Sie dies nicht tun, werden Sie dazu aufgefordert, wenn Sie Configuration Manager das erste Mal verwenden.

Weitere Informationen zum Verwenden von Clientzertifikaten finden Sie unter "Clientzertifikate" auf Seite 107.

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

---

4 Verifizieren der Clientkonfigurationseinstellungen

Öffnen Sie die Datei **client-config.properties**, die sich imVerzeichnis **conf** des Configuration Manager-Installationsverzeichnisses befindet. Legen Sie die Einstellung von **bsf.server.url** auf **https** und den Port auf **8443** fest.

5 Ändern der Datei "server.xml"

Öffnen Sie die Datei **server.xml**, die sich im Ordner <**Configuration Manager-Installationsverzeichnis**>**servers****server-0****conf** 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 Attribute zum HTTPS-Connector hinzufügen:

keystoreFile="<tomcat.keystore-Dateispeicherort>" (siehe Schritt 2 auf Seite 99)
keystorePass="<Kennwort>"

Kommentieren Sie folgende Zeile aus:

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

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 die Datei **server.xml**, die sich im Ordner **<Configuration Manager-Installationsverzeichnis>\servers\server-0\conf** 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="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

Kommentieren Sie folgende Zeile aus:

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

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.

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

Beispiel: java/{Betriebssystemname}/lib.

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.
2. Kopieren Sie **hpcert.cer** auf den Servercomputer in den Ordner **<Configuration Manager-Installationsverzeichnis>\java\bin**

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

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

4 Ändern Sie die Datei **server.xml** (im Ordner **<Configuration Manager-Installationsverzeichnis>\servers\server-0\conf**) wie folgt:

a Nehmen Sie die in Schritt 5 auf Seite 101 beschriebenen Änderungen vor.

b Fügen Sie direkt nach diesen Änderungen die folgenden Attribute zum HTTPS-Connector 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 101 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.

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 99 bis Schritt 6 auf Seite 101 oder unter "Aktivieren von SSL auf dem Servercomputer mit einem Zertifikat von einer Zertifizierungsstelle" auf Seite 102 bis Schritt 5 auf Seite 104 beschrieben.

2 Geben Sie den folgenden URL in den Webbrowser ein:
http://<Configuration Manager-Servername oder IP-Adresse>:8180/cnc.

Aktivieren der Clientzertifikatsauthentifizierung

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

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 99 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 -Installations-verzeichnis>\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 99 beschriebenen Port.
- Ändern Sie **bsf.server.services.url**, um das HTTPS-Protokoll zu verwenden, und ändern Sie den Port in den ursprünglichen Port.

Clientzertifikate

Dieser Abschnitt umfasst die folgenden Themen:

- Clientzertifikatsinformationen auf Seite 107
- Konfiguration auf Seite 111
- Beispiele auf Seite 112

Clientzertifikatsinformationen

In diesem Abschnitt werden die Clientzertifikatsinformationen erläutert und wie eine Benutzer-ID aus einem Clientzertifikat entnommen wird.

- **Benutzer-ID**

  Die Benutzer-ID ist die eindeutige Information aus dem Clientzertifikat, die zur Identifizierung der Identität des Benutzers verwendet wird.

➤ **Grundlegende Clientzertifikatsinformationen**

Zu den grundlegenden Clientzertifikatsinformationen gehören folgende:

Zertifikatsfeld	Beschreibung
Version	Die Version des verschlüsselten Zertifikats. Beispiel: 1 (0x1)
Seriennummer	Eine positive Ganzzahl, die den einzelnen Zertifikaten von der Zertifierungsstelle zugewiesen wird. Beispiel: 0 (0x0)
Signaturalgorithmus	Die Algorithmus-ID, die von der Zertifizierungsstelle zur Signierung des Zertifikats verwendet wurde. Beispiel: md5WithRSAEncryption
Aussteller	Die Entität, die das Zertifikat signiert und herausgegeben hat. Beispiel: CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com
Gültigkeitsdauer	Das Zeitintervall, für das die Zertifizierungsstelle die Verwaltung der Informationen zum Status des Zertifikats gewährleistet: ➤ **Gültig ab**. Gibt das Datum an, an dem der Gültigkeitszeitraum des Zertifikats beginnt. Beispiel: Nov 25 04:34:49 2009 GMT ➤ **Gültig bis**. Gibt das Datum an, an dem der Gültigkeitszeitraum des Zertifikats endet. Beispiel: Nov 25 04:34:49 2010 GMT

Zertifikatsfeld	Beschreibung
Antragsteller	Die Entität, die mit dem öffentlichen Schlüssel verknüpft ist, der im Feld **Schlüsselkennung des Antragstellers** gespeichert ist.
Schlüsselkennung des Antragstellers	Dient zur Aufnahme des öffentlichen Schlüssels und Identifizierung des Algorithmus, mit dem der Schlüssel verwendet wird (z. B. RSA, DSA oder Diffie-Hellman).

Weitere Informationen finden Sie im Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

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

➤ **Feld "Antragsteller"**

Das Feld **Antragsteller** (auch "Subject Distinguish Name" oder "SubjectDN" genannt), gibt die mit dem jeweiligen öffentlichen Schlüssel verbundene Entität an.

Das Feld **Antragsteller** enthält die folgenden relevanten Attribute (es kann auch weitere Attribute enthalten):

Antrag-stellerattribut	Beschreibung des Antragstellerattributs	Beispiel
CN	Allgemeiner Name	CN=Bob BobFamily
emailAddress	E-Mail-Adresse	*emailAddress=bob@example.com*
C	Ländername	C=US
ST	Name des Bundeslands oder Kantons	ST=NY
L	Standortname	L=New York
O	Name der Organisation	O=Work Organization
OU	Name der Organisationseinheit	OU=Managers

Sie können das gesamte SubjectDN-Feld oder das SubjectDN-Attribut verwenden, um die Benutzer-ID aus dem Antragsteller abzurufen.

