HP Universal CMDB

Für Windows und Red Hat Enterprise Linux Betriebsysteme

Softwareversion: 10.00

HP Universal CMDB und Configuration Manager – Handbuch für das Härten

Datum der Dokumentveröffentlichung: Juni 2012

Datum des Software-Release: Juni 2012

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 U.S.-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

© Copyright 2002 - 2012 Hewlett-Packard Development Company, L.P.

Markenhinweise

Adobe™ ist eine Marke von Adobe Systems Incorporated.

Microsoft® und Windows® sind in den USA eingetragene Marken der Microsoft Corporation.

UNIX® ist eine eingetragene Marke von The Open Group.

Aktualisierte Dokumentation

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

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

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

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

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Hier können Sie sich für eine HP Passport-ID registrieren:

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 Online-Website von HP unter:

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

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

Der Online-Support von HP Software bietet Kunden mit Hilfe interaktiver technischer Support-Werkzeuge die Möglichkeit, ihre Probleme 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-Support-Kontakten
- 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

Kapitel 1

Einführung zum Härten

Dieses Kapitel umfasst folgende Themen:

Härten – Übersicht

In diesem Abschnitt wird das Konzept sicherer HP Universal CMDB-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.

HP Universal CMDB 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) HP Universal CMDB-Implementierung erforderlich sind.

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

Es wird dringend empfohlen, dass Sie einen Reverse-Proxy mit HP Universal CMDB verwenden, um eine sichere Architektur zu erstellen. Informationen zum Konfigurieren eines Reverse-Proxy für HP Universal CMDB finden Sie unter "Verwenden eines Reverse-Proxy" auf Seite 34.

Wenn Sie für HP Universal CMDB eine andere als die in diesem Dokument beschriebene sichere Architektur einsetzen müssen, wenden Sie sich an die HP Software-Unterstützung, um zu bestimmen, welche Architektur am besten für Sie geeignet ist.

Informationen zum Härten der Data Flow Probe finden Sie unter "Härten der Data Flow Probe" auf Seite 65.

Hinweis:

- Bei den Härtungsprozeduren wird davon ausgegangen, dass Sie nur die in diesen Kapiteln vorgegebenen Anweisungen umsetzen und keine sonstigen, anderweitig dokumentierten Härtungsschritte 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.
- Bei den Prozeduren in den folgenden Kapiteln wird vorausgesetzt, dass die Durchführung auf dedizierten Computern für HP Universal CMDB erfolgt. Bei paralleler Verwendung der Computer für andere Zwecke als HP Universal CMDB können Probleme auftreten.
- Die in diesem Abschnitt bereitgestellten Informationen zum Härten stellen keine Anleitung für eine Risikobewertung Ihrer Computersysteme dar.

Härten – Vorbereitungen

- Evaluieren Sie die Sicherheitsrisiken/den Sicherstatus Ihres allgemeinen Netzwerks und nutzen Sie diese Kenntnisse, wenn Sie entscheiden, wie HP Universal CMDB optimal in Ihr Netzwerk integriert werden kann.
- Eignen Sie sich umfassende Kenntnisse des technischen HP Universal CMDB-Frameworks sowie der HP Universal CMDB-Sicherheitsfunktionen an.
- Lesen Sie sämtliche Richtlinien für das Härten.
- Stellen Sie sicher, dass HP Universal CMDB uneingeschränkt funktionsfähig ist, bevor Sie mit den Prozeduren beginnen.
- Befolgen Sie die Schritte der Härtungsprozeduren in jedem Kapitel in chronologischer Reihenfolge. Wenn Sie beispielsweise entscheiden, den HP Universal CMDB Server für SSL-Unterstützung zu konfigurieren, lesen Sie den Abschnitt "Aktivieren der SSL-Kommunikation" auf Seite 18 und befolgen Sie dann alle Anweisungen in chronologischer Reihenfolge.
- HP Universal CMDB unterstützt keine Standardauthentifizierung mit leeren Kennwörtern. Lassen Sie das Kennwort nicht leer, wenn Sie die Verbindungsparameter der Standardauthentifizierung einrichten.

Tipp: Drucken Sie die Härtungsprozeduren aus und haken Sie jeden Schritt bei der Umsetzung ab.

Bereitstellen von UCMDB in einer sicheren Architektur

Für die sichere Bereitstellung Ihrer HP Universal CMDB Server werden mehrere Maßnahmen empfohlen:

- **DMZ-Architektur mit Firewall**

  Bei der sicheren Architektur, die in diesem Dokument beschrieben wird, handelt es sich um eine typische DMZ-Architektur, in der ein Gerät als Firewall genutzt wird. Durch das grundlegende Konzept einer solchen Architektur soll eine vollständige Trennung erzielt und der direkte Zugriff zwischen den HP Universal CMDB-Clients und dem HP Universal CMDB Server vermieden werden.

- **Sicherer Browser**

  Internet Explorer und Firefox in einer Windows-Umgebung müssen so konfiguriert sein, dass Java-Skripts, Applets und Cookies auf sichere Weise verarbeitet werden.

- **SSL-Kommunikationsprotokoll**

  Das SSL-Protokoll (Secure Sockets Layer) sichert die Verbindungen zwischen Client und Server. URLs, die eine SSL-Verbindung erfordern, verwenden HTTPS, eine sichere Version von HTTP (Hypertext Transfer Protocol). Weitere Informationen finden Sie unter "Aktivieren der SSL-Kommunikation" auf Seite 18.

- **Reverse-Proxy-Architektur**

  Zu den sicheren und empfohlenen Lösungen zählt die Bereitstellung von HP Universal CMDB mit einem Reverse-Proxy. HP Universal CMDB bietet vollständige Unterstützung für eine sichere Reverse-Proxy-Architektur. Weitere Informationen finden Sie unter "Verwenden eines Reverse-Proxy" auf Seite 34.

Systemzugriff

Abschottung beim Zugriff auf Java JMX

Hinweis: Die hier beschriebene Prozedur kann auch für die JMX-Konsole der Data Flow Probe verwendet werden.

Führen Sie die folgende Prozedur aus, um sicherzustellen, dass erst nach der Eingabe von Anmeldeinformationen auf den JMX RMI-Port zugegriffen werden kann:

1. Nehmen Sie in der Datei **wrapper.conf**, die sich auf dem Server unter **C:\hp\UCMDB\UCMDBServer\bin** befindet, die folgenden Einstellungen vor:

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

   Diese Einstellung bewirkt, dass die JMX-Konsole zur Authentifizierung auffordert.

   - **Für die JMX-Konsole der Data Flow Probe** müssen die folgenden Schritte ausgeführt werden:

     Nehmen Sie in den Dateien **WrapperGateway.conf** und **WrapperManager.conf**, die sich unter **C:\hp\UCMDB\DataFlowProbe\bin** befinden, die folgenden Einstellungen vor:

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

2. Benennen Sie die Datei **jmxremote.password.template** (unter

C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management) in **jmxremote.password** um.

> **Hinweis:** Für die JMX-Konsole der Data Flow Probe befindet sich diese Datei an folgendem Speicherort: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. Fügen Sie in **jmxremote.password** Kennwörter für die Rollen **monitorRole** und **controlRole** hinzu.

   Beispiel:

   monitorRole QED

   controlRole R&D

   In diesem Beispiel würde **monitorRole** das Kennwort **QED** und **controlRole** das Kennwort **R&D** zugewiesen.

   > **Hinweis:** Vergewissern Sie sich, dass nur der Besitzer Lese- und Schreibzugriff auf **jmxremote.password** hat, da die Datei die Kennwörter als Klartext enthält. Der Dateibesitzer muss mit dem Benutzer identisch sein, unter dessen Namen der UCMDB-Server ausgeführt wird.

4. Weisen Sie in der Datei **jmxremote.access** (unter **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) Zugriffsberechtigungen für die Rollen **monitorRole** und **controlRole** zu.

   Beispiel:

   monitorRole readonly

   controlRole readwrite

   In diesem Beispiel würde der Rolle **monitorRole** schreibgeschützter Zugriff und der Rolle **controlRole** Lese-/Schreibzugriff zugewiesen.

   > **Hinweis:** Für die JMX-Konsole der Data Flow Probe befindet sich diese Datei an folgendem Speicherort: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Sichern Sie die Dateien wie folgt:

   - **Nur für Windows:** Führen Sie zum Sichern der Dateien die folgenden Befehle von der Befehlszeile aus:

     cacls jmxremote.password /P <Benutzername>:F

     cacls jmxremote.access /P <Benutzername>:R

     Dabei steht **<Benutzername>** für den Namen des Dateibesitzers, der in den Eigenschaften beider Dateien angezeigt wird. Öffnen Sie die Eigenschaften dieser Dateien und vergewissern Sie sich, dass sie korrekt sind und nur einen Besitzer haben.

   - **Für Solaris- und Linux-Betriebssysteme:** Legen Sie die Dateiberechtigungen für die Kennwortdatei fest, indem Sie Folgendes ausführen:

     chmod 600 jmxremote.password

6. **Für Service Pack-Upgrades, Servermigrationen und Notfallwiederherstellungen:** Ändern Sie das Eigentum der Datei **jmxremote.access** (unter **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) in den Namen des Betriebssystembenutzers, der das Upgrade bzw. die Migrationsinstallation ausführt.

   Hinweis: Für die JMX-Konsole der Data Flow Probe befindet sich diese Datei an folgendem Speicherort: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

Ändern des Systembenutzernamens oder Kennworts für die JMX-Konsole

Die JMX-Konsole verwendet Systembenutzer, d. h. kundenübergreifende Benutzer in einer Mehrkundenumgebung. Sie können sich an der JMX-Konsole mit einem beliebigen Systembenutzernamen anmelden. Die Standardwerte für Benutzername und Kennwort lauten **sysadmin**/**sysadmin**.

Das Kennwort ändern Sie entweder über die JMX-Konsole oder über das Serververwaltungs-Tool.

So ändern Sie die Standardeinstellung für den Systembenutzernamen oder das Kennwort über die JMX-Konsole:

1. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://localhost.<Domänenname>:8080/jmx-console**.
2. Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole an. Standardmäßig lauten diese wie folgt:
   - Anmeldename = **sysadmin**
   - Kennwort = **sysadmin**
3. Suchen Sie **UCMDB:service=Authorization Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
4. Suchen Sie den Vorgang **resetPassword**.
   - Geben Sie im Feld **userName** den Namen **sysadmin** ein.
   - Geben Sie im Feld **password** ein neues Kennwort ein.
5. Klicken Sie auf **Invoke**, um die Änderung zu speichern.

So ändern Sie die Standardeinstellung für den Systembenutzernamen oder das Kennwort über das Serververwaltungs-Tool:

1. **Für Windows:** Führen Sie die folgende Datei aus: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   Für Linux: Führen Sie **server_management.sh** im folgenden Ordner aus: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Melden Sie sich im Tool mit den Anmeldeinformationen für die Authentifizierung an: **sysadmin**/**sysadmin**.
3. Klicken Sie auf den Link **Benutzer**.

4. Wählen Sie den Systembenutzer aus und klicken Sie auf **Kennwort für angemeldeten Benutzer ändern**.
5. Geben Sie das alte und das neue Kennwort ein und klicken Sie auf **OK**.

Ändern des HP Universal CMDB Server-Servicebenutzers

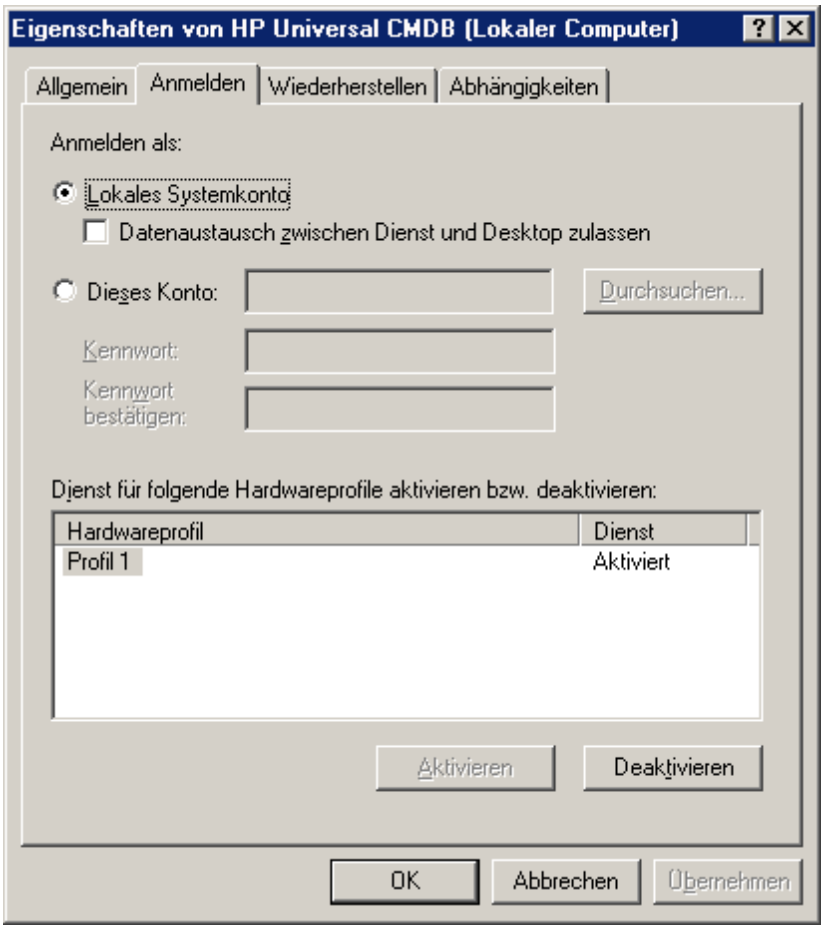
Auf einer Windows-Plattform wird der HP Universal CMDB-Service für die Ausführung aller HP Universal CMDB-Dienste und -Prozesse installiert, wenn Sie das Dienstprogramm für die Server- und Datenbankkonfiguration ausführen. Dieser Service wird standardmäßig unter dem Benutzer **local system** ausgeführt. Sie müssen jedoch möglicherweise einen anderen Benutzer für die Ausführung des Services zuweisen (z. B. wenn Sie NTLM-Authentifizierung verwenden).

Der Benutzer, den Sie für die Ausführung des Services zuweisen, muss über die folgenden Berechtigungen verfügen:

- Ausreichende Datenbankberechtigungen (wie vom Datenbankadministrator definiert)
- Ausreichende Netzwerkberechtigungen
- Administratorberechtigungen auf dem lokalen Server

So ändern Sie den Servicebenutzer:

1. Deaktivieren Sie HP Universal CMDB über das Startmenü (**Start > Alle Programme > HP UCMDB > HP Universal CMDB Server anhalten**) oder indem Sie den HP Universal CMDB Server-Service anhalten. Weitere Informationen finden Sie unter "Starten und Anhalten des HP Universal CMDB Server-Services" im HP Universal CMDB – Bereitstellungshandbuch.
2. Doppelklicken Sie im Windows-Dialogfeld **Dienste** auf **UCMDB_Server**. Das Dialogfeld **Eigenschaften von UCMDB_Server (Lokaler Computer)** wird geöffnet.
3. Klicken Sie auf die Registerkarte **Anmelden**.



4. Aktivieren Sie **Dieses Konto** und wählen Sie über **Durchsuchen** einen anderen Benutzer aus der Liste mit den gültigen Benutzern auf diesem Computer aus.
5. Geben Sie das Windows-Kennwort des ausgewählten Benutzers ein und bestätigen Sie dieses Kennwort.
6. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern, und klicken Sie auf **OK**, um das Dialogfeld zu schließen.
7. Aktivieren Sie HP Universal CMDB über das Startmenü (**Start > Alle Programme > HP UCMDB > HP Universal CMDB Server starten**) oder indem Sie den HP Universal CMDB Server-Service starten. Weitere Informationen finden Sie unter"Starten und Anhalten des HP Universal CMDB Server-Services" im HP Universal CMDB – Bereitstellungshandbuch.

Verschlüsseln des Datenbankkennworts für Configuration Manager

Das CM-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 "Parameter für die Verschlüsselung des Datenbankkennworts von Configuration Manager" oben

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, das die Datei **<Configuration Manager-Installationsverzeichnis>\security\encrypt_repository** und den Verschlüsselungsschlüssel generiert.
3. Führen Sie das Dienstprogramm **bin\encrypt-password.bat** 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.

Parameter für die Verschlüsselung des Datenbankkennworts von Configuration Manager

In der folgenden Tabelle sind die Parameter aus der Datei **encryption.properties** aufgeführt, die für die Verschlüsselung des CM-Datenbankkennworts verwendet werden. Weitere Informationen zum Verschlüsseln des Datenbankkennworts finden Sie unter "Verschlüsseln des Datenbankkennworts für Configuration Manager" auf der vorherigen Seite.

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.

Parameter	Beschreibung
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
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** gesetzt ist. Für **lw** wird **engineName** verwendet.

Kapitel 2

Aktivieren der SSL-Kommunikation

Dieses Kapitel umfasst folgende Themen:

Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat - UCMDB

In diesem Abschnitt wird erläutert, wie Sie HP Universal CMDB für die Unterstützung der Kommunikation über den Secure Sockets Layer-Kanal (SSL) konfigurieren.

HP Universal CMDB verwendet Jetty 6.1 als Standard-Webserver.

1. **Voraussetzungen**

   a. Bevor Sie mit der folgenden Prozedur beginnen, löschen Sie die alte Datei **server.keystore** unter **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

   b. Legen Sie den HP Universal CMDB-Key Store (JKS-Typ) im Ordner **C:\hp\UCMDB\UCMDBServer\conf\security** ab.

2. **Erstellen eines Serverschlüsselspeichers**

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

   - Führen Sie aus dem Verzeichnis **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** den folgenden Befehl aus:

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

     Das Konsolendialogfeld wird geöffnet.