➤ **Erweiterung von Clientzertifikatsinformationen**

Die für X.509 v3-Zertifikate definierten Erweiterungen bieten Methoden für die Verknüpfung zusätzlicher Attribute mit Benutzern oder öffentlichen Schlüsseln sowie für die Verwaltung von Beziehungen zwischen Zertifizierungsstellen. Das Feld "Alternativer Antragstellername" kann die Benutzer-ID enthalten.

➤ **Feld "Alternativer Antragstellername"**

Die Erweiterung **Alternativer Antragstellername** ermöglicht die Bindung von Identitäten an den Antragsteller des Zertifikats. Diese Identitäten können zusätzlich zu oder anstelle der Identität im Feld **Antragsteller** des Zertifikats hinzugefügt werden.

Das Feld **Alternativer Antragstellername** kann die folgenden Identitäten enthalten:

Identität	Beispiel
otherName	Other Name: Prinzipalname= *bobOtherAltName@example.com*
rfc822Name	RFC822-Name =*bobRFC822AltName@example.com*
dNSName	DNS-Name=example1.com
x400Address	
directoryName	Verzeichnisadresse: E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	IP-Adresse=192.168.7.1
registeredID	Registrierte ID=1.2.3.4

Sie können eine der Identitäten verwenden, um die Benutzer-ID aus dem alternativen Antragstellernamen abzurufen.

Konfiguration

Configuration Manager verwendet LW-SSO, um die Benutzer-ID aus einem Clientzertifikat zu nutzen. Die folgenden Attribute werden vom Clientzertifikathandler zum Konfigurieren von LW-SSO für die Nutzung der Benutzer-ID verwendet:

Für die Nutzung von Informationen aus einem Clientzertifikat sollte Configuration Manager so konfiguriert sein, dass die Benutzer-ID abgerufen werden kann.

Die folgenden Dinge müssen entschieden werden:

- Welches Feld sollte verwendet werden: **SubjectDN** oder **Alternativer Antragstellername**?
- Sollte das gesamte Feld oder nur ein Teil des Felds verwendet werden?
- Wird nur ein Teil des Eingabefelds verwendet, dann stellen Sie einen Wert bereit: Stellen Sie das Antragstellerattribut für **SubjectDN** oder die Identität für **Alternativer Antragstellername** bereit.

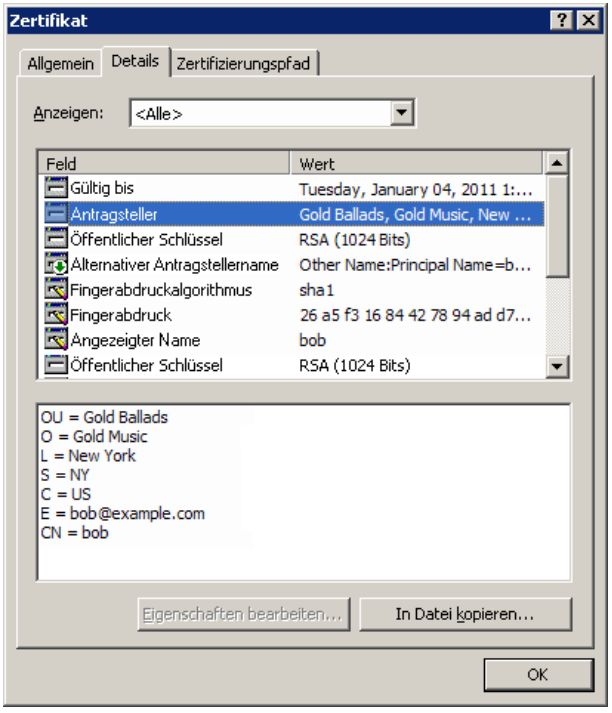
Die folgenden Attribute werden vom Clientzertifikathandler zum Konfigurieren von LW-SSO verwendet:

Attributname	Beschreibung
enabled	Gibt an, ob der Handler aktiviert oder deaktiviert ist. **Wichtig**: Sie sollten den Wert unbedingt explizit auf "false" setzen und den Handler nur aktivieren, wenn die Clientzertifikatvalidierung erforderlich ist.
userIdentifierRetrieveField	Der Parameter **userIdentifierRetrieveField** gibt an, welches Zertifikatsfeld die Benutzer-ID enthält. Die Optionen sind: **SubjectDN** oder **SubjectAlternativeName**.
userIdentifierRetrieveMode	Der Parameter **userIdentifierRetrieveMode** gibt an, ob die Benutzer-ID aus dem gesamten Inhalt des relevanten Felds besteht oder nur aus einem Teil. Die Optionen sind: **EntireField** oder **FieldPart**.

Attributname	Beschreibung
userIdentifierRetrieveFieldPart	Ist **FieldPart** der Wert von **userIdentifierRetrieveMode**, dann gibt dieser Parameter an, welcher Teil des relevanten Felds den Benutzernamen darstellt. Bei dem Wert handelt es sich um einen Codebuchstaben, der auf einer im Zertifikat definierten Legende basiert. **Hinweis**: Das Attribut kann nicht leer sein, wenn **userIdentifierRetrieveMode** auf **FieldPart** gesetzt ist. Das Attribut kann ebenfalls nicht leer sein, wenn **userIdentifierRetrievField** auf **SubjectAlternativeName** gesetzt ist.

Beispiele

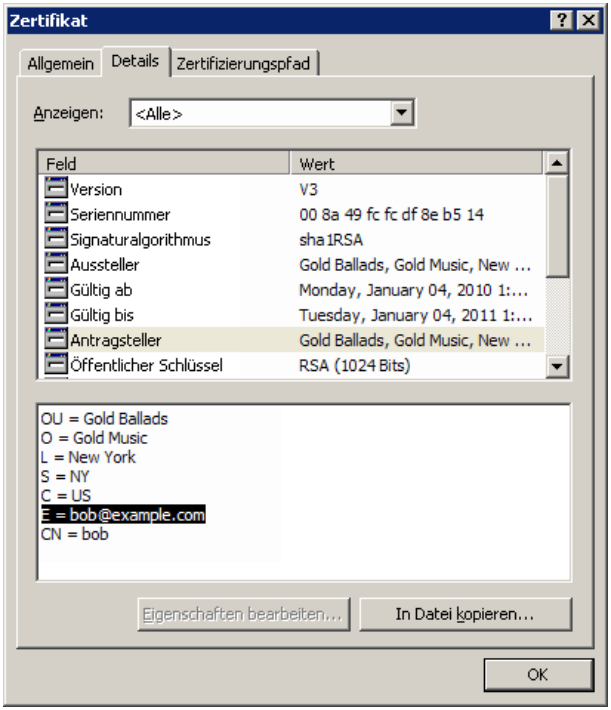
➤ **Die Benutzer-ID ist im Feld "Antragsteller" gespeichert**



Das folgende Beispiel zeigt, wie der Handler konfiguriert werden muss, um die Benutzer-ID dem gesamten SubjectDN-Feld zu entnehmen:

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

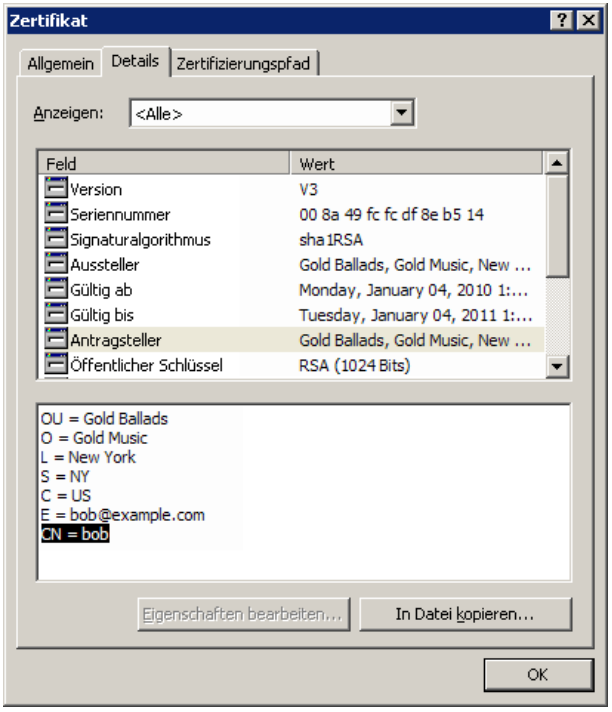
➤ **Die Benutzer-ID ist im E-Mail-Feld des Felds "Antragsteller" gespeichert**



Verwenden Sie die Namen der Felder, die in der Legende des Clientzertifikats angezeigt werden. Das folgende Beispiel zeigt, wie der Handler konfiguriert werden muss, um die Benutzer-ID dem E-Mail-Feld des Felds **Antragsteller** zu entnehmen:

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

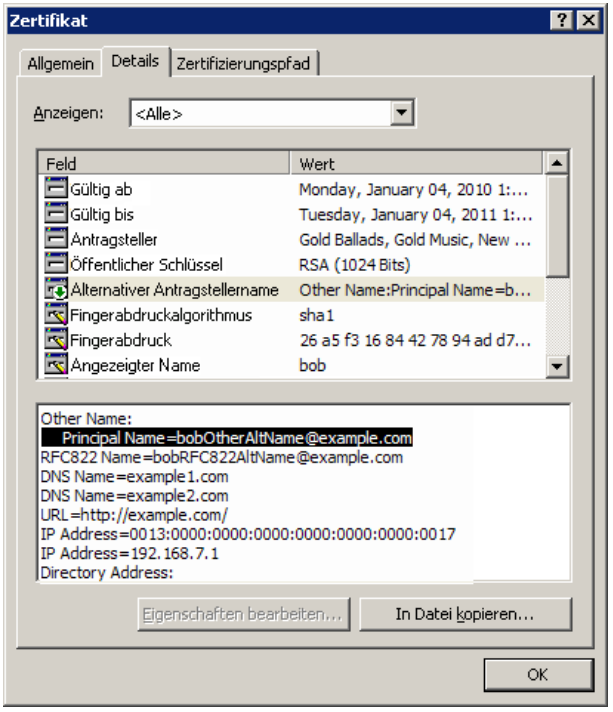
➤ **Die Benutzer-ID ist im Feld "Benutzerdefinierter Name" des Felds "Antragsteller" gespeichert**



Verwenden Sie die Namen der Felder, die in der Legende des Clientzertifikats angezeigt werden. Das folgende Beispiel zeigt, wie der Handler konfiguriert werden muss, um die Benutzer-ID dem Feld **Benutzerdefinierter Name** des Felds **Antragsteller** zu entnehmen:

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

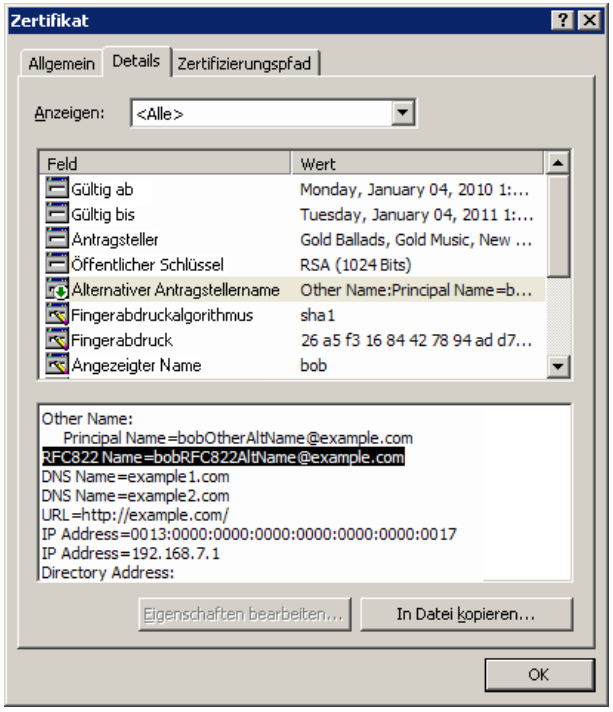
➤ **Die Benutzer-ID ist in der Identität "otherName" des Felds "Alternativer Antragstellername" gespeichert**