   - Geben Sie das Schlüsselspeicherkennwort ein. Wenn das Kennwort geändert wurde, führen Sie den JMX-Vorgang **changeKeystorePassword** unter **UCMDB:service=Security Services** aus. Wenn das Kennwort nicht geändert wurde, verwenden Sie den Standardwert **hppass**.

   - Beantworten Sie die Frage nach Ihrem Vor- und Nachnamen. Geben Sie den HP Universal CMDB-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-Key Store namens **server.keystore** mit einem Serverzertifikat mit der Bezeichnung **hpcert** erstellt.

   b. Exportieren Sie das selbstsignierte Zertifikat in eine Datei:

   Führen Sie aus dem Verzeichnis **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** den folgenden Befehl aus:

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

3. **Platzieren des Zertifikats im vertrauenswürdigen Speicher des Clients**

   Nach dem Erstellen von **server.keystore** und dem Exportieren des Serverzertifikats speichern Sie dieses Zertifikat für jeden Client, der mit HP Universal CMDB über SSL mithilfe dieses selbstsignierten Zertifikats kommunizieren muss, im vertrauenswürdigen Speicher des Clients.

   Hinweis: In **server.keystore** kann nur ein Serverzertifikat vorhanden sein.

4. **Deaktivieren von HTTP-Port 8080**

   Weitere Informationen finden Sie unter "Aktivieren oder Deaktivieren der HTTP/HTTPS-Ports" auf Seite 29.

   Hinweis: Prüfen Sie, ob die HTTPS-Kommunikation funktioniert, bevor Sie den HTTP-Port schließen.

5. **Neustarten des Servers**

6. **Anzeigen von HP Universal CMDB**

Um zu prüfen, ob der UCMDB-Server sicher ist, geben Sie den folgenden URL in den Webbrowser ein: **https://<Name oder IP-Adresse des UCMDB-Servers>:8443/ucmdb-ui**.

Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat - Configuration Manager

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 7.0.19 als Applikationsserver.

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

1. ## Voraussetzungen

   Bevor Sie mit der folgenden Prozedur beginnen, löschen Sie die alte Datei **tomcat.keystore**, die sich eventuell im Ordner **<Configuration Manager-Installationsverzeichnis>\java\windows\x86_64\lib\security** bzw. im Ordner **<Configuration Manager-Installationsverzeichnis>\java\linux\x86_64\lib\security** (je nach Betriebssystem) befindet.

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 auf Ihrem Computer in Internet Explorer zu den Trust Stores des

Clients hinzu (**Extras > Internetoptionen > Inhalte > Zertifikate**). Falls Sie dies nicht tun, werden Sie dazu aufgefordert, wenn Sie Configuration Manager das erste Mal verwenden.

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

4. **Ändern der Datei "server.xml"**

   Öffnen Sie die Datei **server.xml**, die sich unter **<Configuration Manager-Installationsverzeichnis>\servers\server-0\conf** befindet. Suchen Sie nach der Einstellung, die mit

   ```
   Connector port="8143"
   ```

   beginnt (in den Kommentaren). Aktivieren Sie das Skript, indem Sie das Kommentarzeichen entfernen und die folgenden beiden Attribute zum HTTPS-Connector hinzufügen:

   ```
   keystoreFile="<Speicherort der Datei 'tomcat.keystore'>"
   ```
   (siehe Schritt 2)
   ```
   keystorePass="<Kennwort>"
   ```

   Kommentieren Sie folgende Zeile aus:

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

   Hinweis: Sie dürfen den HTTP-Verbindungsport nicht blockieren. Wenn Sie die HTTP-Kommunikation blockieren möchten, können Sie zu diesem Zweck eine Firewall verwenden.

5. **Neustarten des Servers**

   Starten Sie den Configuration Manager-Server neu.

6. **Verifizieren der Serversicherheit**

   Um zu verifizieren, dass der Configuration Manager-Server sicher ist, geben Sie den folgenden URL in den Webbrowser ein: **https://<Name oder IP-Adresse des Configuration Manager-Servers>:8143/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 - UCMDB

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 den alten Key Store des Servers unter **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. **Erstellen eines Serverschlüsselspeichers**

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

   b. Exportieren Sie das Zertifikat mithilfe von Microsoft Management Console (**mmc.exe**) 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: **C:\hp\UCMDB\UCMDBServer\conf\security**.

   d. Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis in **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**.

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

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

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

   e. Geben Sie das Kennwort des Ziel-Key Store ein. Dieses Kennwort muss mit dem übereinstimmen, das zuvor mit der JMX-Methode **changeKeystorePassword** unter Security Services definiert wurde. Wenn das Kennwort nicht geändert wurde, verwenden Sie den Standardwert **hppass**.

   f. Deaktivieren Sie nach dem Erzeugen des Zertifikats den HTTP-Port 8080. Weitere Informationen finden Sie unter "Aktivieren oder Deaktivieren der HTTP/HTTPS-Ports" auf Seite 29.

   g. Wenn Sie ein anderes Kennwort als **hppass** oder das für die PFX-Datei definierte Kennwort verwendet haben, führen Sie die JMX-Methode **changeKeystorePassword** aus und stellen Sie sicher, dass der Schlüssel dasselbe Kennwort aufweist.

   > **Hinweis:** Prüfen Sie, ob die HTTPS-Kommunikation funktioniert, bevor Sie den HTTP-Port schließen.

3. **Neustarten des Servers**

4. **Verifizieren der Serversicherheit**

   Um zu prüfen, ob der UCMDB Server sicher ist, geben Sie den folgenden URL in den Webbrowser ein: **https://<Name oder IP-Adresse des UCMDB-Servers>:8443/ucmdb-ui**.

Achtung: In **server.keystore** kann nur ein Serverzertifikat vorhanden sein.

Aktivieren von SSL auf dem Servercomputer mit einem Zertifikat von einer Zertifizierungsstelle - Configuration Manager

Um ein von einer Zertifizierungsstelle ausgegebenes Zertifikat für Configuration Manager zu verwenden, muss der Key Store 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, löschen Sie die alte Datei **tomcat.keystore**, die sich eventuell im Ordner **<Configuration Manager-Installationsverzeichnis>\java\windows\x86_64\lib\security** bzw. im Ordner **<Configuration Manager-Installationsverzeichnis>\java\linux\x86_64\lib\security** (je nach Betriebssystem) befindet.

2. ## Erstellen eines Serverschlüsselspeichers

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

   b. Exportieren Sie das Zertifikat mithilfe von Microsoft Management Console (**mmc.exe**) 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.

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

   c. Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis in **<Configuration Manager-Installationsverzeichnis>\java\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, das Sie beim Erstellen der PFX-Datei in Schritt b angegeben haben.

3. ## Ändern der Datei "server.xml"

   Öffnen Sie die Datei **server.xml**, die sich unter **<Configuration Manager-**

Installationsverzeichnis>\servers\server-0\conf befindet. Suchen Sie nach der Einstellung, die mit

```
Connector port="8143"
```

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" />
```

Hinweis: Sie dürfen den HTTP-Verbindungsport nicht blockieren. Wenn Sie die HTTP-Kommunikation blockieren möchten, können Sie zu diesem Zweck eine Firewall verwenden.

4. ### Neustarten des Servers

   Starten Sie den Configuration Manager-Server neu.

5. ### Verifizieren der Serversicherheit

   Um sicherzustellen, dass der Configuration Manager-Server sicher ist, geben Sie die folgende URL in den Webbrowser ein: **https://<Name oder IP-Adresse des Configuration Manager-Servers>:8143/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 auf Clientcomputern - UCMDB

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

Wenn der Webbrowser der Zertifizierungsstelle nicht vertraut, müssen Sie entweder den gesamten Trustpfad zum Zertifikat importieren oder das von HP Universal CMDB verwendete Zertifikat explizit in den Trust Store des Browsers importieren.

Das folgende Beispiel zeigt, wie Sie das selbstsignierte Zertifikat **hpcert** in den Windows-Trust Store importieren, damit es von Internet Explorer verwendet werden kann.

So importieren Sie ein Zertifikat in den Windows-Trust Store:

1. Suchen Sie das Zertifikat **hpcert** und benennen Sie es in **hpcert.cer** um.

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

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

3. Befolgen Sie die Anweisungen für das Aktivieren von Trust, indem Sie das Zertifikat mit dem Assistenten zum Importieren von Zertifikaten installieren.

Hinweis: Eine andere Methode zum Importieren des vom UCMDB Server ausgegebenen Zertifikats in den Webbrowser besteht darin, dass Sie sich in UCMDB anmelden und das Zertifikat installieren, wenn die Warnung vor einem nicht vertrauenswürdigen Zertifikat angezeigt wird.

Aktivieren von SSL mit einem Clientzertifikat - Configuration Manager

Wenn das vom Configuration Manager-Webserver verwendete Zertifikat von einer bekannten Zertifizierungsstelle ausgegeben wird, kann Ihr Webbrowser das Zertifikat höchstwahrscheinlich validieren, ohne dass 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\bin\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 unter "Ändern der Datei "server.xml"" auf Seite 23 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. Überprüfen Sie die Serversicherheit wie unter "Verifizieren der Serversicherheit" auf Seite 24 beschrieben.

Aktivieren von SSL auf dem Client-SDK

Sie können HTTPS-Übertragung zwischen dem Client-SDK und dem Server-SDK nutzen:

1. Suchen Sie auf dem Clientcomputer im Produkt, in dem das Client-SDK integriert ist, die Übertragungseinstellung und prüfen Sie, dass HTTPS konfiguriert ist und nicht HTTP.
2. Laden Sie das Zertifikat der Zertifizierungsstelle bzw. das selbstsignierte öffentliche Zertifikat auf den Clientcomputer herunter und importieren Sie es in den Trust Store **cacerts** der JRE, die die Verbindung zum Server herstellt.

   Verwenden Sie den folgenden Befehl:

   ```
   Keytool -import -alias <Name der Zertifizierungsstelle> -
   trustcacerts -file <Pfad des öffentlichen Serverzertifikats> -
   keystore <Pfad zum Client-JRE-Trust Store cacerts (z. B.
   x:\Programme\java\jre\lib\security\cacerts)>
   ```

Aktivieren der gegenseitigen Zertifikatsauthentifizierung für SDK

Dieser Modus verwendet SSL und ermöglicht sowohl die Serverauthentifizierung durch die UCMDB als auch die Clientauthentifizierung durch den UCMDB-API-Client. Sowohl der Server als auch der UCMDB-API-Client senden ihre Zertifikate zur Authentifizierung an die andere Entität.

Hinweis: Die folgende Methode zum Aktivieren von SSL auf dem SDK mit gegenseitiger Authentifizierung ist die sicherste Methode und daher der empfohlene Kommunikationsmodus.

1. Härten Sie den UCMDB-API-Client-Connector in UCMDB:

   a. Rufen Sie die UCMDB-JMX-Konsole auf: Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://<Name oder IP-Adresse des UCMDB-Computers>:8080/jmx-console**. Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden (die Standardeinstellung lautet **sysadmin/sysadmin**).

   b. Suchen Sie **UCMDB:service=Ports Management Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.

   c. Suchen Sie den Vorgang **PortsDetails** und klicken Sie auf **Invoke**. Achten Sie auf die Portnummer für HTTPS mit Clientauthentifizierung. Die Standardeinstellung lautet 8444 und sollte aktiviert sein.

   d. Kehren Sie zur Seite **Operations** zurück.

   e. Um den UCMDB-API-Connector dem Modus mit gegenseitiger Authentifizierung

zuzuordnen, rufen Sie die Methode **mapComponentToConnectors** mit den folgenden Parametern auf:

- **componentName**: ucmdb-api
- **isHTTPSWithClientAuth**: true
- Alle anderen Kennzeichen: false

Die folgende Meldung wird angezeigt:

```
Operation succeeded. Component ucmdb-api is now mapped to:
HTTPS_CLIENT_AUTH ports.
```

f. Kehren Sie zur Seite **Operations** zurück.

2. Stellen Sie sicher, dass die JRE, die den UCMDB-API-Client ausführt, über einen Key Store mit einem Clientzertifikat verfügt.
3. Exportieren Sie das UCMDB-API-Clientzertifikat aus dem Key Store.
4. Importieren Sie das exportierte UCMDB-API-Clientzertifikat in den UCMDB Server-Trust Store.
   a. Kopieren Sie auf dem UCMDB-Computer die erstellte Datei mit dem UCMDB-API-Clientzertifikat in das folgende UCMDB-Verzeichnis:

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

   b. Führen Sie folgenden Befehl aus:

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

   c. Geben Sie das Kennwort für den UCMDB Server-Trust Store ein (Standardeinstellung **hppass**).

   d. Geben Sie auf die Frage, ob Sie diesem Zertifikat vertrauen, **y** ein und drücken Sie dann die **Eingabetaste**.

   e. Stellen Sie sicher, dass die Ausgabe **Certificate was added to keystore** lautet.
5. Exportieren Sie das UCMDB-Serverzertifikat aus dem Key Store des Servers.
   a. Führen Sie auf dem UCMDB-Computer den folgenden Befehl aus:

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

   b. Geben Sie das Kennwort für den UCMDB Server-Trust Store ein (Standardeinstellung **hppass**).

   c. Prüfen Sie, ob das Zertifikat im folgenden Verzeichnis erstellt wurde:

      C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
6. Importieren Sie das exportierte UCMDB-Zertifikat in die JRE des UCMDB-API-Client-Trust Store.
7. Starten Sie den UCMDB Server und den UCMDB-API-Client neu.

8. Verwenden Sie den folgenden Code, um eine Verbindung vom UCMDB-API-Client zum UCMDB-API-Server herzustellen:

```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https", <EIN_HOSTNAME>,
<PORTNUMMER_FÜR_HTTPS_MIT_CLIENTAUTHENTIFIZIERUNG
(Standardeinstellung:8444>));
UcmdbService ucmdbService = provider.connect
(provider.createCertificateCredentials(<Client-Key Store, z. B.:
"c:\\client.keystore">, <Key Store-Kennwort>),
provider.createClientContext(<Client-ID>));
```

Ändern der Kennwörter für den Server-Key Store

Nach dem Installieren des Servers ist der HTTPS-Port offen und der Speicher ist mit einem schwachen Kennwort (Standardeinstellung **hppass**) geschützt. Wenn Sie ausschließlich mit SSL arbeiten möchten, müssen Sie das Kennwort ändern.

In der folgenden Prozedur wird erklärt, wie Sie nur das Kennwort für den Server-Key Store ändern. Sie sollten jedoch mit derselben Prozedur auch das Kennwort für den Server-Trust Store ändern.

Hinweis: Sie müssen jeden Schritt dieser Prozedur durchführen.

1. Starten Sie den UCMDB Server.
2. Nehmen Sie die Kennwortänderung in der JMX-Konsole vor.
   a. Starten Sie den Webbrowser und geben Sie die Serveradresse wie folgt ein: **http://<UCMDB Server-Hostname oder -IP>:8080/jmx-console**.

      Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

   b. Klicken Sie unter **UCMDB** auf **UCMDB:service=Security Services**, um die Seite **Operations** zu öffnen.

   c. Suchen Sie den Vorgang **changeKeystorePassword** und führen Sie ihn aus.

      Dieses Feld darf nicht leer sein und muss mindestens sechs Zeichen enthalten. Das Kennwort wird nur in der Datenbank geändert.
3. Halten Sie den UCMDB Server an.
4. Führen Sie Befehle aus.

   Führen Sie aus dem Verzeichnis **C:\hp\UCMDB\UCMBServer\bin\jre\bin** die folgenden Befehle aus:

   a. Ändern Sie das Kennwort des Speichers:

      keytool -storepasswd -new <neues Key Store-Kennwort> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <derzeitiges Key Store-Kennwort>

b. Durch den folgenden Befehl wird der interne Schlüssel des Key Store angezeigt. Der erste Parameter ist der Alias. Speichern Sie diesen Parameter für den nächsten Befehl:

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

c. Ändern Sie das Kennwort für den Schlüssel (falls der Speicher nicht leer ist):

keytool -keypasswd -alias <Alias> -keypass <derzeitiges Kennwort> -new <neues Kennwort> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

d. Geben Sie das neue Kennwort ein.

5. Starten Sie den UCMDB Server.
6. Wiederholen Sie die Prozedur für den Server-Trust Store.

Aktivieren oder Deaktivieren der HTTP/HTTPS-Ports

Sie können die HTTP- und HTTPS-Ports über die Benutzeroberfläche oder über die JMX-Konsole aktivieren oder deaktivieren.

So aktivieren oder deaktivieren Sie die HTTP/HTTPS-Ports über die Benutzeroberfläche:

1. Melden Sie sich in HP Universal CMDB an.
2. Wählen Sie **Verwaltung > Infrastruktureinstellungen** aus.
3. Geben Sie im Feld **Filter** (nach Name) entweder **http** oder **https** ein, um die HTTP-Einstellungen anzuzeigen.
   - **HTTP(S)-Verbindungen aktivieren**. **True**: Der Port ist aktiviert. **False**: Der Port ist deaktiviert.
4. Starten Sie den Server neu, damit die Änderung angewendet wird.

> **Achtung:** Der HTTPS-Port ist standardmäßig offen; wird der Port geschlossen, funktioniert **Server_Management.bat** nicht mehr.

So aktivieren oder deaktivieren Sie die HTTP/HTTPS-Ports über die JMX-Konsole:

1. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: http://localhost.<Domänenname>:8080/jmx-console.
2. Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole an. Standardmäßig lauten diese wie folgt:
   - Anmeldename = **sysadmin**
   - Kennwort = **sysadmin**
3. Suchen Sie **UCMDB:service=Ports Management Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
4. Zum Aktivieren oder Deaktivieren des HTTP-Ports suchen Sie den Vorgang **HTTPSetEnable** und legen den Wert fest.

- **True:** Der Port ist aktiviert.
- **False:** Der Port ist deaktiviert.

5. Zum Aktivieren oder Deaktivieren des HTTPS-Ports suchen Sie den Vorgang **HTTPSSetEnable** und legen den Wert fest.
   - **True:** Der Port ist aktiviert.
   - **False:** Der Port ist deaktiviert.
6. Zum Aktivieren oder Deaktivieren des HTTPS-Ports mit Clientauthentifizierung suchen Sie den Vorgang **HTTPSClientAuthSetEnable** und legen den Wert fest.
   - **True:** Der Port ist aktiviert.
   - **False:** Der Port ist deaktiviert.

Zuordnen der UCMDB-Webkomponenten zu Ports

Sie können die Zuordnung jeder UCMDB-Komponente zu den verfügbaren Ports über die JMX-Konsole konfigurieren.

So zeigen Sie die aktuellen Konfigurationen der Komponenten an:

1. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://localhost.<Domänenname>:8080/jmx-console**.
2. Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole an. Standardmäßig lauten diese wie folgt:

   Anmeldename = **sysadmin**

   Kennwort = **sysadmin**
3. Suchen Sie **UCMDB:service=Ports Management Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
4. Suchen Sie den Vorgang **ComponentsConfigurations** und klicken Sie auf **Invoke**.
5. Für jede Komponente werden die gültigen Ports und die derzeit zugeordneten Ports angezeigt.

So ordnen Sie die Komponenten zu:

1. Suchen Sie **UCMDB:service=Ports Management Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
2. Suchen Sie die Methode **mapComponentToConnectors**.
3. Geben Sie im Feld für den Wert einen Komponentennamen ein. Wählen Sie für jeden Port **True** oder **False** aus, abhängig von Ihrer Auswahl. Klicken Sie auf **Invoke**. Die ausgewählte Komponente wird den ausgewählten Ports zugeordnet. Sie können die Komponentennamen bestimmen, indem Sie die Methode **serverComponentsNames** aufrufen.
4. Wiederholen Sie den Prozess für jede relevante Komponente.

Hinweis:

- Jede Komponente muss mindestens einem Port zugeordnet sein. Wenn Sie eine Komponente keinem Port zuordnen, wird sie standardmäßig dem HTTP-Port zugeordnet.
- Wenn Sie eine Komponente sowohl dem HTTPS-Port als auch dem HTTPS-Port mit Clientauthentifizierung zuordnen, wird nur die Option für die Clientauthentifizierung zugeordnet (die andere Option ist in diesem Fall redundant).

Sie können auch den Wert ändern, der den einzelnen Ports zugewiesen wurde.

So legen Sie Werte für die Ports fest:

1. Suchen Sie **UCMDB:service=Ports Management Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
2. Um einen Wert für den HTTP-Port festzulegen, suchen Sie die Methode **HTTPSetPort** und geben im Feld **Value** einen Wert ein. Klicken Sie auf **Invoke**.
3. Um einen Wert für den HTTPS-Port festzulegen, suchen Sie die Methode **HTTPSSetPort** und geben im Feld **Value** einen Wert ein. Klicken Sie auf **Invoke**.
4. Um einen Wert für den HTTPS-Port mit Clientauthentifizierung festzulegen, suchen Sie die Methode **HTTPSClientAuthSetPort** und geben im Feld **Value** einen Wert ein. Klicken Sie auf **Invoke**.

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.

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

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

2. Kopieren Sie die Zertifikatsdatei in einen temporären Speicherort auf dem lokalen Configuration Manager-Computer.
3. Führen Sie eine neue Installation von Configuration Manager durch oder rekonfigurieren Sie eine vorhandene Installation. Weitere Anweisungen finden Sie in den entsprechenden Abschnitten im interaktiven *HP Universal CMDB – Bereitstellungshandbuch*.

   Setzen Sie das Protokoll im UCMDB-Konfigurationsbildschirm auf **HTTPS** und wählen Sie die Zertifikatsdatei aus, die Sie in Schritt 2 kopiert haben.

Um Configuration Manager für die Zusammenarbeit mit anderen Produkten (z. B. Load Balancer) und SSL zu konfigurieren, importieren Sie das Sicherheitszertifikat des Produkts in den Trust Store von Configuration Manager (Standard-JRE-Trust Store), indem Sie den folgenden Befehl ausführen:

```
<CM JAVA-STARTVERZEICHNIS>\bin\keytool -import -trustcacerts -alias
<Alias>
-keystore <CM JAVA-STARTVERZEICHNIS>\lib\security\cacerts -storepass
changeit
-file <Zertifikatsdatei>
```

Aktivieren des UCMDB KPI-Adapters für die Verwendung mit SSL

Sie können die Informationen des UCMDB KPI-Adapters konfigurieren, die unter Verwendung von Secure Sockets Layer (SSL) gesendet werden sollen.

1. Exportieren Sie das Configuration Manager-Zertifikat:

   ```
   <CM JAVA-STARTVERZEICHNIS>\bin\keytool -export -alias tomcat -
   keystore
   <CM JAVA-STARTVERZEICHNIS>\lib\security\tomcat.keystore -storepass
   <Key Store-Kennwort> -file <Name der Zertifikatsdatei>
   ```

2. Importieren Sie das von Configuration Manager exportierte Zertifikat in den Trust Store von UCMDB. Gehen Sie dazu wie folgt vor:

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

3. Importieren Sie das von Configuration Manager exportierte Zertifikat in den Trust Store der Probe. Gehen Sie dazu wie folgt vor:

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

      ```
      <Data Flow Probe-Verzeichnis>\bin\jre\bin\keytool.exe -import -v
      -keystore <Data Flow Probe-
      Verzeichnis>\conf\security\MAMTrustStoreExp.jks -file
      <Zertifikatdatei> -alias tomcat
      ```

   b. Geben Sie das Key Store-Kennwort ein: logomania.

   c. Geben Sie auf die Frage, ob Sie diesem Zertifikat vertrauen, **y** ein und drücken Sie dann die **Eingabetaste**.

      Die folgende Meldung wird angezeigt:

      Das Zertifikat wurde zum Key Store hinzugefügt.

      Weitere Informationen zum Härten der Data Flow Probe finden Sie unter "Härten der Data Flow Probe" auf Seite 65.

4. Starten Sie UCMDB, die Data Flow Probe und Configuration Manager neu.

Konfigurieren der SSL-Unterstützung für den UCMDB-Browser

Hinweis: Die hier gegebenen Anweisungen gelten für Version 1.7 des UCMDB-Browsers. Wenn Sie eine neuere Version des UCMDB-Browsers verwenden, die unabhängig von der übrigen UCMDB-Produktsuite aktualisiert wurde, lesen Sie den Abschnitt über das Konfigurieren der SSL-Unterstützung im *UCMDB Browser Installation and Configuration Guide* für die Version.

So installieren und konfigurieren Sie SSL-Unterstützung bei Tomcat:

1. Erstellen Sie eine Key Store-Datei, um den privaten Schlüssel und das selbstsignierte Zertifikat des Servers zu speichern. Führen Sie dazu einen der folgenden Befehle aus:
   - Für Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - Für Unix: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   Verwenden Sie für beide Befehle den Kennwortwert **changeit** (für alle anderen Felder, die im Konsolendialogfeld angezeigt werden, können Sie einen beliebigen Wert verwenden).
2. Entfernen Sie in der Datei **$CATALINA_BASE/conf/server.xml** die Kommentarzeichen vom Eintrag **SSL HTTP/1.1 Connector**, wobei **$CATALINA_BASE** dem Tomcat-Installationsverzeichnis entspricht.

   Hinweis: Eine vollständige Beschreibung zur Konfiguration von **server.xml** für die Verwendung von SSL finden Sie auf der offiziellen Tomcat-Website von Apache: http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html
3. Starten Sie den Tomcat-Server neu.

So verwenden Sie das HTTPS-Protokoll für die Verbindung zum UCMDB-Server:

1. Öffnen Sie die Datei **ucmdb_browser_config.xml** und weisen Sie dem Tag **<protocol>** den Wert **https** und dem Tag **<port>** den HTTPS-Portwert des UCMDB-Servers (standardmäßig 8443) zu.
2. Laden Sie das öffentliche Zertifikat des UCMDB-Servers auf den Computer herunter, auf dem der UCMDB-Browser installiert ist (wenn Sie SSL auf dem UCMDB-Server verwenden, kann Ihnen der UCMDB-Administrator das Zertifikat zur Verfügung stellen) und importieren Sie es in den Trust Store **cacerts** der JRE, die die Verbindung zum Server herstellt. Führen Sie dazu den folgenden Befehl aus:

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

   Dabei steht **<Zertifikatsdatei des UCMDB-Servers>** für den vollständigen Pfad zum öffentlichen Zertifikat des UCMDB-Servers.
3. Starten Sie den Tomcat-Server neu.

Kapitel 3

Verwenden eines Reverse-Proxy

In diesem Abschnitt werden die Sicherheitsauswirkungen von Reverse-Proxys beschrieben und Sie finden Anweisungen für die Verwendung eines Reverse-Proxy mit HP Universal CMDB und Configuration Manager. Es werden nur die Sicherheitsaspekte eines Reverse-Proxy besprochen, aber keine anderen Themen wie Caching und Load Balancing.

Dieses Kapitel umfasst folgende Themen:

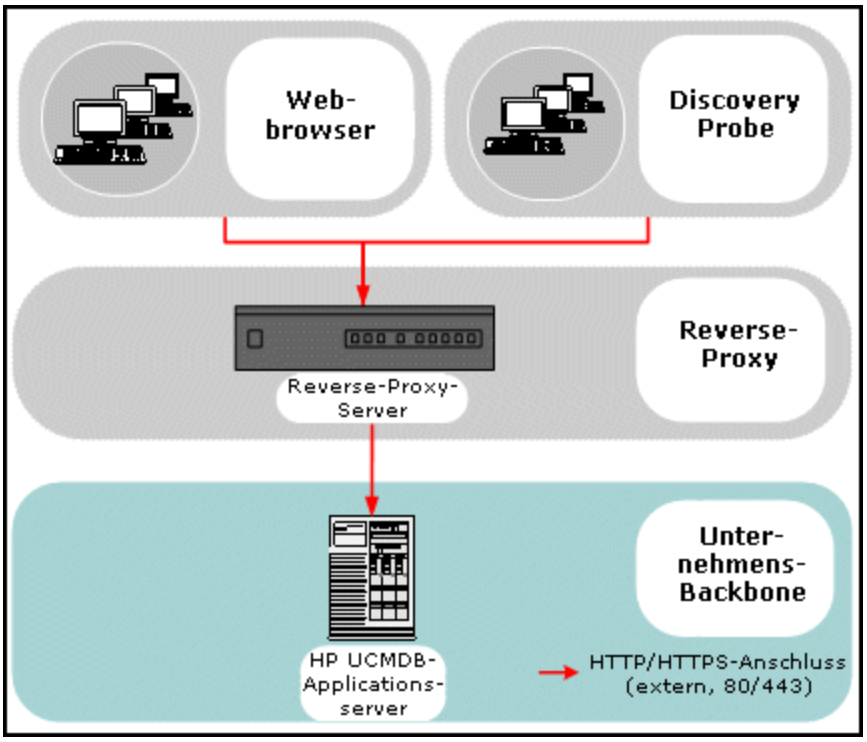
Reverse-Proxy – Übersicht

Bei einem Reverse-Proxy handelt es sich um einen Vermittlungsserver, der sich zwischen dem Clientcomputer und den Webservern befindet. Für den Clientcomputer erscheint der Reverse-Proxy als Standard-Webserver, der die Anfragen des Clientcomputers über das HTTP-Protokoll beantwortet.

Der Clientcomputer sendet normale Anfragen für Webinhalte und verwendet dabei den Namen des Reverse-Proxy statt dem Namen eines Webservers. Der Reverse-Proxy sendet die Anfrage an einen der Webserver. Obwohl die Antwort vom Reverse-Proxy an den Clientcomputer zurückgesendet wird, scheint es auf dem Clientcomputer so, als würde die Antwort vom Webserver gesendet.

Es ist möglich, mehrere Reverse-Proxys mit verschiedenen URLs einzurichten, die die gleiche UCMDB/CM-Instanz repräsentieren. Alternativ kann ein einzelner Reverse-Proxy-Server verwendet werden, um auf mehrere UCMDB/CM-Server zuzugreifen, indem unterschiedliche Stammkontexte für jeden UCMDB/CM-Server festgelegt werden.

HP Universal CMDB und Configuration Manager unterstützen einen Reverse-Proxy in einer DMZ-Architektur. Der Reverse-Proxy ist ein HTTP-Vermittler zwischen der Data Flow Probe und dem Webclient und dem HP Universal CMDB/CM-Server.



Hinweis:

- Verschiedene Typen von Reverse-Proxys erfordern eine unterschiedliche Konfigurationssyntax. Ein Beispiel für die Konfiguration eines Apache 2.0.x-Reverse-Proxy finden Sie unter " Beispiel: Apache 2.0.x-Konfiguration " auf Seite 37.
- Sie müssen die Einstellung für den Frontend-URL nur konfigurieren, wenn Sie mit dem Scheduler einen Direkt-Link zu einem Report erstellen.

Sicherheitsaspekte bei der Verwendung eines Reverse-Proxy-Servers

Ein Reverse-Proxy-Server fungiert als „Bastion-Host“. Der Proxy ist so konfiguriert, dass er als einziger Computer direkt von externen Clients adressiert wird und damit das restliche interne Netzwerk abschirmt. Durch die Verwendung eines Reverse-Proxy ist es möglich, den Applikationsserver auf einem separaten Computer im internen Netzwerk unterzubringen.

In diesem Abschnitt wird die Verwendung einer DMZ und eines Reverse-Proxy in einer Back-to-Back-Topologieumgebung besprochen.

Durch die Verwendung eines Reverse-Proxy in einer solchen Umgebung werden insbesondere die folgenden Sicherheitsvorteile erzielt:

- Es erfolgt keine DMZ-Protokollübersetzung. Das eingehende Protokoll und das ausgehende Protokoll sind identisch (nur die Kopfzeile ändert sich).
- Nur HTTP-Zugriff auf den Reverse-Proxy ist erlaubt, sodass die Kommunikation durch Stateful Packet Inspection-Firewalls besser geschützt ist.

- Auf dem Reverse-Proxy kann ein statischer, begrenzter Satz von Weiterleitungsanfragen definiert werden.
- Die meisten Sicherheitsfunktionen von Webservern sind auf dem Reverse-Proxy verfügbar (Authentifizierungsmethoden, Verschlüsselung usw.).
- Der Reverse-Proxy überwacht die IP-Adressen der eigentlichen Server sowie die Architektur des internen Netzwerks.
- Der Reverse-Proxy ist der einzige zugängliche Client des Webservers.
- Diese Konfiguration unterstützt NAT-Firewalls (im Gegensatz zu anderen Lösungen).
- Der Reverse-Proxy erfordert eine minimale Anzahl an offenen Ports in der Firewall.
- Der Reverse-Proxy erzielt im Vergleich zu anderen Bastion-Lösungen eine gute Leistung.

Konfigurieren eines Reverse-Proxy

In diesem Abschnitt wird beschrieben, wie Sie einen Reverse-Proxy konfigurieren.

Konfigurieren eines Reverse-Proxy über die Infrastruktureinstellungen

In der folgenden Prozedur wird erklärt, wie Sie mithilfe der Infrastruktureinstellungen einen Reverse-Proxy konfigurieren. Diese Konfiguration ist nur erforderlich, wenn Sie mit dem Scheduler einen Direkt-Link zu einem Report erstellen.

So konfigurieren Sie einen Reverse-Proxy:

1. Wählen Sie die Kategorie **Verwaltung > Infrastructure Settings Manager > Allgemeine Einstellungen** aus.
2. Ändern Sie die Einstellung **Frontend-URL**. Geben Sie die Adresse ein, z. B. **https://mein_Proxy_Server:443/**.

Hinweis: Nachdem Sie diese Änderung vorgenommen haben, ist es nicht mehr möglich, direkt über einen Client auf den HP Universal CMDB-Server zuzugreifen. Sie können die Reverse-Proxy-Konfiguration jedoch über die JMX-Konsole auf dem Servercomputer ändern. Weitere Informationen finden Sie unten unter "Konfigurieren eines Reverse-Proxy mit der JMX-Konsole".

Konfigurieren eines Reverse-Proxy mit der JMX-Konsole

Sie können über die JMX-Konsole auf dem HP Universal CMDB-Servercomputer Änderungen an der Reverse-Proxy-Konfiguration vornehmen. Diese Konfiguration ist nur erforderlich, wenn Sie mit dem Scheduler einen Direkt-Link zu einem Report erstellen.

So ändern Sie eine Reverse-Proxy-Konfiguration:

1. Starten Sie auf dem HP Universal CMDB Server-Computer den Webbrowser und geben Sie die folgende Adresse ein:

   http://<Computername oder IP-Adresse>.<Domänenname>:8080/jmx-console

   Dabei steht **<Computername oder IP-Adresse>** für den Computer, auf dem HP Universal CMDB installiert ist. Eventuell müssen Sie sich mit dem Benutzernamen und dem Kennwort anmelden.

2. Klicken Sie auf den Link **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

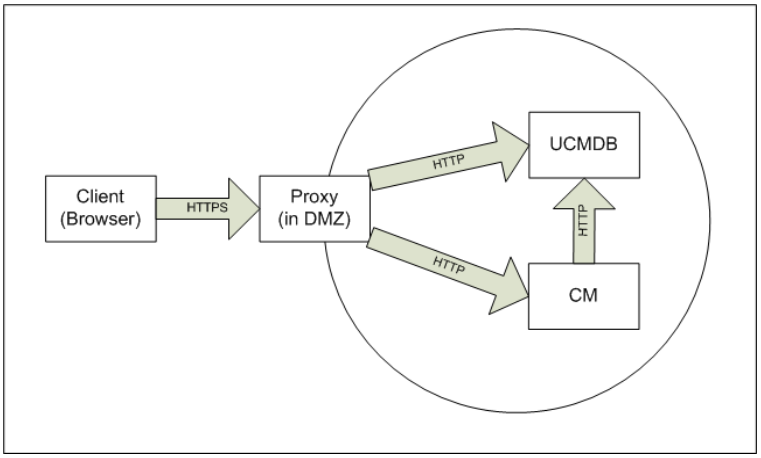
   Geben Sie im Feld **setUseFrontendURLBySettings** den Server-Proxy-URL ein, z. B. `https://mein_Proxy_Server:443/`.

3. Klicken Sie auf **Invoke**.
4. Zum Anzeigen des Werts für diese Einstellung verwenden Sie die Methode **showFrontendURLInSettings**.

Beispiel: Apache 2.0.x-Konfiguration

In diesem Abschnitt wird ein Beispiel für eine Konfigurationsdatei beschrieben, die die Verwendung eines Apache 2.0.x-Reverse-Proxy in einem Fall unterstützt, in dem sowohl Data Flow Proben als auch Applikationsbenutzer eine Verbindung zu HP Universal CMDB herstellen.

Die folgende Grafik verdeutlicht den Konfigurationsprozess für einen Reverse-Proxy für Configuration Manager und UCMDB.



Hinweis:

- In diesem Beispiel lauten der DNS-Name und -Port des HP Universal CMDB-Computers **UCMDB_server**.
- In diesem Beispiel lauten der DNS-Name und -Port des HP Configuration Manager-Computers **UCMDB_CM_server**.
- Diese Änderung sollten nur Benutzer vornehmen, die sich mit der Apache-Verwaltung auskennen.

1. Öffnen Sie die Datei **<Stammverzeichnis des Apache-Computers>\Webserver\conf\httpd.conf**.
2. Aktivieren Sie die folgenden Module:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
   - **LoadModule headers_module modules/mod_headers.so**
3. Fügen Sie in der Datei httpd.conf die folgenden Zeilen hinzu:

```
ProxyRequests off
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
```

```
ProxyPassReverse /cm http://UCMDB_Server /cm

ProxyPass /cnc http://UCMDB_CM_server/cnc

ProxyPassReverse /cnc http://UCMDB_CM_server/cnc

ProxyPass /docs http://UCMDB_CM_server/docs

ProxyPassReverse /docs http://UCMDB_CM_server/docs

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

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

ProxyPreserveHost On

RequestHeader set X-Reverse-Proxy "https://<SRP-Host>:<SRP-Port>"
```

Hinweis: Die Zeile `ProxyPreserveHost On` ist nur erforderlich, wenn es einen virtuellen Host gibt.

Achtung: Wichtig ist, dass die Zeile `RequestHeader set X-Reverse-Proxy "https://<SRP-Host>:<SRP-Port>"` hinzugefügt wird, da die Konfiguration sonst nicht funktioniert.

4. Speichern Sie Ihre Änderungen.

Verbinden der Data Flow Probe über einen Reverse-Proxy oder Load Balancer mit gegenseitiger Authentifizierung

Führen Sie die folgende Prozedur aus, um die Data Flow Probe über einen Reverse-Proxy oder Load Balancer mittels gegenseitiger Authentifizierung zu verbinden. Diese Prozedur gilt für die folgende Konfiguration:

- Gegenseitige SSL-Authentifizierung zwischen der Probe und einem Reverse-Proxy oder Load Balancer auf der Basis eines Clientzertifikats, das von der Probe bereitgestellt und vom Reverse-Proxy oder Load Balancer benötigt wird.
- Reguläre SSL-Verbindung zwischen dem Reverse-Proxy oder Load Balancer und dem UCMDB-Server.

Hinweis: In den folgenden Anweisungen wird der Key Store **cKeyStoreFile** als Probe-Key Store verwendet. Dies ist ein vordefinierter Client-Key Store, der Bestandteil der Data Flow Probe-Installation ist und selbstsignierte Zertifikate enthält. Weitere Informationen finden Sie unter "Standard-Key Store und -Trust Store von Server und Data Flow Probe" auf Seite 80.

Es wird empfohlen, dass Sie einen neuen, eindeutigen Key Store mit einem neu erzeugten privaten Schlüssel erstellen. Weitere Informationen finden Sie unter "Erzeugen eines Key Store für die Data Flow Probe" auf Seite 79.

Anfordern eines Zertifikats von einer Zertifizierungsstelle

Fordern Sie das Stammzertifikat der Zertifizierungsstelle an und importieren Sie es in die folgenden Speicherorte:

- Trust Store der Data Flow Probe
- Trust Store **cacerts** der JVM der Data Flow Probe
- Trust Store des UCMDB-Servers
- Trust Store des Reverse-Proxy

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Trust Store der Data Flow Probe.

   a. Speichern Sie das Stammzertifikat der Zertifizierungsstelle im folgenden Verzeichnis: <Data Flow Probe-Installationsverzeichnis>\conf\security\<Name der Zertifikatsdatei>.

   b. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Trust Store der Data Flow Probe, indem Sie das folgende Skript ausführen:

   ```
   <Data Flow Probe-
   Installationsverzeichnis>\bin\jre\bin\keytool.exe -import -
   trustcacerts -alias <Ihr Alias> -file
   C:\hp\UCMDB\DataFlowProbe\conf\security\<Name der
   Zertifikatsdatei> -keystore <Data Flow Probe-
   Installationsverzeichnis>\conf\security\MAMTrustStoreExp.jks
   ```

   Das Standardkennwort lautet **logomania**.

2. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Trust Store **cacerts** der JVM der Data Flow Probe, indem Sie das folgende Skript ausführen:

   ```
   <Data Flow Probe-Installationsverzeichnis>\bin\jre\bin\keytool.exe
   -import -trustcacerts -alias <Ihr Alias> -file <Data Flow Probe-
   Installationsverzeichnis>\conf\security\<Name der Zertifikatsdatei>
   -keystore <Data Flow Probe-
   Installationsverzeichnis>\bin\jre\lib\security\cacerts
   ```

   Das Standardkennwort lautet **changeit**.

3. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den UCMDB-Trust Store.

   a. Speichern Sie das Stammzertifikat der Zertifizierungsstelle im folgenden Verzeichnis: <UCMDB-Installationsverzeichnis>\conf\security\<Name der Zertifikatsdatei>.

   b. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den UCMDB-Trust Store, indem Sie das folgende Skript ausführen:

   ```
   <UCMDB-Installationsverzeichnis>\bin\jre\bin\keytool.exe -import
   -trustcacerts -alias <Ihr Alias> -file <UCMDB-
   Installationsverzeichnis>\conf\security\<Name der
   Zertifikatsdatei> -keystore <UCMDB-
   Installationsverzeichnis>\conf\security\server.truststore
   ```

   Das Standardkennwort lautet **hppass**.

4. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Trust Store des Reverse Proxy. Dieser Schritt ist vom Anbieter abhängig.

Konvertieren des Zertifikats in einen Java-Key Store

Fordern Sie bei Ihrer Zertifizierungsstelle das Clientzertifikat (und den privaten Schlüssel) für die Data Flow Probe im PFX/PKCS12-Format an und konvertieren Sie es in einen Java-Key Store, indem Sie das folgende Skript ausführen:

```
<Data Flow Probe-Installationsverzeichnis>\bin\jre\bin\keytool.exe -
importkeystore -srckeystore <vollständiger Pfad zum PFX-Key Store> -
destkeystore <vollständiger Pfad zum neuen Ziel-Key Store> -
srcstoretype PKCS12
```

Sie werden zur Eingabe der Kennwörter von Quell- und Ziel-Key Store aufgefordert.

Verwenden Sie für den Quell-Key Store das gleiche Kennwort wie beim Exportieren des PFX-Key Store.

Das Standardkennwort für den Ziel-Key Store der Data Flow Probe lautet **logomania**.

Hinweis: Wenn Sie für den Ziel-Key Store ein anderes Kennwort eingegeben haben als das Standardkennwort (logomania), müssen Sie das neue Kennwort in verschlüsselter Form in der Datei **<Data Flow Probe-Installationsverzeichnis>\conf\ssl.properties** (javax.net.ssl.keyStorePassword) angeben. Weitere Informationen finden Sie unter "Verschlüsseln der Kennwörter für den Key Store und Trust Store der Probe" auf Seite 79.

Speichern Sie den neuen Key Store im folgenden Verzeichnis: **<Data Flow Probe-Installationsverzeichnis>\conf\security**.

Achtung: Überschreiben Sie nicht die Datei **MAMKeyStoreExp.jks**.

Ändern der SSL-Eigenschaftendatei für die Verwendung des neu erstellten Key Store

Legen Sie den Key Store mit dem Clientzertifikat in der Datei **<Data Flow Probe-Installationsverzeichnis>\conf\ssl.properties** auf **javax.net.ssl.keyStore** fest.

Wenn Sie für Ihren Key Store ein anderes Kennwort verwenden als das Standardkennwort (logomania), müssen Sie **javax.net.ssl.keyStorePassword** nach der Verschlüsselung aktualisieren. Weitere Informationen zum Verschlüsseln des Kennworts finden Sie unter "Verschlüsseln der Kennwörter für den Key Store und Trust Store der Probe" auf Seite 79.

Überprüfen der Data Flow Probe-Konfiguration

Bearbeiten Sie die Datei **<Data Flow Probe-Installationsverzeichnis>\conf\DataFlowProbe.properties** wie folgt:

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

serverName = <Adresse des Reverse-Proxy-Servers>

serverPortHttps = <HTTPS-Port, der vom Reverse-Proxy abgehört wird, um
Anfragen an UCMDB umzuleiten>
```

Konfigurieren von UCMDB für die Verwendung von SSL

Weitere Informationen finden Sie unter "Aktivieren der SSL-Kommunikation" auf Seite 18.

Wenn das Zertifikat des UCMDB-Servers von der gleichen Zertifizierungsstelle erstellt wird wie die übrigen Zertifikate in dieser Prozedur, vertraut der Reverse-Proxy oder Load Balancer dem UCMDB-Zertifikat.

Kapitel 4

Verwalten der Data Flow-Anmeldeinformationen

Dieses Kapitel umfasst folgende Themen:

Verwalten der Data Flow-Anmeldeinformationen – Übersicht

Zur Ausführung einer Discovery oder Integration müssen Sie die Anmeldeinformationen für den Zugriff auf das Remote-System einrichten. Anmeldeinformationen werden im Dialogfeld **Data Flow Probe einrichten** konfiguriert und im UCMDB-Server gespeichert. Weitere Informationen finden Sie im Abschnitt über die Data Flow Probe-Einrichtung im *HP Universal CMDB – Handbuch zur Datenflussverwaltung*.

Der Speicher mit den Anmeldeinformationen wird von der Confidential Manager-Komponente verwaltet. Weitere Informationen finden Sie unter "Confidential Manager" auf Seite 95.

Die Data Flow Probe kann über den Confidential Manager-Client auf die Anmeldeinformationen zugreifen. Der Confidential Manager-Client befindet sich auf der Data Flow Probe und kommuniziert mit dem Confidential Manager-Server, der sich auf dem UCMDB-Server befindet. Die Kommunikation zwischen dem Confidential Manager-Client und dem Confidential Manager-Server ist verschlüsselt und der Confidential Manager-Client erfordert eine Authentifizierung, wenn er eine Verbindung zum Confidential Manager-Server herstellt.

Die Authentifizierung des Confidential Manager-Clients auf dem Confidential Manager-Server basiert auf einer LW-SSO-Komponente. Bevor die Verbindung zum Confidential Manager-Server hergestellt wird, sendet der Confidential Manager-Client ein LW-SSO-Cookie. Der Confidential Manager-Server prüft das Cookie und beginnt nach erfolgreicher Prüfung die Kommunikation mit dem Confidential Manager-Client. Weitere Informationen zu LW-SSO finden Sie unter "Konfigurieren der LW-SSO-Einstellungen" auf Seite 49.

Die Kommunikation zwischen dem Confidential Manager-Client und dem Confidential Manager-Server ist verschlüsselt. Informationen zum Aktualisieren der Verschlüsselungskonfiguration finden Sie unter "Konfigurieren der Verschlüsselung für die Confidential Manager-Kommunikation " auf Seite 49.

Achtung: Die Confidential Manager-Authentifizierung verwendet die auf dem Computer definierte koordinierte Universalzeit (UTC). Für eine erfolgreiche Authentifizierung müssen

Data Flow Probe und UCMDB-Server auf Universalzeit eingestellt sein. Server und Probe befinden sich möglicherweise in unterschiedlichen Zeitzonen und die UTC ist unabhängig von Zeitzonen und Sommerzeit.

Der Confidential Manager-Client behält die Anmeldeinformationen in einem lokalen Cache. Der Confidential Manager-Client ist so konfiguriert, dass alle Anmeldeinformationen vom Confidential Manager-Server heruntergeladen und in einem Cache gespeichert werden. Änderungen an den Anmeldeinformationen werden automatisch in regelmäßigen Abständen vom Confidential Manager-Server synchronisiert. Beim Cache kann es sich um einen Dateisystem- oder einen Arbeitsspeicher-Cache handeln, abhängig von den vorkonfigurierten Einstellungen. Darüber hinaus ist der Cache verschlüsselt und gegen externen Zugriff geschützt. Informationen zum Aktualisieren der Cache-Einstellungen finden Sie unter "Konfigurieren des Cache-Modus für den Confidential Manager-Client auf der Probe" auf Seite 54. Informationen zum Aktualisieren der Cache-Verschlüsselung finden Sie unter "Konfigurieren der Verschlüsselungseinstellungen für den Cache des Confidential Manager-Clients auf der Probe" auf Seite 54.

Informationen zur Fehlerbehebung finden Sie unter "Ändern der Meldungsebene für die Protokolldatei des Confidential Manager-Clients" auf Seite 57.

Sie können Anmeldeinformationen von einem UCMDB-Server auf einen anderen kopieren. Weitere Informationen finden Sie unter "Exportieren und Importieren von Anmelde- und Bereichsinformationen im verschlüsselten Format" auf Seite 56.

Hinweis: Das **DomainScopeDocument** (DSD), das zum Speichern von Anmeldeinformationen auf der Probe verwendet wurde (in UCMDB Version 9.01 oder niedriger), enthält keine sensiblen Anmeldeinformationen mehr. Die Datei enthält nun eine Liste der Proben sowie Informationen zum Netzwerkbereich. Außerdem enthält sie eine Liste mit Einträgen für die Anmeldeinformationen jeder Domäne. Diese Einträge enthalten nur die ID der Anmeldeinformationen und einen Netzwerkbereich (wie für den jeweiligen Eintrag definiert).

Dieser Abschnitt umfasst die folgenden Themen:

Grundlegende Sicherheitsvoraussetzungen

Beachten Sie die folgende Sicherheitsvoraussetzung:

Sie haben die JMX-Konsole von UCMDB Server und Probe so geschützt, dass nur UCMDB-Systemadministratoren darauf zugreifen können und auch das bevorzugt nur mit **localhost**-Zugriff.

Ausführen der Data Flow Probe im separaten Modus

Wenn Probe Gateway und Probe Manager als separate Prozesse ausgeführt werden, wird die Client-Komponente von Confidential Manager zu einem Teil des Manager-Prozesses. Anmeldeinformationen werden im Cache gespeichert und nur vom Probe Manager verwendet. Für den Zugriff auf den Confidential Manager-Server im UCMDB-System wird die Confidential Manager-Clientanfrage vom Gateway-Prozess verarbeitet und von dort an das UCMDB-System weitergeleitet.

Diese Konfiguration erfolgt automatisch, wenn die Probe im separaten Modus konfiguriert ist.

Aktualisieren der Anmeldeinformationen im Cache

Bei der ersten erfolgreichen Verbindung zum Confidential Manager-Server lädt der Confidential Manager-Client alle relevanten Anmeldeinformationen herunter (alle in der Probendomäne konfigurierten Anmeldeinformationen). Nach der ersten erfolgreichen Kommunikation wird der Confidential Manager-Client kontinuierlich mit dem Confidential Manager-Server synchronisiert. Die Synchronisierung erfolgt in Intervallen von einer Minute, wobei nur die Abweichungen zwischen dem Confidential Manager-Server und dem Confidential Manager-Client synchronisiert werden. Werden die Anmeldeinformationen auf dem UCMDB-Server geändert (z. B. neue Anmeldeinformationen werden hinzugefügt oder vorhandene Anmeldeinformationen werden aktualisiert oder gelöscht), erhält der Confidential Manager-Client eine sofortige Benachrichtigung vom UCMDB-Server und führt eine zusätzliche Synchronisierung durch.

Synchronisieren aller Proben mit Konfigurationsänderungen

Für die erfolgreiche Kommunikation muss der Confidential Manager-Client mit der Authentifizierungskonfiguration (LW-SSO-Init-Zeichenkette) und der Verschlüsselungskonfiguration (Verschlüsselung für die Confidential Manager-Kommunikation) des Confidential Manager-Servers aktualisiert werden. Beispiel: Wenn die Init-Zeichenkette auf dem Server geändert wird, muss die Probe die neue Init-Zeichenkette kennen, um die Authentifizierung durchzuführen.

Der UCMDB-Server überwacht ständig, ob Änderungen an der Verschlüsselungskonfiguration für die Confidential Manager-Kommunikation und an der Confidential Manager-Authentifizierungskonfiguration vorgenommen wurden. Diese Überwachung erfolgt alle 15 Sekunden; im Falle von Änderungen wird die aktualisierte Konfiguration an die Proben gesendet. Die Konfiguration wird in verschlüsselter Form an die Proben weitergeleitet und wird auf der Probe in einem sicheren Speicher abgelegt. Bei der Verschlüsselung der gesendeten Konfiguration wird ein symmetrischer Verschlüsselungsschlüssel verwendet. Standardmäßig werden der UCMDB-Server und die Data Flow Probe mit demselben symmetrischen Standard-Verschlüsselungsschlüssel installiert. Für optimale Sicherheit wird dringend empfohlen, diesen Schlüssel zu ändern, bevor Anmeldeinformationen zum System hinzugefügt werden. Weitere Informationen finden Sie unter "Erzeugen oder Aktualisieren des Verschlüsselungsschlüssels" auf Seite 58.

Hinweis: Aufgrund des Überwachungsintervalls von 15 Sekunden kann es vorkommen, dass der Confidential Manager-Client auf der Seite der Probe über eine Zeitspanne von 15 Sekunden nicht mit der neuesten Konfiguration aktualisiert wird.