Verwenden Sie die Namen der Identitäten, die in der Legende des Clientzertifikats angezeigt werden. Das folgende Beispiel zeigt, wie der Handler konfiguriert werden muss, um die Benutzer-ID der Identität **otherName** des Felds Alternativer Antragstellername zu entnehmen:

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

➤ **Die Benutzer-ID ist in der Identität "rfc822Name" des Felds "Alternativer Antragstellername" gespeichert**



Verwenden Sie die Namen der Identitäten, die in der Legende des Clientzertifikats angezeigt werden. Das folgende Beispiel zeigt, wie der Handler konfiguriert werden muss, um die Benutzer-ID der Identität **rfc822Name** des Felds Alternativer Antragstellername zu entnehmen:

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

Konfigurieren von Configuration Manager für die Verwendung von UCMDB mit SSL

Sie können Configuration Manager für die Verwendung von UCMDB mit SSL (Secure Sockets Layer) konfigurieren. Der SSL-Connector an Port 8443 ist in UCMDB standardmäßig aktiviert.

So exportieren Sie das Serverzertifikat und importieren es in den Clientvertrauensspeicher

1 Wechseln Sie zu <**UCMDB-Installationsverzeichnis**>**bin****jre****bin** und führen Sie folgenden Befehl aus:

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

2 Importieren Sie das Zertifikat in den Configuration Manager-Vertrauensspeicher (der Standard-JRE-Vertrauensspeicher):

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

3 Legen Sie die UCMDB-Verbindungseigenschaften in Configuration Manager fest:

Wechseln Sie zu **System** > **Systemeinstellungen** > **Integrationen** > **UCMDB Foundation**. Legen Sie die Verbindungsstrategie zu **HTTPS**, den UCMDB-Server-Port zum UCMDB-HTTPS-Port und den URL für den UCMDB-Zugriff auf https://<Hostname>:8443 fest.

4 Speichern Sie den Konfigurationssatz und aktivieren Sie ihn. Starten Sie Configuration Manager neu.

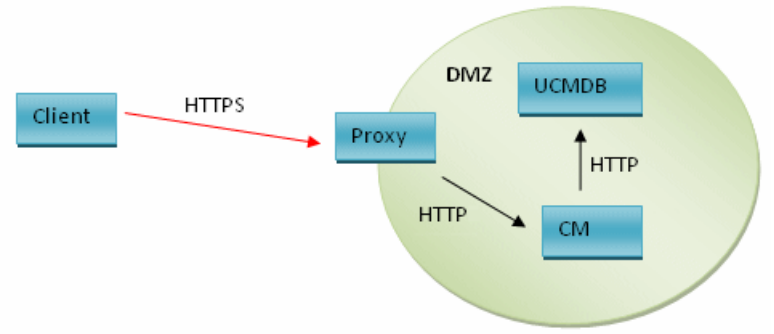
Um Configuration Manager für die Verwendung mit anderen Produkten (wie Load Balancer) und SSL (Secure Sockets Layer) zu konfigurieren, importieren Sie das Sicherheitszertifikat des Produkts in den Configuration Manager-Vertrauensspeicher (Standard-JRE-Vertrauensspeicher), indem Sie folgenden Befehl ausführen:

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

Reverse-Proxy

Befinden sich Configuration Manager und UCMDB in einer DMZ, sollten Sie das System für die Verwendung eines Reverse-Proxy-Servers konfigurieren. Die Konfigurationsschritte sind identisch mit denen für die Konfiguration von UCMDB für die Verwendung eines Reverse-Proxy. Um den Zugriff auf Configuration Manager zu aktivieren, müssen Sie die Pfade **/cnc** und **/bsf** den URLs des Remoteservers zuordnen, auf dem Configuration Manager installiert ist.

Das folgende Bild zeigt den Konfigurationsprozess für einen Reverse-Proxy für Configuration Manager:



Handelt es sich bei dem Reverse-Proxy beispielsweise um einen Apache-Server, fügen Sie der Datei **Apache2.2\conf\extra\httpd-ssl.conf** folgende Zeilen hinzu und starten Sie den Apache-Server dann neu:

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

Unterschiedliche Reverse-Proxy-Typen können unterschiedliche Konfigurationsschritte erfordern. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Proxy-Server.

So konfigurieren Sie einen Reverse-Proxy für Configuration Manager:

Aktualisieren Sie die Datei **client-config.properties** im Ordner **<Configuration Manager-Installationsverzeichnis>\conf** wie folgt:

```
bsf.server.url=https://<Proxyservername>:443/bsf
```

Der Standard-HTTPS-Port für den Apache-Proxy ist 443.

Teil II

Anhänge

A

Kapazitätsbeschränkungen

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

Maximale Anzahl von Ansichten	100
Maximale Anzahl von Richtlinien	300
Maximale Anzahl zusammengesetzter CIs pro Ansicht	5000
Maximale Anzahl gleichzeitiger Benutzer	50
Maximale Anzahl zusammengesetzter CIs im Konfigurationsanalysemodul	1000

B

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.

Weitere Fehlerbehebungsinformationen zu LW-SSO finden Sie unter "LW-SSO – Fehlerbehebung und Einschränkungen" auf Seite 144.

Dieser Abschnitt umfasst die folgenden Themen:

➤ "Unterstützung für mehrere Domänen" auf Seite 126

➤ "URL-Funktion zum Beziehen von SecurityToken" auf Seite 126

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.

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

C

Fehlerbehebung

Dieses Kapitel umfasst die folgenden Themen:

Allgemeine Fehlerbehebung und Einschränkungen

Einschränkungen

Sie können neue CI-Typen, die Sie in UCMDB erstellt haben, erst sehen, wenn Sie sich bei Configuration Manager abgemeldet und dann erneut wieder angemeldet haben.

Fehlerbehebung

Problem. Das Attribut **Name** des CI-Typs **Node** verfügt nicht über die Qualifikation **Änderung überwacht** und wird während der CI-Autorisierung nicht in den autorisierten Status kopiert. Dies geschieht, wenn Configuration Manager, Version 9.20 ohne Content Pack 9 für UCMDB installiert wird.

Lösung. Führen Sie eine der folgenden Aktionen aus:

- Legen Sie für das Attribut **Name** manuell den Qualifizierer **Änderung überwacht** im CIT Manager von UCMDB fest.
- Installieren Sie Content Pack 9.

Problem. Wenn Sie den Configuration Manager-Dienst starten, erhalten Sie eine Fehlermeldung wie diese:

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

Lösung. Führen Sie folgende Aktion aus:

1. Wechseln Sie zum Ordner **<Configuration Manager-Installationsverzeichnis>\cnc\bin** und führen Sie den folgenden Befehl aus:

   ```
   edit-server-0.bat
   ```

2. Wechseln Sie zur Registerkarte **Start**. Wählen Sie in der Dropdownliste **Mode** (unten) statt **exe** den Eintrag **jvm** aus.
3. Wechseln Sie zur Registerkarte **Shutdown**. Ändern Sie im Feld **Class** den letzten Namen von **Boostrap** in **Bootstrap**.
4. Klicken Sie auf **OK**.
5. Führen Sie den Dienst aus.

Deployment Manager – Fehlerbehebung und Einschränkungen

Öffnen Sie zur Fehlerbehebung von Deployment Manger das Sitzungsprotokoll aus der vorherigen Sitzung, das sich in folgendem Verzeichnis befindet.

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

Allgemeine Richtlinien für eine erneute Bereitstellung

Achten Sie bei der Installation auf Warnungen und Fehler, die auf der Seite **Validation** des Deployment Manager angezeigt werden, und klicken Sie auf die jeweilige Detailschaltfläche neben den einzelnen bereitgestellten Komponenten.

Sobald bei der Bereitstellung ein Problem erkannt und eine Lösung gefunden wurde, führen Sie die folgenden Schritte durch:

1. Deinstallieren Sie die bereitgestellten Produkte und starten Sie den Computer neu.
2. Starten Sie den Deployment Manager neu und geben Sie alle Konfigurationen ein.

Probleme bei der Bereitstellung

Problem. Berechtigungsfehler bei der Bereitstellung.

Laut Sitzungsprotokoll gibt es ein Problem mit den Datenbankbenutzerberechtigungen beim Erstellen eines neuen Schemas.

Lösung. Sie müssen über die entsprechenden Berechtigungen verfügen, um eine neue Datenbank zu erstellen. Stellen Sie sicher, dass die zur Bereitstellung verwendeten Benutzeranmeldeinformationen für Tablespace- und Schemaerstellung ausreichend sind.

Problem. Schema-/Datenbankbankkonfigurationsfehler in UCMDB.

Laut Sitzungsprotokoll konnte der Deployment Manager kein Schema bzw. keine Datenbank erstellen.

Lösung:

Hinweis: Beachten Sie, dass Sie kein neues UCMDB-Schema erstellen und mit einem vorhandenen UCMDB-Historienschema verbinden können (unabhängig vom Typ des Datenbankservers).

Stellen Sie sicher, dass UCMDB-Schema und UCMDB-Historienschema nicht den folgenden Verbindungstyp verwenden:

- UCMDB-Schema – Neues Schema erstellen
- UCMDB-Historienschema – Mit einem vorhandenen Schema verbinden

Problem. Schema-/Datenbankbankkonfigurationsfehler in UCMDB.

Laut Sitzungsprotokoll konnte das Schema nicht erstellt werden.

Lösung. Öffnen Sie das Sitzungsprotokoll und suchen Sie nach der folgenden Meldung:
SQL error executing statement CREATE USER <Schemaname>

Achten Sie bei der Benennung des Oracle-Schemas auf der Seite **Database Configuration** des Deployment Manager darauf, nur Buchstaben (a-z), Ziffern (0-9) und den Bindestrich ('-') zu verwenden.

Problem. Das Schema kann nicht erstellt werden, weil nicht genügend Speicherplatz vorhanden ist.

Lösung. Erhöhen Sie den freien Speicherplatz für das Schema oder die Datenbank. Verwenden Sie dazu die von Oracle und Microsoft bereitgestellten Standardverwaltungsschnittstellen.

Problem. Bei der Datenbankkonfiguration gab es folgenden Fehler:
NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

Bei der Auswahl eines MSSQL-Servers mit NTLM-Authentifizierung für die UCMDB-Datenbankkonfiguration schlägt die Datenbankkonfiguration fehl und verursacht einen Bereitstellungsfehler.

Lösung. Stellen Sie UCMDB auf einem lokalen Hostcomputer bereit (der einzige Ort, an dem die NTLM-Authentifizierung unterstützt wird).

Problem. Configuration Manager-Datenbankkonfigurationsfehler beim Erstellen einer neuen Datenbank.

Im Deployment Manager-Detailbereich werden möglicherweise folgende Fehlermeldungen angezeigt:

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

oder

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

Lösung. Stellen Sie sicher, dass der Datenbankbenutzer über folgende Rollenberechtigungen verfügt:

- Connect
- Resource

Problem. Bereitstellung konnte nicht ausgeführt werden, da nicht genügend Speicherplatz auf dem Zielhostcomputer vorhanden ist.

Lösung. Melden Sie sich am Zielhostcomputer an und stellen Sie sicher, dass genügend Speicherplatz für eine erfolgreiche Bereitstellung vorhanden ist:

- UCMDB erfordert 1 GB freien Speicherplatz.
- Configuration Manager erfordert 1 GB freien Speicherplatz.
- DDMA erfordert 1 GB freien Speicherplatz.