Wenn Sie die automatische Synchronisierung der Kommunikations- und Authentifizierungskonfiguration für Confidential Manager zwischen dem UCMDB-Server und der Data Flow Probe deaktivieren, sollten Sie jedes Mal, wenn Sie die Kommunikations- und Authentifizierungskonfiguration für Confidential Manager auf dem UCMDB-Server aktualisieren, auch alle Proben mit der neuen Konfiguration aktualisieren. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" auf Seite 51.

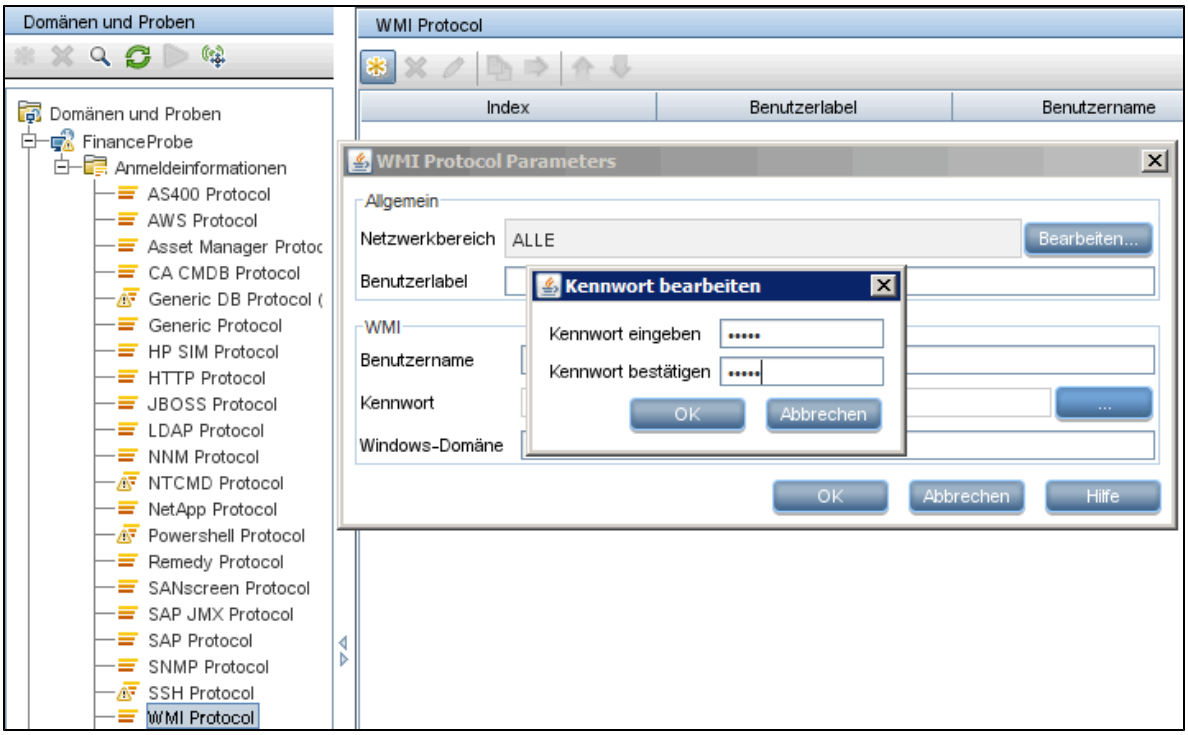
Sicheres Speichern auf der Probe

Alle sensiblen Informationen (wie z. B. die Kommunikations- und Authentifizierungskonfiguration für Confidential Manager und der Verschlüsselungsschlüssel) werden auf der Probe in einem sicheren Speicher in der Datei **secured_storage.bin** gespeichert, die sich im Verzeichnis **C:\hp\UCMDB\DataFlowProbe\conf\security** befindet. Dieser sichere Speicher wird mit DPAPI verschlüsselt; der Verschlüsselungsprozess beruht auf dem Windows-Benutzerkennwort. Bei DPAPI handelt es sich um eine Standardmethode für den Schutz sensibler Daten, darunter Zertifikate und private Schlüssel, auf Windows-Systemen. Die Probe sollte immer unter demselben Windows-Benutzer ausgeführt werden, damit die Probe die Daten im sicheren Speicher selbst nach Kennwortänderungen noch lesen kann.

Anzeigen von Anmeldeinformationen

Hinweis: In diesem Abschnitt wird das Anzeigen von Anmeldeinformationen beschrieben, wenn die Datenrichtung von der CMDB zu HP Universal CMDB verläuft.

Kennwörter werden nicht von der CMDB an die Applikation gesendet. Dies bedeutet, dass HP Universal CMDB im Kennwortfeld nur Sterne (*) anzeigt, unabhängig vom Inhalt:



Aktualisieren von Anmeldeinformationen

Hinweis: In diesem Abschnitt wird das Aktualisieren von Anmeldeinformationen beschrieben, wenn die Datenrichtung von HP Universal CMDB zur CMDB verläuft.

- In dieser Richtung wird die Kommunikation nicht verschlüsselt, sodass Sie die Verbindung zum UCMDB-Server über HTTPS bzw. SSL oder über ein vertrauenswürdiges Netzwerk herstellen sollten.

  Obwohl die Kommunikation nicht verschlüsselt wird, werden Kennwörter nicht als Klartext über das Netzwerk gesendet. Sie werden mit einem Standardschlüssel verschlüsselt; daher wird dringend die Verwendung von SSL empfohlen, um die Vertraulichkeit bei der Übertragung sicherzustellen.

- Sie können Sonderzeichen und nicht englische Zeichen für Kennwörter verwenden.

Konfigurieren der Authentifizierungs- und Verschlüsselungseinstellungen für den Confidential Manager-Client

Diese Aufgabe beschreibt das Konfigurieren der Authentifizierungs- und Verschlüsselungseinstellungen für den Confidential Manager-Client auf dem UCMDB-Server und umfasst die folgenden Schritte:

- "Konfigurieren der LW-SSO-Einstellungen" oben
- "Konfigurieren der Verschlüsselung für die Confidential Manager-Kommunikation " oben

Konfigurieren der LW-SSO-Einstellungen

In dieser Prozedur wird beschrieben, wie Sie die LW-SSO-Init-Zeichenkette auf dem UCMDB-Server ändern. Diese Änderung wird automatisch an die Proben gesendet (als verschlüsselte Zeichenkette), es sei denn, der UCMDB-Server ist so konfiguriert, dass dieser Vorgang nicht automatisch erfolgt. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" auf Seite 51.

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console**.
2. Klicken Sie auf **UCMDB-UI:name=LW-SSO Configuration**, um die Seite **JMX MBEAN View** anzuzeigen.
3. Suchen Sie die Methode **setInitString**.
4. Geben Sie eine neue LW-SSO-Init-Zeichenkette ein.
5. Klicken Sie auf **Invoke**.

Konfigurieren der Verschlüsselung für die Confidential Manager-Kommunikation

In dieser Prozedur wird beschrieben, wie Sie die Verschlüsselungseinstellungen für die Confidential Manager-Kommunikation auf dem UCMDB-Server ändern. Diese Einstellungen bestimmen, wie die Kommunikation zwischen dem Confidential Manager-Client und dem Confidential Manager-Server verschlüsselt wird. Diese Änderung wird automatisch an die Proben gesendet (als verschlüsselte Zeichenkette), es sei denn, der UCMDB-Server ist so konfiguriert, dass dieser Vorgang nicht automatisch erfolgt. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" auf Seite 51.

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console.**
2. Klicken Sie auf **UCMDB:service=Security Services**, um die Seite **JMX MBEAN View** zu öffnen.
3. Klicken Sie auf die Methode **CMGetConfiguration**.
4. Klicken Sie auf **Invoke**.

   Die XML-Datei mit der derzeitigen Confidential Manager-Konfiguration wird angezeigt.
5. Kopieren Sie die Inhalte der angezeigten XML-Datei.
6. Kehren Sie zurück zu **Security Services** und der Seite **JMX MBEAN View**.
7. Klicken Sie auf die Methode **CMSetConfiguration**.
8. Fügen Sie die kopierte XML-Datei in das Feld **Value** ein.
9. Aktualisieren Sie die relevanten Übertragungseinstellungen.

Informationen zu den Werten, die aktualisiert werden können, finden Sie unter "Confidential Manager-Verschlüsselungseinstellungen" auf Seite 63.

Beispiel:

```
<transport>
        <encryptTransportMode>true</encryptTransportMode>
        <CMEncryptionDecryption>
                <encryptDecryptInitString>radiohead</encryptDecryptInitString>
                <cryptoSource>lw</cryptoSource>
                <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
                <cipherType>symmetricBlockCipher</cipherType>
                <engineName>AES</engineName>
                <algorithmModeName>CBC</algorithmModeName>
                <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
                <keySize>256</keySize>
                <pbeCount>20</pbeCount>
                <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
                <encodingMode>Base64Url</encodingMode>
                <useMacWithCrypto>false</useMacWithCrypto>
                <macType>hmac</macType>
                <macKeySize>256</macKeySize>
                <macHashName>SHA256</macHashName>
        </CMEncryptionDecryption>
</transport>
```

10. Klicken Sie auf **Invoke**.

Manuelles Konfigurieren der Authentifizierungs- und Verschlüsselungseinstellungen für den Confidential Manager-Client auf der Probe

Diese Aufgabe umfasst folgende Schritte:

- "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" oben

- "Konfigurieren der Authentifizierungs- und Verschlüsselungseinstellungen für den Confidential Manager-Client auf der Probe" oben
- "Konfigurieren der Kommunikationsverschlüsselung für Confidential Manager auf der Probe" auf der nächsten Seite

Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben

Standardmäßig ist der UCMDB-Server so konfiguriert, dass die Confidential Manager/LW-SSO-Einstellungen automatisch an alle Proben gesendet werden. Diese Informationen werden als verschlüsselte Zeichenkette an die Proben gesendet, wo die Informationen nach dem Empfang entschlüsselt werden. Sie können den UCMDB-Server so konfigurieren, dass die Confidential Manager/LW-SSO-Konfigurationsdateien nicht automatisch an alle Proben gesendet werden. In diesem Fall sind Sie selbst dafür verantwortlich, alle Proben manuell mit den neuen Confidential Manager/LW-SSO-Einstellungen zu aktualisieren.

So deaktivieren Sie die automatische Synchronisierung der Confidential Manager/LW-SSO-Einstellungen:

1. Klicken Sie in UCMDB auf **Verwaltung > Infrastructure Settings Manager > Allgemeine Einstellungen**.
2. Wählen Sie **Automatische Synchronisierung der CM/LW-SSO-Konfiguration und der Init-Zeichenfolge für Probe aktivieren** aus.
3. Klicken Sie auf das Feld **Wert** und ändern Sie **True** in **False**.
4. Klicken Sie auf die Schaltfläche **Save**.
5. Starten Sie den UCMDB-Server neu.

Konfigurieren der Authentifizierungs- und Verschlüsselungseinstellungen für den Confidential Manager-Client auf der Probe

Diese Prozedur ist relevant, wenn der UCMDB-Server so konfiguriert wurde, dass die Konfigurationen und Einstellungen für LW-SSO/Confidential Manager nicht automatisch an die Proben gesendet werden. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" unten.

1. Starten Sie auf dem Probe-Computer den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:1977**.

   Hinweis: Wenn Probe Manager und Probe Gateway als separate Prozesse ausgeführt

werden, muss die Adresse auf dem Probe Manager-Computer wie folgt eingegeben werden: **http://localhost:1978**.

2. Klicken Sie auf **type=CMClient**, um die Seite **JMX MBEAN View** zu öffnen.
3. Suchen Sie die Methode **setLWSSOInitString** und geben Sie dieselbe Init-Zeichenfolge wie in der LW-SSO-Konfiguration für UCMDB an.
4. Klicken Sie auf die Schaltfläche **setLWSSOInitString**.

Konfigurieren der Kommunikationsverschlüsselung für Confidential Manager auf der Probe

Diese Prozedur ist relevant, wenn der UCMDB-Server so konfiguriert wurde, dass die Konfigurationen und Einstellungen für LW-SSO/Confidential Manager nicht automatisch an die Proben gesendet werden. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der Authentifizierungs- und Verschlüsselungseinstellungen des Confidential Manager-Clients zwischen Server und Proben" auf der vorherigen Seite.

1. Starten Sie auf dem Probe-Computer den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:1977**.

   Hinweis: Wenn Probe Manager und Probe Gateway als separate Prozesse ausgeführt werden, muss die Adresse auf dem Probe Manager-Computer wie folgt eingegeben werden: **http://localhost:1978**.

2. Klicken Sie auf **type=CMClient**, um die Seite **JMX MBEAN View** zu öffnen.
3. Aktualisieren Sie die folgenden Übertragungseinstellungen:

   Hinweis: Sie müssen dieselben Einstellungen aktualisieren wie auf dem UCMDB-Server. Dabei erfordern einige der Methoden, die Sie auf der Probe aktualisieren, möglicherweise mehrere Parameter. Zum Anzeigen der derzeitigen Probe-Konfiguration klicken Sie auf der Seite **JMX MBEAN View** auf **displayTransportConfiguration**. Weitere Informationen finden Sie unter "Konfigurieren der Verschlüsselung für die Confidential Manager-Kommunikation " auf Seite 49. Informationen zu den Werten, die aktualisiert werden können, finden Sie unter "Confidential Manager-Verschlüsselungseinstellungen" auf Seite 63.

   a. **setTransportInitString** ändert die Einstellung **encryptDecryptInitString**.

   b. **setTransportEncryptionAlgorithm** ändert die Einstellungen für Confidential Manager auf der Probe gemäß der folgenden Zuordnung:

      - Die Einstellung **Engine name** bezieht sich auf den <engineName>-Eintrag und legt den Namen der Engine fest.
      - Die Einstellung **Key size** bezieht sich auf den <keySize>-Eintrag und legt die

Schlüsselgröße fest.

- Die Einstellung **Algorithm padding name** bezieht sich auf den <algorithmPaddingName>-Eintrag und legt den Namen des Auffüllalgorithmus fest.
- Die Einstellung **PBE count** bezieht sich auf den <pbeCount>-Eintrag und legt die Anzahl der PBE-Ausführungen fest.
- Die Einstellung **PBE digest algorithm** bezieht sich auf den <pbeDigestAlgorithm>-Eintrag und legt den PBE-Typ fest.

c. **setTransportEncryptionLibrary** ändert die Einstellungen für Confidential Manager auf der Probe gemäß der folgenden Zuordnung:

- Die Einstellung **Encryption Library name** bezieht sich auf den <cryptoSource>-Eintrag und legt den Namen der Verschlüsselungsbibliothek fest.
- Die Einstellung **Support previous lightweight cryptography versions** bezieht sich auf den <lwJCEPBECompatibilityMode>-Eintrag und legt fest, ob vorherige schwache Kryptographie unterstützt wird.

d. **setTransportMacDetails** ändert Einstellungen für Confidential Manager auf der Probe gemäß der folgenden Zuordnung:

- Die Einstellung **Use MAC with cryptography** bezieht sich auf den <useMacWithCrypto>-Eintrag und legt fest, ob MAC bei der Kryptographie verwendet wird.
- Die Einstellung **MAC key size** bezieht sich auf den <macKeySize>-Eintrag und legt die MAC-Schlüsselgröße fest.

4. Klicken Sie auf die Schaltfläche **reloadTransportConfiguration**, damit die Änderungen auf der Probe angewendet werden.

Weitere Informationen zu den verschiedenen Einstellungen und ihren möglichen Werten finden Sie unter "Confidential Manager-Verschlüsselungseinstellungen" auf Seite 63.

Konfigurieren des Client-Cache für Confidential Manager

Diese Aufgabe umfasst folgende Schritte:

- "Konfigurieren des Cache-Modus für den Confidential Manager-Client auf der Probe" auf der nächsten Seite
- "Konfigurieren der Verschlüsselungseinstellungen für den Cache des Confidential Manager-Clients auf der Probe" auf der nächsten Seite

Konfigurieren des Cache-Modus für den Confidential Manager-Client auf der Probe

Der Confidential Manage-Client speichert Anmeldeinformationen im Cache und aktualisiert sie, wenn sich die Informationen auf dem Server ändern. Der Cache kann sich im Dateisystem oder im Arbeitsspeicher befinden:

- **Speicherung im Dateisystem**: Selbst wenn die Probe neu gestartet wird und keine Verbindung zum Server herstellen kann, sind die Anmeldeinformationen weiterhin verfügbar.
- **Speicherung im Arbeitsspeicher**: Beim Neustart der Probe wird der Cache geleert und alle Informationen werden erneut vom Server abgerufen. Ist der Server nicht verfügbar, enthält die Probe keine Anmeldeinformationen, sodass keine Discovery oder Integration ausgeführt werden kann.

So ändern Sie diese Einstellung:

1. Öffnen Sie die Datei **DataFlowProbe.properties** in einem Texteditor. Diese Datei befindet sich im Ordner **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Suchen Sie nach dem folgenden Attribut:
   com.hp.ucmdb.discovery.common.security.storeCMData=true
   - Zum Speichern der Informationen im Dateisystem behalten Sie den Standardwert (**true**) bei.
   - Zum Speichern der Informationen im Arbeitsspeicher geben Sie **false** ein.
3. Speichern Sie die Datei **DataFlowProbe.properties**.
4. Starten Sie die Probe neu.

Konfigurieren der Verschlüsselungseinstellungen für den Cache des Confidential Manager-Clients auf der Probe

In dieser Prozedur wird beschrieben, wie Sie die Verschlüsselungseinstellungen für die Cache-Datei im Dateisystem des Confidential Manager-Clients ändern. Beachten Sie, dass die Cache-Datei im Dateisystem des Confidential Manager-Clients nach dem Ändern ihrer Verschlüsselungseinstellungen neu erstellt wird. Diese Neuerstellung erfordert einen Neustart der Probe und eine vollständige Synchronisierung mit dem UCMDB-Server.