Hinweis: Neben den spezifischen Produktanforderungen werden weitere 1 GB freier Speicherplatz für die Verarbeitung temporärer Dateien benötigt.

Problem. Das Dienstprogramm zum Pingen von UCMDB schlägt fehl.

Dieses Dienstprogramm wird vom Configuration Manager-Computer ausgeführt und prüft, ob die Verbindung zur vorhandenen UCMDB-Instanz verfügbar ist. Öffnen Sie das Sitzungsprotokoll und suchen Sie nach der folgenden Meldung:
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

Lösung:

- Vergewissern Sie sich, dass Port 8080 auf dem UCMDB-Zielserver nicht durch die Windows-Firewall blockiert ist.
- Vergewissern Sie sich, dass der Zugriff vom Configuration Manager-Computer auf den UCMDB-Server möglich ist und die UCMDB-Bereitstellung erfolgreich abgeschlossen wurde und ordnungsgemäß ausgeführt wird.

Verbindung zum Hostcomputer nicht verfügbar

Problem. RPC-Fehler: Nicht verfügbar oder unbekannter Fehler.

Das Klicken auf die Schaltfläche **Test Connection** führt zu dem RPC-Fehler **Nicht verfügbar**.

Lösung. Korrigieren Sie ggf. den Hostnamen und stellen Sie sicher, dass der WMI-Dienst und die Serverdienste ausgeführt werden und die Windows-Firewall nicht den Zugriff auf die WMI-Schnittstelle blockiert.

Deaktivieren Sie die Windows-Firewall oder fügen Sie eine Firewallausnahme hinzu, um den Remoteverwaltungszugriff zu ermöglichen.

Öffnen Sie dazu in der Systemsteuerung **Firewall** und wählen Sie **Eingehende Regeln aus.** Aktivieren Sie alle Dateien und Drucker, WMI-Regeln und Port 8080.

Fehler bei Testverbindung

Problem. Zugriff verweigert.

Der Zugriff wird verweigert wegen eines falschen Benutzernamens und/oder Kennworts, ungültiger DNS-Einstellungen oder weil der bei der Bereitstellung verwendete Benutzername nicht über administrative Anmeldeinformationen für den Zielhostcomputer verfügt.

Lösung. Stellen Sie sicher, dass die angegebenen Anmeldeinformationen richtig sind und der Benutzer über administrative Anmeldeinformationen für den Zielhostcomputer verfügt.

Zugriff auf Anwendung nicht möglich

Problem. Nach einer erfolgreichen Bereitstellung ist kein Zugriff auf die Anwendung möglich (UCMDB oder Configuration Manager).

Lösung. Stellen Sie sicher, dass die folgenden UCMDB- und Configuration Manager-Dienste vorhanden sind und ausgeführt werden.

- **UCMDB_Server**-Dienst
- **HPUCMDBCMoasisSNAPSHOTserver0**-Dienst

Prüfen Sie die Bereitstellungsprotokolle in den Sitzungsverzeichnissen auf Fehler.

LW-SSO ist deaktiviert

Problem. Erfolgreiche Bereitstellung – LW-SSO-Funktionen sind deaktiviert.

Lösung. Stellen Sie sicher, dass LW-SSO-Init-Zeichenfolge und -Domäne in UCMDB und Configuration Manager (und ggf. OO) identisch sind.

Prüfen Sie die LW-SSO-Konfigurationseinstellungen in den Produkten mithilfe der folgenden Methoden:

- Configuration Manager – Öffnen Sie die Datei **lwssofmconf.xml** und überprüfen Sie die Definitionen für die Domäne und die Init-Zeichenfolge. Die Datei befindet sich im Ordner **<Configuration Manager-Installationsverzeichnis>\conf**.
- UCMDB – Öffnen Sie UCMDB und wählen Sie **Manager** > **Verwaltung** > **Infrastructure Settings Manager** aus.

Wenn sowohl Configuration Manager als auch UCMDB sich auf Hostcomputern mit unterschiedlichen DNS-Domänen befinden, stellen Sie sicher, dass die Einstellungen in **Vertrauenswürdige Domänen** beide DNS-Domänen beinhaltet und für beide Produkte aktiviert sind.

Sie können den Deployment Manager im Debugmodus aktivieren, um weitere Informationen zur Bereitstellung zu erhalten. Im Debugmodus werden zusätzliche Informationen zur Bereitstellung bereitgestellt.

So aktivieren Sie den Debugmodus:

1. Öffnen Sie nach der Ausführung des Deployment Manager ein Browserfenster und geben Sie %temp% in die Adressleiste ein.
2. Wechseln Sie zum Ordner **hpmdb-dm**.
3. Öffnen Sie die **ini**-Datei in einem Texteditor und fügen Sie die folgende Eigenschaft zur letzten Zeile in der Datei hinzu:

   –Ddebug.mode=true

4. Verwenden Sie **%temp%\HP\ucmdb-dm\ucmdb-dm.exe**, um den Deployment Manager auszuführen.

Configuration Manager-Zugriff – Fehlerbehebung und Einschränkungen

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.

Fehlerbehebung

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

Lösung. Stellen Sie den vorherigen Konfigurationssatz wieder her. Gehen Sie in diesem Fall folgendermaßen vor:

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

   <Configuration Manager-Installationsverzeichnis>\bin\export-cs.bat <Datenbankeigenschaften> --history

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

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

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

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

3 Halten Sie den Configuration Manager-Dienst an.

4 Führen Sie den folgenden Befehl aus, um den vorherigen Konfigurationssatz zu importieren und aktivieren:

```
<Configuration Manager-Installationsverzeichnis>\bin\import-cs.bat
<Datenbankeigenschaften> -i <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 **System** > **Systemeinstellungen** > **Integrationen** > **UCMDB Foundation**, ändern Sie die Einstellungen 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 Schaltfläche **Test** klicken.) Das Datenbankkennwort muss erneut verschlüsselt werden und die neuen Anmeldeinformationen müssen in der Konfigurationsdatei eingegeben werden. Gehen Sie in diesem Fall folgendermaßen vor:

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

   <Configuration Manager-Installationsverzeichnis>\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 Ordner **<Configuration Manager-Installationsverzeichnis>\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: **<Configuration Manager-Installationsverzeichnis>\servers\server-0\conf\server.xml**. Aktualisieren Sie außerdem die relevanten Ports:
  - HTTP (8180): Zeile 69
  - HTTPS (8443): Zeilen 71, 90

Problem. Sie erhalten die Meldung, dass nicht genügend Arbeitsspeicher vorhanden ist.

Lösung. Führen Sie die folgenden Schritte aus, um die Serverstartparameter zu ändern:

1. Führen Sie die folgende Batchdatei aus:

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

2. Ändern Sie die folgenden Einstellungen:

   -Dapplication.ms=<anfängliche Speicherpoolgröße>
   -Dapplication.ms=<maximale Speicherpoolgröße>

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 unter **System** > **Systemeinstellungen** konfiguriert werden.
- Führen Sie einen JMX-Aufruf aus, um die Offline-Analyseberechnung in der relevanten Ansicht auszuführen.
- Wechseln Sie zu **Verwaltung** > **Richtlinien** > **Konfigurationsrichtlinien**. 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 Foundation** 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 "Single Sign-On (SSO)" auf Seite 77. Stellen Sie außerdem sicher, dass der angemeldete Configuration Manager-Benutzer im UCMDB-Benutzerverwaltungssystem festgelegt ist.

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

Lösung. Gehen Sie in diesem Fall folgendermaßen vor:

1. Wechseln Sie zu **System** > **Systemeinstellungen** > **Integrationen** > **UCMDB Foundation**.
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.

LW-SSO – 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.

Fehlerbehebung

Problem: Nach der Anmeldung wird kein LW-SSO-Cookie erstellt.

- **Mögliche Ursache:** Eine nicht leere Domäne ist im LW-SSO-Element der Konfiguration nicht ordnungsgemäß definiert.
- **Mögliche Lösung**: Stellen Sie sicher, dass die im LW-SSO-Element der Konfiguration definierte Domäne der Domäne der Applikation entspricht.
- **Mögliche Ursache:** Eine nicht leere Domäne, die als Parameter an die Funktion **enableSSO** übergeben wird, ist falsch.

- **Mögliche Lösung**: Stellen Sie sicher, dass die Domäne, die als Parameter an die Funktion **enableSSO** übergeben wird, der Domäne der Applikation entspricht.
- **Mögliche Ursache:** Sie haben nicht mit dem vollqualifizierten Domänennamen (FQDN) im Anmelde-URL auf die Applikation zugegriffen, wenn eine Domäne in der LW-SSO-Konfiguration definiert ist (Beispiel: http://192.168.12.13/WebApp).
- **Mögliche Lösung**: Stellen Sie sicher, dass Sie mit dem vollqualifizierten Domänennamen (FQDN) im Anmelde-URL auf die Applikation zugreifen (Beispiel: http://myserver.companydomain.com/WebApp).

Problem: LW-SSO kann kein Cookie für die automatische AutoCookieCreation-Funktion erstellen.

- **Mögliche Ursache:** Eine Domäne ist im LW-SSO-Element der Konfiguration nicht ordnungsgemäß definiert.
- **Mögliche Lösung**: Stellen Sie sicher, dass die im LW-SSO-Element der Konfiguration definierte Domäne der Domäne der Applikation entspricht.

Problem: Das LW-SSO-Token ist nicht überprüft.

- **Mögliche Ursache:** Die beiden Applikationen haben unterschiedliche initString-Parameter im Crypto-Element der Konfiguration (oder anderen Crypto-Parametern).
- **Mögliche Lösung**: Verwenden Sie denselben initString-Parameter in beiden Applikationen (zusätzlich zu allen anderen Crypto-Parametern im LW-SSO-Erstellungselement).
- **Mögliche Ursache:** Die GMT-Zeit weicht zwischen beiden Anwendungen um mehr als 15 Minuten ab.
- **Mögliche Lösung**: Stellen Sie sicher, dass alle Applikationen, die Teil einer LW SSO-Integration sind, dieselbe GMT-Zeit mit einer maximalen Abweichung von 15 Minuten aufweisen.
- **Mögliche Ursache:** Eine Domäne im LW-SSO-Element der Konfiguration ist leer und Sie greifen auf eine zweite Applikation auf einem anderen Computer mit derselben DNS-Domäne zu.
- **Mögliche Lösung**: Stellen Sie sicher, dass die im LW-SSO-Element der Konfiguration definierte Domäne der Domäne der Applikation entspricht.

- **Mögliche Ursache:** Es ist keine Domäne im LW-SSO-Element der Konfiguration definiert und Sie greifen auf eine zweite Applikation auf einem anderen Computer mit derselben DNS-Domäne zu.
- **Mögliche Lösung**: Fügen Sie dem LW-SSO-Element eine Domäne hinzu und stellen Sie sicher, dass die Domäne als identisch mit der Applikationsdomäne definiert ist.