1. Starten Sie auf dem Probe-Computer den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:1977**.

   Hinweis: Wenn Probe Manager und Probe Gateway als separate Prozesse ausgeführt werden, muss die Adresse auf dem Probe Manager-Computer wie folgt eingegeben werden: **http://localhost:1978**.

2. Klicken Sie auf **type=CMClient**, um die Seite **JMX MBEAN View** zu öffnen.
3. Aktualisieren Sie die folgenden Cache-Einstellungen:

   Hinweis: Einige der Methoden, die Sie auf der Probe aktualisieren, erfordern möglicherweise mehrere Parameter. Zum Anzeigen der derzeitigen Probe-Konfiguration klicken Sie auf der Seite **JMX MBEAN View** auf **displayCacheConfiguration**.

   a. **setCacheInitString** ändert die Einstellung <encryptDecryptInitString> für den Dateisystem-Cache.

b. **setCacheEncryptionAlgorithm** ändert die Einstellungen für den Dateisystem-Cache gemäß der folgenden Zuordnung:

- Die Einstellung **Engine name** bezieht sich auf den <engineName>-Eintrag und legt den Namen der Engine fest.
- Die Einstellung **Key size** bezieht sich auf den <keySize>-Eintrag und legt die Schlüsselgröße fest.
- Die Einstellung **Algorithm padding name** bezieht sich auf den <algorithmPaddingName>-Eintrag und legt den Namen des Auffüllalgorithmus fest.
- Die Einstellung **PBE count** bezieht sich auf den <pbeCount>-Eintrag und legt die Anzahl der PBE-Ausführungen fest.
- Die Einstellung **PBE digest algorithm** bezieht sich auf den <pbeDigestAlgorithm>-Eintrag und legt den PBE-Typ fest.

c. **setCacheEncryptionLibrary** ändert die Einstellungen für den Dateisystem-Cache gemäß der folgenden Zuordnung:

- Die Einstellung **Encryption Library name** bezieht sich auf den <cryptoSource>-Eintrag und legt den Namen der Verschlüsselungsbibliothek fest.
- Die Einstellung **Support previous lightweight cryptography versions** bezieht sich auf den <lwJCEPBECompatibilityMode>-Eintrag und legt fest, ob vorherige schwache Kryptographie unterstützt wird.

d. **setCacheMacDetails** ändert die Einstellungen für den Dateisystem-Cache gemäß der folgenden Zuordnung:

- Die Einstellung **Use MAC with cryptography** bezieht sich auf den <useMacWithCrypto>-Eintrag und legt fest, ob MAC bei der Kryptographie verwendet wird.
- Die Einstellung **MAC key size** bezieht sich auf den <macKeySize>-Eintrag und legt die MAC-Schlüsselgröße fest.

4. Klicken Sie auf die Schaltfläche **reloadCacheConfiguration**, damit die Änderungen auf der Probe angewendet werden. Dadurch wird die Probe neu gestartet.

> **Hinweis:** Stellen Sie sicher, dass während dieser Aktion kein Job auf der Probe ausgeführt wird.

Weitere Informationen zu den verschiedenen Einstellungen und ihren möglichen Werten finden Sie unter "Confidential Manager-Verschlüsselungseinstellungen" auf Seite 63.

Exportieren und Importieren von Anmelde- und Bereichsinformationen im verschlüsselten Format

Sie können Anmelde- und Netzwerkbereichsinformationen im verschlüsselten Format exportieren und importieren, um die Anmeldeinformationen von einem UCMDB-Server auf einen anderen zu

kopieren. Diesen Vorgang können Sie z. B. bei der Wiederherstellung nach einem Systemabsturz oder im Rahmen eines Upgrades durchführen.

- **Beim Exportieren von Anmeldeinformationen** müssen Sie ein (selbst gewähltes) Kennwort eingeben. Die Informationen werden mit diesem Kennwort verschlüsselt.
- **Beim Importieren von Anmeldeinformationen** müssen Sie das Kennwort verwenden, das beim Exportieren der DSD-Datei definiert wurde.

Hinweis: Das Exportdokument mit den Anmeldeinformationen enthält auch Bereichsinformationen, die auf dem System definiert sind, von dem das Dokument exportiert wurde. Beim Importieren des Dokuments mit den Anmeldeinformationen werden auch die Bereichsinformationen importiert.

Achtung: Zum Importieren von Anmeldeinformationen aus dem **domainScopeDocument** der UCMDB-Version 8.02 müssen Sie die Datei **key.bin** verwenden, die sich im System der Version 8.02 befindet.

So exportieren Sie Anmeldeinformationen vom UCMDB-Server:

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console**. Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.
2. Klicken Sie auf **UCMDB:service=DiscoveryManager**, um die Seite **JMX MBEAN View** zu öffnen.
3. Suchen Sie den Vorgang **exportCredentialsAndRangesInformation**. Führen Sie folgende Aktionen aus:
   - Geben Sie Ihre Kunden-ID ein (die Standard-ID lautet 1).
   - Geben Sie einen Namen für die exportierte Datei ein.
   - Geben Sie Ihr Kennwort ein.
   - Legen Sie **isEncrypted=True** fest, wenn die exportierte Datei mit dem angegebenen Kennwort verschlüsselt werden soll, oder legen Sie **isEncrypted=False** fest, wenn die exportierte Datei nicht verschlüsselt werden soll (in diesem Fall werden Kennwörter und andere sensible Informationen nicht exportiert).
4. Klicken Sie zum Exportieren auf **Invoke**.

   Wenn der Exportvorgang erfolgreich abgeschlossen wurde, befindet sich die Datei im folgenden Ordner: **c:\hp\UCMDB\UCMDBServer\conf\discovery\<Kundenverzeichnis>**.

So importieren Sie Anmeldeinformationen vom UCMDB-Server:

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console**.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.
2. Klicken Sie auf **UCMDB:service=DiscoveryManager**, um die Seite **JMX MBEAN View** zu öffnen.

3. Suchen Sie einen der folgenden Vorgänge:
   - Suchen Sie den Vorgang **importCredentialsAndRangesInformation**, wenn die zu importierende Datei von einem UCMDB-Server mit einer höheren Version als 8.02 exportiert wurde.
   - Suchen Sie den Vorgang **importCredentialsAndRangesWithKey**, wenn die zu importierende Datei von einem UCMDB-Server mit der Version 8.02 exportiert wurde.
4. Geben Sie Ihre Kunden-ID ein (die Standard-ID lautet 1).
5. Geben Sie den Namen der zu importierenden Datei ein. Diese Datei muss sich im Verzeichnis **c:\hp\UCMDB\UCMDBServer\conf\discovery\<Kundenverzeichnis>** befinden.
6. Geben Sie das Kennwort ein. Dieses Kennwort muss mit dem identisch sein, das zum Exportieren der Datei verwendet wurde.
7. Wenn die Datei aus einem UCMDB-System mit der Version 8.02 exportiert wurde, geben Sie den Dateinamen **key.bin** ein. Diese Datei muss sich zusammen mit der zu importierenden Datei im Verzeichnis **c:\hp\UCMDB\UCMDBServer\conf\discovery\<Kundenverzeichnis>** befinden.
8. Klicken Sie auf **Invoke**, um die Anmeldeinformationen zu importieren.

Ändern der Meldungsebene für die Protokolldatei des Confidential Manager-Clients

Die Probe stellt zwei Protokolldateien bereit, die Informationen zur Confidential Manager-bezogenen Kommunikation zwischen dem Confidential Manager-Server und dem Confidential Manager-Client enthalten. Diese Dateien sind:

- "Protokolldatei des Confidential Manager-Clients" oben
- "LW-SSO-Protokolldatei" auf der nächsten Seite

Protokolldatei des Confidential Manager-Clients

Die Datei **security.cm.log** befindet sich im Ordner **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Das Protokoll enthält Informationsmeldungen, die zwischen dem Confidential Manager-Server und dem Confidential Manager-Client ausgetauscht werden. Die Protokollebene dieser Meldungen ist standardmäßig auf INFO festgelegt.

So ändern Sie die Protokollebene der Meldungen in DEBUG:

1. Navigieren Sie auf dem Data Flow Probe Manager-Server zu **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Öffnen Sie die Datei **security.properties** in einem Texteditor.
3. Ändern Sie die Zeile:

   ```
   loglevel.cm=INFO
   ```

in

```
loglevel.cm=DEBUG
```

4. Speichern Sie die Datei.

LW-SSO-Protokolldatei

Die Datei **security.lwsso.log** befindet sich im Ordner **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Das Protokoll enthält Informationsmeldungen, die sich auf LW-SSO beziehen. Die Protokollebene dieser Meldungen ist standardmäßig auf INFO festgelegt.

So ändern Sie die Protokollebene der Meldungen in DEBUG:

1. Navigieren Sie auf dem Data Flow Probe Manager-Server zu **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Öffnen Sie die Datei **security.properties** in einem Texteditor.
3. Ändern Sie die Zeile:

   ```
   loglevel.lwsso=INFO
   ```

   in

   ```
   loglevel.lwsso=DEBUG
   ```

4. Speichern Sie die Datei.

Erzeugen oder Aktualisieren des Verschlüsselungsschlüssels

Sie können einen Verschlüsselungsschlüssel erzeugen oder aktualisieren, der zum Ver- oder Entschlüsseln der Kommunikations- und Authentifizierungskonfiguration von Confidential Manager verwendet wird, wenn diese zwischen dem UCMDB-Server und der Data Flow Probe ausgetauscht werden. In beiden Fällen (Erzeugen oder Aktualisieren) erstellt der UCMDB-Server einen neuen Verschlüsselungsschlüssel anhand der von Ihnen angegebenen Parameter (z. B. Schlüssellänge, PBE-Zyklen, JCE-Provider) und verteilt diesen Schlüssel an die Proben.

Durch das Ausführen der Methode **generateEncryptionKey** wird ein neuer Verschlüsselungsschlüssel erzeugt. Dieser Schlüssel wird nur im sicheren Speicher abgelegt und sein Name und seine Details sind nicht bekannt. Wenn Sie eine vorhandene Data Flow Probe erneut installieren oder eine neue Probe mit dem UCMDB-Server verbinden, wird dieser neu erzeugte Schlüssel nicht von der neuen Probe erkannt. In diesen Fällen sollten Sie die Methode **changeEncryptionKey** zum Ändern von Verschlüsselungsschlüsseln verwenden. Auf diese Weise können Sie den vorhandenen Schlüssel (dessen Name und Ort bekannt sind) beim erneuten Installieren einer Probe oder beim Installieren einer neuen Probe importieren, indem Sie die Methode **importEncryptionKey** in der JMX-Konsole der Probe ausführen.

Hinweis:

- Der Unterschied zwischen den Methoden zum Erzeugen eines Schlüssels (**generateEncryptionKey**) und zum Aktualisieren eines Schlüssels (**changeEncryptionKey**) besteht darin, dass durch **generateEncryptionKey** ein neuer, zufällig ausgewählter Verschlüsselungsschlüssel erstellt wird, während durch **changeEncryptionKey** ein Verschlüsselungsschlüssel importiert wird, dessen Namen Sie angeben.
- In jedem System kann nur ein einziger Verschlüsselungsschlüssel vorliegen, unabhängig von der Anzahl der installierten Proben.

Diese Aufgabe umfasst folgende Schritte:

- "Erzeugen eines neuen Verschlüsselungsschlüssels" oben
- "Aktualisieren eines Verschlüsselungsschlüssels auf einem UCMDB-Server" auf der nächsten Seite
- "Aktualisieren eines Verschlüsselungsschlüssels auf einer Probe" auf Seite 61
- "Manuelles Ändern des Verschlüsselungsschlüssels, wenn Probe Manager und Probe Gateway auf separaten Computern installiert sind" auf Seite 62
- "Definieren mehrerer JCE-Provider" auf Seite 62

Erzeugen eines neuen Verschlüsselungsschlüssels

Sie können einen neuen Schlüssel erzeugen, den der UCMDB-Server und die Data Flow Probe für die Ver- oder Entschlüsselung verwenden sollen. Der UCMDB-Server ersetzt den alten Schlüssel durch den neu erzeugten Schlüssel und verteilt diesen Schlüssel an die Proben.

So erzeugen Sie einen neuen Verschlüsselungsschlüssel über die JMX-Konsole:

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console**.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

2. Klicken Sie auf **UCMDB:service=DiscoveryManager**, um die Seite **JMX MBEAN View** zu öffnen.

3. Suchen Sie den Vorgang **generateEncryptionKey**.

   a. Geben Sie für den Parameter **customerId** den Wert **1** (Standardwert) ein.

   b. Geben Sie für **keySize** die Länge des Verschlüsselungsschlüssels an. Gültige Werte sind 128, 192 oder 256.

   c. Geben Sie für **usePBE** den Wert **True** oder **False** an:

      - **True:** Zusätzliche PBE-Hash-Zyklen verwenden.
      - **False:** keine zusätzlichen PBE-Hash-Zyklen verwenden.

   d. Für **jceVendor** können Sie festlegen, dass ein anderer JCE-Provider als der Standard-

Provider verwendet wird. Ist das Feld leer, wird der Standard-Provider verwendet.

e. Geben Sie für **autoUpdateProbe** den Wert **True** oder **False** an:

- **True:** Der Server verteilt den neuen Schlüssel automatisch an die Proben.
- **False:** Der neue Schlüssel muss manuell auf den Proben abgelegt werden.

f. Geben Sie für **exportEncryptionKey** den Wert **True** oder **False** an:

- **True:** Das neue Kennwort wird nicht nur erstellt und im sicheren Speicher abgelegt, sondern der Server exportiert das neue Kennwort auch in das Dateisystem (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Durch diese Option können Sie Proben manuell mit dem neuen Kennwort aktualisieren.
- **False:** Das neue Kennwort wird nicht in das Dateisystem exportiert. Zum manuellen Aktualisieren von Proben setzen Sie **autoUpdateProbe** auf **False** und **exportEncryptionKey** auf **True**.

> **Hinweis:** Stellen Sie sicher, dass die Probe ausgeführt wird und mit dem Server verbunden ist. Wird die Probe angehalten, kann der Schlüssel nicht an die Probe übermittelt werden. Wenn Sie den Schlüssel vor dem Anhalten der Probe ändern, wird der Schlüssel erneut an die Probe gesendet, nachdem sie wieder ausgeführt wird. Wenn Sie den Schlüssel jedoch vor dem Anhalten der Probe mehrmals geändert haben, müssen Sie den Schlüssel manuell über die JMX-Konsole ändern. (Wählen Sie **False** für **exportEncryptionKey** aus.)

4. Klicken Sie auf **Invoke**, um den Verschlüsselungsschlüssel zu erzeugen.

Aktualisieren eines Verschlüsselungsschlüssels auf einem UCMDB-Server

Mit der Methode **changeEncryptionKey** importieren Sie Ihren eigenen Verschlüsselungsschlüssel auf den UCMDB-Server und verteilen ihn an alle Proben.

So aktualisieren Sie einen Verschlüsselungsschlüssel über die JMX-Konsole:

1. Starten Sie auf dem UCMDB-Server den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:8080/jmx-console.**

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

2. Klicken Sie auf **UCMDB:service=DiscoveryManager**, um die Seite **JMX MBEAN View** zu öffnen.

3. Suchen Sie den Vorgang **changeEncryptionKey**.

   a. Geben Sie für den Parameter **customerId** den Wert **1** (Standardwert) ein.

   b. Geben Sie für **newKeyFileName** den Namen des neuen Schlüssels ein.

   c. Geben Sie für **keySizeInBits** die Länge des Verschlüsselungsschlüssels an. Gültige Werte sind 128, 192 oder 256.

d. Geben Sie für **usePBE** den Wert **True** oder **False** an:

- **True:** Zusätzliche PBE-Hash-Zyklen verwenden.
- **False:** keine zusätzlichen PBE-Hash-Zyklen verwenden.

e. Für **jceVendor** können Sie festlegen, dass ein anderer JCE-Provider als der Standard-Provider verwendet wird. Ist das Feld leer, wird der Standard-Provider verwendet.

f. Geben Sie für **autoUpdateProbe** den Wert **True** oder **False** an:

- **True:** Der Server verteilt den neuen Schlüssel automatisch an die Proben.
- **False:** Der neue Schlüssel muss manuell über die JMX-Konsole der Probe verteilt werden.

> **Hinweis:** Stellen Sie sicher, dass die Probe ausgeführt wird und mit dem Server verbunden ist. Wird die Probe angehalten, kann der Schlüssel nicht an die Probe übermittelt werden. Wenn Sie den Schlüssel vor dem Anhalten der Probe ändern, wird der Schlüssel erneut an die Probe gesendet, nachdem sie wieder ausgeführt wird. Wenn Sie den Schlüssel jedoch vor dem Anhalten der Probe mehrmals geändert haben, müssen Sie den Schlüssel manuell über die JMX-Konsole ändern. (Wählen Sie **False** für **autoUpdateProbe** aus.)

4. Klicken Sie auf **Invoke**, um den Verschlüsselungsschlüssel zu erzeugen und zu aktualisieren.

Aktualisieren eines Verschlüsselungsschlüssels auf einer Probe

Wenn Sie festlegen, dass der UCMDB-Server den Verschlüsselungsschlüssel nicht automatisch an alle Proben verteilen soll (aus Sicherheitsgründen), sollten Sie den neuen Verschlüsselungsschlüssel auf alle Proben herunterladen und die Methode **importEncryptionKey** auf der Probe ausführen:

1. Speichern Sie die Datei mit dem Verschlüsselungsschlüssel im Verzeichnis **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. Starten Sie auf dem Probe-Computer den Webbrowser und geben Sie die folgende Adresse ein: **http://localhost:1977**.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

   > **Hinweis:** Wenn Probe Manager und Probe Gateway als separate Prozesse ausgeführt werden, muss die Adresse auf dem Probe Manager-Computer wie folgt eingegeben werden: **http://localhost:1978**.