Problem: LW-SSO kann das LW-SSO-Token in einer Umgebung mit mehreren Domänen nicht überprüfen.

- **Mögliche Ursache:** In der Konfiguration einer der Applikationen ist eine Domäne im LW-SSO-Element nicht ordnungsgemäß definiert.
- **Mögliche Lösung**: Die im LW-SSO-Element der Applikationskonfiguration definierte Domäne muss der Domäne der Applikation gemäß der tatsächlich verwendeten Domänen entsprechen.
- **Mögliche Ursache:** In der Konfiguration einer der Applikationen ist eine Domäne in den trustedHosts-Einstellungen (oder protectedDomains-Einstellungen) nicht ordnungsgemäß definiert.
- **Mögliche Lösung**: Stellen Sie sicher, dass die Domänen in den trustedHosts-Einstellungen (oder protectedDomains-Einstellungen) aller Applikationskonfigurationen richtig definiert sind.
- **Mögliche Ursache:** Das LW-SSO-Sitzungscookie wird bei Verwendung von Internet Explorer 6.x, 7.x oder 8.x blockiert oder abgelehnt.
- **Mögliche Lösung**: Fügen Sie alle LW-SSO-Server in den Internet Explorer-Sicherheitszonen auf dem Computer als Intranetzone oder vertrauenswürdige Zone hinzu (Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites > Erweitert). Auf diese Weise können alle Cookies akzeptiert werden.
- **Mögliche Ursache:** Einige Applikationen haben unterschiedliche initString-Parameter im Crypto-Element der Konfiguration (oder anderen Crypto-Parametern).
- **Mögliche Lösung**: Verwenden Sie denselben initString-Parameter in beiden Applikationen (zusätzlich zu allen anderen Crypto-Parametern im LW-SSO-Erstellungselement).
- **Mögliche Ursache:** Bei einigen Applikationen weicht die GMT-Zeit um mehr als 15 Minuten ab.

- **Mögliche Lösung**: Stellen Sie sicher, dass alle Applikationen, die Teil einer LW SSO-Integration sind, dieselbe GMT-Zeit mit einer maximalen Abweichung von 15 Minuten aufweisen.
- **Mögliche Ursache:** Ein Link mit mehreren Domänen führt von der geschützten (HTTPS) zur nicht geschützten (HTTP) Ressource.
- **Mögliche Lösung**: Stellen Sie beim Verlinken oder Übergreifen von einer Domäne zur anderen sicher, dass die erste Link- bzw. domänenübergreifende Anforderung von einer geschützten Ressource (HTTPs) zu einer anderen geschützten Ressource (HTTPS) geht.

IPv6-Unterstützung – Fehlerbehebung und Einschränkungen

Einschränkungen

- Der URL darf keine IP-Adresse enthalten.
- Das Betriebssystem muss IPv6 und IPv4 unterstützen. Sie können sich nicht am Configuration Manager-Server anmelden, wenn die IPv4-Adresse nicht geschlossen ist oder nicht unterstützt wird.
- 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.

Fehlerbehebung

Problem. Nach dem Konfigurieren einer UCMDB-Verbindung zu einer IPv6-Adresse bei der Installation funktioniert die Menüoption **Verwaltung** > **UCMDB Foundation** nicht.

Lösung. Führen Sie folgende Aktion aus:

1. Wechseln Sie zu **System** > **Systemeinstellungen** > **Integrationen** > **UCMDB Foundation**.
2. Fügen Sie um die IP-Adresse im URL-Feld für den UCMDB-Zugriff eckige Klammern hinzu. Der URL sollte folgendermaßen aussehen: http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Speichern Sie den Konfigurationssatz und aktivieren Sie ihn.
4. Starten Sie Configuration Manager neu.

Authentifizierung – Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden bekannte Authentifizierungsprobleme beschrieben.

Problem: Bei der Authentifizierung einer Applikation nach einer Umleitung an einen Authentifizierungspunkt erhalten Sie Fehler 500.

- **Mögliche Ursache:** Die .WAR von Configuration Manager und die .WAR von BSF haben unterschiedliche initString-Parameter im Crypto-Element der Konfiguration (oder anderen Crypto-Parametern).
- **Mögliche Lösung:** Verwenden Sie denselben initString-Parameter in beiden Applikationen (zusätzlich zu allen anderen Crypto-Parametern im LW-SSO-Erstellungselement).

Problem: Bei der Authentifizierung einer Applikation nach einer Umleitung an einen Authentifizierungspunkt können Sie das Anmeldeformular nicht sehen.

Lösung: Das Cookie für die Configuration Manager-Authentifizierungssitzung wird bei Verwendung von Internet Explorer, Version 6.0, 7.0 oder 8.0 blockiert oder abgelehnt. Fügen Sie den Configuration Manager-Server in den Internet Explorer-Sicherheitszonen auf dem Computer als Intranetzone oder vertrauenswürdige Zone hinzu (**Extras** > **Internetoptionen** > **Sicherheit** > **Lokales Intranet** > **Sites** > **Erweitert**). Auf diese Weise können alle Cookies akzeptiert werden.

Problem: Sie erhalten nach der Authentifizierung den Fehler 403.

- **Mögliche Ursache:** Eine Domäne ist im LW-SSO-Element der Applikationskonfiguration nicht ordnungsgemäß definiert.
- **Mögliche Lösung:** Stellen Sie sicher, dass die im LW-SSO-Element der Applikationskonfiguration definierte Domäne der Domäne der Applikation entspricht.
- **Mögliche Ursache:** Sie haben nicht mit dem vollqualifizierten Domänennamen (FQDN) im Anmelde-URL auf die Applikation zugegriffen, wenn eine Domäne in der LW-SSO-Konfiguration definiert ist (Beispiel: http://192.168.12.13/WebApp).
- **Mögliche Lösung:** Stellen Sie sicher, dass Sie mit dem vollqualifizierten Domänennamen (FQDN) im Anmelde-URL auf die Applikation zugreifen (Beispiel: http://myserver.companydomain.com/WebApp).

Problem: Nach der Authentifizierung wird die Seite **Get Acegi User Details** angezeigt.

Lösung: Das Cookie für die Configuration Manager-Authentifizierungssitzung wird bei Verwendung von Internet Explorer, Version 6.0, 7.0 oder 8.0 blockiert oder abgelehnt. Fügen Sie den Configuration Manager-Server in den Internet Explorer-Sicherheitszonen auf dem Computer als Intranetzone oder vertrauenswürdige Zone hinzu (**Extras** > **Internetoptionen** > **Sicherheit** > **Lokales Intranet** > **Sites** > **Erweitert**). Auf diese Weise können alle Cookies akzeptiert werden.