3. Klicken Sie in der Probendomäne auf **type=SecurityManagerService**.
4. Suchen Sie die Methode **importEncryptionKey**.

5. Geben Sie den Namen der Datei mit dem Verschlüsselungsschlüssel ein, die sich im Verzeichnis **C:\hp\UCMDB\DataFlowProbe\conf\security** befindet. Diese Datei enthält den zu importierenden Schlüssel.
6. Klicken Sie auf die Schaltfläche **importEncryptionKey**.
7. Starten Sie die Probe neu.

Manuelles Ändern des Verschlüsselungsschlüssels, wenn Probe Manager und Probe Gateway auf separaten Computern installiert sind

1. Starten Sie auf dem Probe Manager-Computer den Probe Manager-Service (**Start > Programme > HP UCMDB > Probe Manager**).
2. Importieren Sie den Schlüssel vom Server über die JMX-Konsole von Probe Manager. Weitere Informationen finden Sie unter "Erzeugen eines neuen Verschlüsselungsschlüssels" auf Seite 59.
3. Starten Sie nach dem erfolgreichen Importieren des Verschlüsselungsschlüssels die Probe Manager- und Probe Gateway-Services neu.

Definieren mehrerer JCE-Provider

Wenn Sie einen Verschlüsselungsschlüssel über die JMX-Konsole erzeugen, können Sie mit den Methoden **changeEncryptionKey** und **generateEncryptionKey** mehrere JCE-Provider definieren.

So ändern Sie den Standard-JCE-Provider:

1. Registrieren Sie die JAR-Dateien für JCE-Provider im Verzeichnis **$JRE_HOME/lib/ext**.
2. Kopieren Sie die JAR-Dateien in den Ordner **$JRE_HOME**:
   - Für den UCMDB-Server: $JRE_HOME befindet sich unter **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - Für die Data Flow Probe: $JRE_HOME befindet sich unter **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Fügen Sie die Provider-Klasse am Ende der Provider-Liste in der Datei **$JRE_HOME\lib\security\java.security** hinzu.
4. Aktualisieren Sie die Dateien **local_policy.jar** und **US_export_policy.jar** so, dass sie unbegrenzte JCE-Richtlinien enthalten. Sie können diese JAR-Dateien von der Sun-Website herunterladen.
5. Starten Sie den UCMDB-Server und die Data Flow Probe neu.
6. Suchen Sie das Feld für den JCE-Provider für die Methode **changeEncryptionKey** oder **generateEncryptionKey** und fügen Sie den Namen des JCE-Provider hinzu.

Confidential Manager-Verschlüsselungseinstellungen

In dieser Tabelle sind die Verschlüsselungseinstellungen aufgelistet, die mit den verschiedenen JMX-Methoden geändert werden können. Diese Verschlüsselungseinstellungen gelten für die Verschlüsselung der Kommunikation zwischen dem Confidential Manager-Client und dem Confidential Manager-Server sowie für die Verschlüsselung des Confidential Manager-Client-Cache.

Name der Confidential Manager-Einstellung	Name der Probe-Confidential Manager-Einstellung	Beschreibung der Einstellung	Mögliche Werte	Standardwert
cryptoSource	Encryption Library name	Diese Einstellung definiert, welche Verschlüsselungsbibliothek verwendet wird.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE Compatibility Mode	Support previous lightweight cryptography versions	Diese Einstellung definiert, ob vorherige schwache Kryptographie unterstützt wird oder nicht.	true, false	true
engineName	Engine name	Name des Verschlüsselungsmechanismus	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Länge des Verschlüsselungsschlüssels in Bit	Für AES – 128, 192 oder 256; Für DES - 64; Für 3DES - 192; Für Blowfish – eine beliebige Zahl zwischen 32 und 448	256
algorithm Padding Name	Algorithm padding name	Auffüllstandards	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE count	Wie oft der Hash ausgeführt wird, um den Schlüssel aus dem Kennwort (Init-Zeichenfolge) zu erstellen	Beliebige positive Zahl	20
pbeDigest	PBE digest	Hashing-Typ	SHA1,	SHA1

Name der Confidential Manager-Einstellung	Name der Probe-Confidential Manager-Einstellung	Beschreibung der Einstellung	Mögliche Werte	Standardwert
Algorithm	algorithm		SHA256, MD5	
useMacWith Crypto	Use MAC with cryptography	Gibt an, ob MAC bei der Kryptographie verwendet wird	true, false	false
macKeySize	MAC key size	Abhängig vom MAC-Algorithmus	256	256

Fehlerbehebung und Einschränkungen

Wenn Sie den Standarddomänennamen auf dem UCMDB-Server ändern möchten, müssen Sie zuvor sicherstellen, dass die Data Flow Probe nicht aktiv ist. Wenn der Standarddomänenname geändert wurde, müssen Sie das Skript **DataFlowProbe\tools\clearProbeData.bat** auf der Seite der Data Flow Probe ausführen.

Hinweis: Nach der Ausführung des Skripts **clearProbeData.bat** wird auf der Seite der Probe ein Discovery-Zyklus gestartet, sobald die Probe wieder aktiv ist.

Kapitel 5

Härten der Data Flow Probe

Dieses Kapitel umfasst folgende Themen:

Ändern des verschlüsselten Kennworts für die MySQL-Datenbank

In diesem Abschnitt wird erklärt, wie Sie das verschlüsselte Kennwort für den MySQL-Datenbankbenutzer ändern.

1. Erstellen der verschlüsselten Form eines Kennworts (AES, 192 Bit-Schlüssel)

   a. Rufen Sie die JMX-Konsole der Data Flow Probe auf. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://<Name oder IP-Adresse des Data Flow Probe-Computers>:1977**. Wenn Sie die Data Flow Probe lokal ausführen, geben Sie **http://localhost:1977** ein.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

> **Hinweis:** Wenn Sie keinen Benutzer erstellt haben, melden Sie sich mit dem Standardbenutzernamen sysadmin und dem Standardkennwort sysadmin an.

b. Suchen Sie den Service **Type=MainProbe** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.

c. Suchen Sie den Vorgang **getEncryptedDBPassword**.

d. Geben Sie im Feld **DB Password** das zu verschlüsselnde Kennwort ein.

e. Rufen Sie den Vorgang über die Schaltfläche **getEncryptedDBPassword** auf.

Durch diesen Aufruf wird eine verschlüsselte Kennwortzeichenfolge erstellt. Beispiel:

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

2. Anhalten der Data Flow Probe

Start > Alle Programme > HP UCMDB > Data Flow Probe anhalten

3. Ausführen des Skripts set_dbuser_password.cmd

Dieses Skript befindet sich im folgenden Ordner:
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd

Führen Sie das Skript **set_dbuser_password.cmd** mit dem neuen Kennwort als erstem Argument und dem Kennwort für das MySQL-Stammkonto als zweitem Argument aus (lassen Sie das zweite Argument leer, wenn das MySQL-Stammkonto nicht kennwortgeschützt ist).

Beispiel:

set_dbuser_password <Mein Kennwort><Stammkennwort>.

Das Kennwort muss in unverschlüsselter Form (als Klartext) eingegeben werden.

4. Aktualisieren des Kennworts in den Data Flow Probe-Konfigurationsdateien

a. Das Kennwort muss in den Konfigurationsdateien verschlüsselt sein. Zum Abrufen des Kennworts in verschlüsselter Form verwenden Sie die JMX-Methode **getEncryptedDBPassword**, wie in Schritt 1 beschrieben.

b. Fügen Sie das verschlüsselte Kennwort zu den folgenden Eigenschaften in der Datei **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** hinzu.

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

  Beispiel:

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

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

5. Starten der Data Flow Probe

Start > Alle Programme > HP UCMDB > Data Flow Probe starten

Das Skript clearProbeData.bat: Verwendung

Durch das Skript **clearProbeData.bat** wird der Datenbankbenutzer neu erstellt, ohne sein derzeitiges Kennwort zu ändern.

Das Skript erwartet das Kennwort für das MySQL-Stammkonto als erstes Argument. Wenn keine Parameter übertragen werden, geht es davon aus, dass das Kennwort für das MySQL-Stammkonto leer ist.

Nach der Ausführung des Skripts:

- Prüfen Sie die folgende Datei auf Fehler:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log
- Löschen Sie die folgende Datei, da sie das Datenbankkennwort enthält:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

Einrichten des verschlüsselten Kennworts für die JMX-Konsole

In diesem Abschnitt wird erklärt, wie Sie das Kennwort für den JMX-Benutzer verschlüsseln. Das verschlüsselte Kennwort wird in der Datei **DataFlowProbe.properties** gespeichert. Benutzer müssen sich für den Zugriff auf die JMX-Konsole anmelden.

1. **Erstellen der verschlüsselten Form eines Kennworts (AES, 192 Bit-Schlüssel)**

   a. Rufen Sie die JMX-Konsole der Data Flow Probe auf. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://<Name oder IP-Adresse des Data Flow Probe-Computers>:1977**. Wenn Sie die Data Flow Probe lokal ausführen, geben Sie **http://localhost:1977** ein.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

   > **Hinweis:** Wenn Sie keinen Benutzer erstellt haben, melden Sie sich mit dem Standardbenutzernamen sysadmin und dem Standardkennwort sysadmin an.

   b. Suchen Sie den Service **Type=MainProbe** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.

   c. Suchen Sie den Vorgang **getEncryptedKeyPassword**.

   d. Geben Sie im Feld **Key Password** das zu verschlüsselnde Kennwort ein.

   e. Rufen Sie den Vorgang über die Schaltfläche **getEncryptedKeyPassword** auf.

   Durch diesen Aufruf wird eine verschlüsselte Kennwortzeichenfolge erstellt. Beispiel:

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

2. **Anhalten der Data Flow Probe**

   Start > Alle Programme > HP UCMDB > Data Flow Probe anhalten

3. **Hinzufügen des verschlüsselten Kennworts**

Fügen Sie das verschlüsselte Kennwort zur folgenden Eigenschaft in der Datei **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** hinzu.

appilog.agent.Probe.JMX.BasicAuth.Pwd

Beispiel:

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

Hinweis: Zum Deaktivieren der Authentifizierung lassen Sie diese Felder leer. In diesem Fall können Benutzer die Hauptseite der Probe-JMX-Konsole ohne Authentifizierung aufrufen.

4. **Starten der Data Flow Probe**

   Start > Alle Programme > HP UCMDB > Data Flow Probe starten

   Testen Sie das Ergebnis in einem Webbrowser.

Festlegen des Kennworts für "UpLoadScanFile"

In diesem Abschnitt wird beschrieben, wie Sie das Kennwort für **UpLoadScanFile** zum Speichern von Offsite-Scandateien festlegen. Das verschlüsselte Kennwort wird in der Datei **DataFlowProbe.properties** gespeichert. Benutzer müssen sich für den Zugriff auf die JMX-Konsole anmelden.

1. **Erstellen der verschlüsselten Form eines Kennworts (AES, 192 Bit-Schlüssel)**

   a. Rufen Sie die JMX-Konsole der Data Flow Probe auf. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://<Name oder IP-Adresse des Data Flow Probe-Computers>:1977**. Wenn Sie die Data Flow Probe lokal ausführen, geben Sie **http://localhost:1977** ein.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

   Hinweis: Wenn Sie keinen Benutzer erstellt haben, melden Sie sich mit dem Standardbenutzernamen sysadmin und dem Standardkennwort sysadmin an.

   b. Suchen Sie den Service **Type=MainProbe** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.

   c. Suchen Sie den Vorgang **getEncryptedKeyPassword**.

   d. Geben Sie im Feld **Key Password** das zu verschlüsselnde Kennwort ein.

   e. Rufen Sie den Vorgang über die Schaltfläche **getEncryptedKeyPassword** auf.

   Durch diesen Aufruf wird eine verschlüsselte Kennwortzeichenfolge erstellt. Beispiel:

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

2. **Anhalten der Data Flow Probe**

   Start > Alle Programme > HP UCMDB > Data Flow Probe anhalten

3. **Hinzufügen des verschlüsselten Kennworts**

   Fügen Sie das verschlüsselte Kennwort zur folgenden Eigenschaft in der Datei **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** hinzu.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Beispiel:

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

4. **Starten der Data Flow Probe**

   Start > Alle Programme > HP UCMDB > Data Flow Probe starten

   Testen Sie das Ergebnis in einem Webbrowser.

Remotezugriff auf den MySQL-Server

In diesem Abschnitt wird beschrieben, wie Sie den Zugriff auf das MySQL Data Flow Probe-Konto von Remotecomputern aus zulassen/einschränken.

Hinweis:

- Standardmäßig ist der Zugriff eingeschränkt.
- Es ist nicht möglich, von Remotecomputern aus auf das MySQL-Stammkonto zuzugreifen.

So lassen Sie den MySQL-Zugriff zu:

1. Führen Sie das folgende Skript im Eingabeaufforderungsfenster aus:

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

2. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für das MySQL-Stammkonto als erstes Argument ein. (Dieses Kennwort ist identisch mit dem Kennwort, das bei der Installation der Probe eingegeben wurde).

So schränken Sie den MySQL-Zugriff ein:

1. Führen Sie das folgende Skript im Eingabeaufforderungsfenster aus:

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

2. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für das MySQL-Stammkonto als erstes Argument ein. (Dieses Kennwort ist identisch mit dem Kennwort, das bei der Installation der Probe eingegeben wurde).

Aktivieren von SSL zwischen UCMDB Server und Data Flow Probe mit gegenseitiger Authentifizierung

Sie können sowohl für die Data Flow Probe als auch für den UCMDB-Server Authentifizierung mit Zertifikaten einrichten. Das Zertifikat für jede Komponente wird gesendet und authentifiziert, bevor die Verbindung hergestellt wird.

Hinweis: Die folgende Methode zum Aktivieren von SSL auf der Data Flow Probe mit gegenseitiger Authentifizierung ist die sicherste Methode und daher der empfohlene Kommunikationsmodus. Diese Methode ersetzt die Prozedur für die Standardauthentifizierung.

Dieser Abschnitt umfasst die folgenden Themen:

Übersicht

UCMDB unterstützt die folgenden Kommunikationsmodi zwischen dem UCMDB Server und der Data Flow Probe:

- **Serverauthentifizierung.** Dieser Modus verwendet SSL und die Probe authentifiziert das UCMDB Server-Zertifikat. Weitere Informationen finden Sie unter "Aktivieren von SSL mit Serverauthentifizierung (unidirektional)" auf der nächsten Seite.
- **Gegenseitige Authentifizierung.** Dieser Modus verwendet SSL und ermöglicht sowohl die Serverauthentifizierung durch die Probe als auch die Clientauthentifizierung durch den Server. Weitere Informationen finden Sie unter "Aktivieren der gegenseitigen (wechselseitigen) Zertifikatsauthentifizierung" auf Seite 73.
- **Standard-HTTP.** Keine SSL-Kommunikation. Dies ist der Standardmodus und die Data Flow Probe-Komponente in UCMDB erfordert keine Zertifikate. Die Data Flow Probe kommuniziert mit dem Server über das HTTP-Standardprotokoll.

Hinweis: Discovery kann keine Zertifikatsketten verwenden, wenn mit SSL gearbeitet wird. Wenn Sie Zertifikatsketten verwenden, sollten Sie daher ein selbstsigniertes Zertifikat generieren, damit die Data Flow Probe mit dem UCMDB-Server kommunizieren kann.

Key Stores und Trust Stores

Der UCMDB Server und die Data Flow Probe nutzen Key Stores und Trust Stores:

- **Key Store.** Eine Datei mit Schlüsseleinträgen (ein Zertifikat und ein übereinstimmender privater Schlüssel).
- **Trust Store.** Eine Datei mit Zertifikaten, die zum Prüfen eines Remote-Host verwendet werden (z. B. muss der Trust Store der Data Flow Probe bei der Nutzung von Serverauthentifizierung das UCMDB Server-Zertifikat enthalten).

Einschränkung bei der gegenseitigen Authentifizierung

Der Key Store der Data Flow Probe (wie in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties** definiert) darf nur einen einzigen Schlüsseleintrag enthalten.

Aktivieren von SSL mit Serverauthentifizierung (unidirektional)

Dieser Modus verwendet SSL und die Probe authentifiziert das Server-Zertifikat.

Diese Aufgabe umfasst folgende Themen:

- "Voraussetzungen" oben
- "Konfigurieren von UCMDB Server" oben
- "Konfigurieren von Data Flow Probe" auf Seite 73
- "Neustarten der Computer" auf Seite 73

Voraussetzungen

1. Stellen Sie sicher, dass sowohl UCMDB als auch die Data Flow Probe ausgeführt werden.

   Hinweis: Wenn die Probe im separaten Modus installiert wurde, beziehen sich diese Anweisungen auf das Probe Gateway.

2. Sollten UCMDB oder die Data Flow Probe nicht in den Standardordnern installiert sein, notieren Sie sich die tatsächlichen Speicherorte und ändern Sie die Befehle entsprechend.

Konfigurieren von UCMDB Server

1. **Exportieren des UCMDB-Zertifikats**

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <Key Store-Alias> -keystore <Key Store-Dateipfad> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   Dabei gilt:

   - **Key Store-Alias** ist der Name des Key Store.
   - **Key Store-Dateipfad** ist die vollständige Pfadangabe des Speicherorts der Key Store-Datei.

Verwenden Sie beispielsweise für den vordefinierten server.keystore den folgenden Befehl:

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

b. Geben Sie das Schlüsselspeicherkennwort ein. Für den vordefinierten Key Store ist das Kennwort beispielsweise **hppass**.

c. Prüfen Sie, ob das Zertifikat im folgenden Verzeichnis erstellt wurde: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Härten Sie den Data Flow Probe-Connector in UCMDB.**

a. Rufen Sie die UCMDB-JMX-Konsole auf: Geben Sie folgende URL im Browser ein: **http://<Name oder IP-Adresse des UCMDB-Computers>:8080/jmx-console**. Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

b. Wählen Sie den folgenden Service aus: **Ports Management Services**.

c. Rufen Sie die Methode **PortsDetails** auf und notieren Sie sich die Port-Nummer für HTTPS. (Standardeinstellung: 8443). Stellen Sie sicher, dass in der Spalte **Ist aktiviert** der Wert **True** eingetragen ist.

d. Wechseln Sie zurück zu **Ports Management Services**.

e. Um den Data Flow Probe-Connector dem Modus mit Serverauthentifizierung zuzuordnen, rufen Sie die Methode **mapComponentToConnectors** mit den folgenden Parametern auf:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Alle anderen Kennzeichen**: false

Die folgende Meldung wird angezeigt:

Operation succeeded. Component mam-collectors is now mapped to: HTTPS ports.

f. Wechseln Sie zurück zu **Ports Management Services**.

g. Um den Confidential Manager-Connector dem Modus mit Serverauthentifizierung zuzuordnen, rufen Sie die Methode **mapComponentToConnectors** mit den folgenden Parametern auf:

- **componentName**: cm
- **isHTTPS**: true
- **Alle anderen Kennzeichen**: false

Die folgende Meldung wird angezeigt:

Operation succeeded. Component cm is now mapped to: HTTPS ports.

3. **Kopieren Sie das UCMDB-Zertifikat auf jeden Probe-Computer.**

   Kopieren Sie die Zertifikatsdatei **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** vom UCMDB Servercomputer auf jedem Data Flow Probe-Computer in den folgenden Ordner: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Konfigurieren von Data Flow Probe

Hinweis: Sie müssen jeden Data Flow Probe-Computer konfigurieren.

1. **Importieren Sie die Datei server.cert, die nach den Anweisungen von** "Exportieren des UCMDB-Zertifikats" auf Seite 71 **erstellt wurde, in den Trust Store der Probe.**

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

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

   b. Geben Sie das Key Store-Kennwort ein: logomania.

   c. Geben Sie auf die Frage, ob Sie diesem Zertifikat vertrauen, **y** ein und drücken Sie dann die **Eingabetaste**.

   Die folgende Meldung wird angezeigt:

   Das Zertifikat wurde zum Key Store hinzugefügt.

2. **Öffnen Sie die Datei DiscoveryProbe.properties. Sie befindet sich im Verzeichnis C:\HP\UCMDB\DataFlowProbe\conf**

   a. Aktualisieren Sie die Eigenschaft **appilog.agent.probe.protocol** in **HTTPS**.

   b. Aktualisieren Sie den Wert der Eigenschaft **serverPortHttps** auf die relevante Portnummer. (Verwenden Sie die Port-Nummer aus Schritt 2c unter "Konfigurieren von UCMDB Server" auf Seite 71.)

Neustarten der Computer

Starten Sie sowohl den UCMDB Server, als auch die Probe-Computer neu.

Aktivieren der gegenseitigen (wechselseitigen) Zertifikatsauthentifizierung

Dieser Modus verwendet SSL und ermöglicht sowohl die Serverauthentifizierung durch die Probe als auch die Clientauthentifizierung durch den Server. Sowohl der Server als auch die Probe senden ihre Zertifikate zur Authentifizierung an die andere Entität.

Diese Aufgabe umfasst folgende Themen:

Voraussetzungen

1. Stellen Sie sicher, dass sowohl UCMDB als auch die Data Flow Probe ausgeführt werden.

   Hinweis: Wenn die Probe im separaten Modus installiert wurde, beziehen sich diese Anweisungen auf das Probe Gateway.

2. Sollten UCMDB oder die Data Flow Probe nicht in den Standardordnern installiert sein, notieren Sie sich die tatsächlichen Speicherorte und ändern Sie die Befehle entsprechen.

Anfängliche UCMDB Server-Konfiguration

1. **Exportieren des UCMDB-Zertifikats**

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <Key Store-Alias> -keystore <Key Store-Dateipfad> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   Dabei gilt:

   - **Key Store-Alias** ist der Name des Key Store.
   - **Key Store-Dateipfad** ist die vollständige Pfadangabe des Speicherorts der Key Store-Datei.

   Verwenden Sie beispielsweise für den vordefinierten server.keystore den folgenden Befehl:

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

   b. Geben Sie das Schlüsselspeicherkennwort ein. Für den vordefinierten Key Store ist das Kennwort beispielsweise **hppass**.

   c. Prüfen Sie, ob das Zertifikat im folgenden Verzeichnis erstellt wurde: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Härten Sie den Data Flow Probe-Connector in UCMDB.**

   a. Rufen Sie die UCMDB-JMX-Konsole auf: Geben Sie folgende URL im Browser ein: **http://<Name oder IP-Adresse des UCMDB-Computers>:8080/jmx-console**. Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

b. Wählen Sie den folgenden Service aus: **Ports Management Services**.

c. Rufen Sie die Methode **PortsDetails** auf und notieren Sie sich die Port-Nummer für HTTPS mit Client-Authentifizierung. (Standardeinstellung: 8444). Stellen Sie sicher, dass in der Spalte **Ist aktiviert** der Wert **True** eingetragen ist.

d. Wechseln Sie zurück zu **Ports Management Services**.

e. Um den Data Flow Probe-Connector dem Modus mit gegenseitiger Authentifizierung zuzuordnen, rufen Sie die Methode **mapComponentToConnectors** mit den folgenden Parametern auf:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Alle anderen Kennzeichen**: false

Die folgende Meldung wird angezeigt:

Operation succeeded. Component mam-collectors is now mapped to: HTTPS_CLIENT_AUTH ports.

f. Wechseln Sie zurück zu **Ports Management Services**.

g. Um den Confidential Manager-Connector dem Modus mit gegenseitiger Authentifizierung zuzuordnen, rufen Sie die Methode **mapComponentToConnectors** mit den folgenden Parametern auf:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Alle anderen Kennzeichen**: false

Die folgende Meldung wird angezeigt:

Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.

3. **Kopieren Sie das UCMDB-Zertifikat auf jeden Probe-Computer.**

Kopieren Sie die Zertifikatsdatei **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** vom UCMDB Servercomputer auf jedem Data Flow Probe-Computer in den folgenden Ordner: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Konfigurieren von Data Flow Probe

Hinweis: Sie müssen jeden Data Flow Probe-Computer konfigurieren.

1. I**mportieren Sie die Datei server.cert, die nach den Anweisungen von "Exportieren des UCMDB-Zertifikats" auf Seite 1 erstellt wurde, in den Trust Store der Probe.**

a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

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

b. Geben Sie das Key Store-Kennwort ein: logomania.

c. Geben Sie auf die Frage, ob Sie diesem Zertifikat vertrauen, **y** ein und drücken Sie dann die **Eingabetaste**.

Die folgende Meldung wird angezeigt:

Das Zertifikat wurde zum Keystore hinzugefügt.

2. **Erstellen Sie eine neue Datei "client.keystore".**

a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

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

Dabei ist **probeName** der eindeutige Alias der Data Flow Probe.

Hinweis: Stellen Sie sicher, dass der Alias eindeutig ist, und verwenden Sie die Probenamen-ID, die der Probe bei der Definition zugewiesen wurde.

b. Geben Sie für den Key Store ein Kennwort mit mindestens 6 Zeichen ein und notieren Sie es.

c. Geben Sie das Kennwort erneut ein, um es zu bestätigen.

d. Drücken Sie die Eingabetaste und beantworten Sie jede der folgenden Fragen:

Wie lauten Ihr Vor- und Ihr Nachname? [Unbekannt]:

Wie lautet der Name Ihrer Organisationseinheit?[Unbekannt]:

Wie lautet der Name Ihrer Organisation?[Unbekannt]:

Wie lautet der Name Ihrer Stadt oder Ihres Ortes?[Unbekannt]:

Wie lautet der Name Ihres Bundesland?[Unbekannt]:

Wie lautet der zweistellige Ländercode für diese Einheit?[Unbekannt]:

e. Geben Sie **Ja** ein, wenn Sie Folgendes gefragt werden: **Ist CN=Unbekannt, OU=Unbekannt, O=Unbekannt, L=Unbekannt, ST=Unbekannt, C=Unbekannt richtig?**

f. Drücken Sie die Eingabetaste und beantworten Sie die folgende Frage:

Geben Sie das Schlüsselkennwort für <probekey> ein (EINGABETASTE, falls es mit dem Kennwort für Key Store identisch ist):

g. Stellen Sie sicher, dass die Datei im folgenden Ordner erstellt wurde und dass sie größer als 0 ist: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Exportieren des neuen Clientzertifikats**

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

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

   b. Geben Sie auf Aufforderung das Schlüsselspeicherkennwort ein. (Das ist das Kennwort aus dem oben genannten Schritt 2b.)

   Die folgende Meldung wird angezeigt:

   Zertifikat gespeichert in der Datei <C:\hp\UCMDB\DataFlowProbe\conf\security\<probeName>.cert>

4. **Öffnen Sie die Datei DiscoveryProbe.properties. Sie befindet sich im Verzeichnis C:\HP\UCMDB\DataFlowProbe\conf**

   a. Aktualisieren Sie die Eigenschaft **appilog.agent.probe.protocol** in **HTTPS**.

   b. Aktualisieren Sie den Wert der Eigenschaft **serverPortHttps** auf die relevante Portnummer. (Verwenden Sie die Port-Nummer aus Schritt 2c unter "Anfängliche UCMDB Server-Konfiguration" auf Seite 74.)

5. **Öffnen Sie die Datei ssl.properties. Sie befindet sich im Verzeichnis C:\HP\UCMDB\DataFlowProbe\conf\security**

   a. Aktualisieren Sie den Wert der Eigenschaft **javax.net.ssl.keyStore** auf **client.keystore**.

   b. Verschlüsseln Sie das Kennwort aus dem oben genannten Schritt 2b:

      i. Starten Sie die Data Flow Probe (oder stellen Sie sicher, dass sie bereits ausgeführt wird).

      ii. Rufen Sie die JMX-Konsole der Probe auf: Wechseln Sie zu: **http://<Probenhostname>:1977**

      Wenn die Probe lokal ausgeführt wird, wechseln Sie zum Beispiel zu: **http://localhost:1977**.

      iii. Klicken Sie auf den Link **type=MainProbe**.

      iv. Führen Sie einen Bildlauf nach unten zu dem Vorgang **getEncryptedKeyPassword** durch.

      v. Geben Sie das Kennwort in das Feld **Key Password** ein.

      vi. Klicken Sie auf die Schaltfläche **getEncryptedKeyPassword**.

   c. Kopieren Sie das verschlüsselte Kennwort und fügen Sie es als Wert der Eigenschaft

javax.net.ssl.keyStorePassword ein, um sie zu aktualisieren.

> **Hinweis:** Zahlen werden durch Kommas abgetrennt. Beispiel: -20,50,34,-40,-50.)

6. **Kopieren Sie das Probe-Zertifikat auf den UCMBD-Computer.**

   Kopieren Sie die Datei **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** von dem Data Flow Probe-Computer in das Verzeichnis **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert** des UCMDB-Computers.

Weitere UCMDB Server-Konfiguration

1. **Fügen Sie jedes Probe-Zertifikat dem Trust Store von UCMDB hinzu.**

   > **Hinweis:** Für jedes Probe-Zertifikat müssen Sie die folgenden Schritte abschließen.

   a. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus:

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

   b. Geben Sie das Schlüsselspeicherkennwort ein. Für den vordefinierten Key Store ist das Kennwort beispielsweise **hppass**.

   c. Geben Sie auf die Frage, ob Sie diesem Zertifikat vertrauen, **y** ein und drücken Sie dann die **Eingabetaste**.

   Die folgende Meldung wird angezeigt:

   > **Das Zertifikat wurde zum Key Store hinzugefügt.**

Neustarten der Computer

Starten Sie sowohl den UCMDB Server, als auch die Probe-Computer neu.

Steuern des Speicherorts der domainScopeDocument-Datei

Im Dateisystem der Probe befinden sich (standardmäßig) sowohl der Verschlüsselungsschlüssel als auch die Datei **domainScopeDocument**. Nach jedem Start ruft die Probe die Datei **domainScopeDocument** vom Server ab und speichert sie in ihrem Dateisystem. Um zu verhindern, dass unbefugte Benutzer diese Anmeldeinformationen erhalten, können Sie die Probe so konfigurieren, dass die Datei **domainScopeDocument** im Arbeitsspeicher der Probe und nicht in ihrem Dateisystem gespeichert wird.

So steuern Sie den Speicherort der Datei "domainScopeDocument":

1. Öffnen Sie **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** und ändern Sie

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

   in

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

   Nun ist die Datei **domainScopeDocument** nicht mehr im Ordner **serverData** von Probe Gateway und Probe Manager enthalten.

   Weitere Informationen zur Verwendung der Datei **domainScopeDocument** zum Härten von DFM finden Sie unter "Verwalten der Data Flow-Anmeldeinformationen" auf Seite 43.

2. Starten Sie die Probe neu.

Erzeugen eines Key Store für die Data Flow Probe

1. Führen Sie auf dem Probe-Computer den folgenden Befehl aus:

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

2. Geben Sie ein Kennwort für den neuen Key Store ein.
3. Geben Sie Ihre Informationen ein, wenn Sie dazu aufgefordert werden.
4. Auf die Frage **Is CN=… C=… Correct?** geben Sie **yes** ein und drücken die **Eingabetaste**.
5. Drücken Sie erneut die **Eingabetaste**, um das Key Store-Kennwort als Schlüsselkennwort zu übernehmen.
6. Prüfen Sie, ob **client.keystore** im folgenden Verzeichnis erstellt wurde: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Verschlüsseln der Kennwörter für den Key Store und Trust Store der Probe

Die Kennwörter für den Key Store und Trust Store der Probe werden in verschlüsselter Form in der Datei **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties** gespeichert. In dieser Prozedur wird das Verschlüsseln des Kennworts erklärt.

1. Starten Sie die Data Flow Probe (oder stellen Sie sicher, dass sie bereits ausgeführt wird).
2. Rufen Sie die JMX-Konsole der Data Flow Probe auf: Öffnen Sie einen Browser und geben Sie die folgende Adresse ein: **http://<Name oder IP-Adresse des Data Flow Probe-Computers>:1977**. Wenn Sie die Data Flow Probe lokal ausführen, geben Sie **http://localhost:1977** ein.

   Hinweis: Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden. Wenn Sie keinen Benutzer erstellt haben, melden Sie sich mit dem

Standardbenutzernamen sysadmin und dem Standardkennwort sysadmin an.

3. Suchen Sie den Service **Type=MainProbe** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
4. Suchen Sie den Vorgang **getEncryptedKeyPassword**.
5. Geben Sie Ihr Key Store- oder Trust Store-Kennwort im Feld **Key Password** ein und rufen Sie den Vorgang auf, indem Sie auf **getEncryptedKeyPassword** klicken.
6. Durch diesen Aufruf wird eine verschlüsselte Kennwortzeichenfolge erstellt. Beispiel:

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

7. Kopieren Sie das verschlüsselte Kennwort und fügen Sie es in die Zeile für den Key Store oder Trust Store in der folgenden Datei ein:
   C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.

Standard-Key Store und -Trust Store von Server und Data Flow Probe

Dieser Abschnitt umfasst die folgenden Themen:

UCMDB-Server

Die Dateien befinden sich im folgenden Verzeichnis:
C:\HP\UCMDB\UCMDBServer\conf\security.

Entität	Dateiname/Ausdruck	Kennwort/Ausdruck	Alias
Server-Key Store	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Server-Trust Store	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (Standard-Trust-Eintrag)
Client-Key Store	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

Die Dateien befinden sich im folgenden Verzeichnis:
C:\HP\UCMDB\DataFlowProbe\conf\security.

Entität	Dateiname/Ausdruck	Kennwort/Ausdruck	Alias
Probe-Key Store	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
Data Flow Probe verwendet den Key Store **cKeyStoreFile** während der gegenseitigen Authentifizierung als Standard-Key Store. Dieser Client-Key Store ist Teil der UCMDB-Installation.			
Probe-Trust Store	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (Standard-Trust-Eintrag)
Das Kennwort **cKeyStorePass** ist das Standard-Kennwort für **cKeyStoreFile**.			

Kapitel 6

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

Dieses Kapitel umfasst folgende 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.

- **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**

  Bei der Funktion für mehrere Domänen müssen für alle Applikationen, die Teil einer LW-SSO-Integration sind, die **trustedHosts**-Einstellungen konfiguriert 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 werden, sollte für die Hostapplikation die richtige Domäne im **lwsso**-Element der Konfiguration festgelegt werden.

Systemanforderungen für LW-SSO

Applikation	Version	Kommentare
Java	1.5 und höher	
HTTP-Servlets-API	2.1 und höher	
Internet Explorer	6.0 und höher	Der Browser sollte HTTP-Sitzungscookies und die HTTP-302-Weiterleitungsfunktion unterstützen.
Firefox	2.0 und höher	Der Browser sollte HTTP-Sitzungscookies und die HTTP-302-Weiterleitungsfunktion unterstützen.
JBoss-Authentifizierung	JBoss 4.0.3 JBoss 4.3.0	
Tomcat-Authentifizierung	Tomcat 5.0.28 im eigenständigen Modus Tomcat 5.5.20 im eigenständigen Modus	
Acegi-Authentifizierung	Acegi 0.9.0 Acegi 1.0.4	
Webservice-Engines	Axis 1 - 1,4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

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 **initString**-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 der 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 eine Applikation, die einen gemeinsamen **initString**-Parameter verwendet, sich an einem nicht vertrauenswürdigen Speicherort befindet oder von diesem aus zugänglich ist.
- **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 Applikation (AppA) anmeldet und auf eine zweite Applikation (AppB) zugreift, die Benutzercontainer oder Applikationsauthentifizierung verwendet, der Benutzer durch den Fehler bei der Zuordnung gezwungen werden, sich manuell bei AppB anzumelden und einen Benutzernamen einzugeben. Wenn der Benutzer einen anderen Benutzernamen verwendet als den, mit dem er sich bei AppA angemeldet hat, kann es zu dem folgenden Verhalten kommen: Wenn der Benutzer im Anschluss auf eine dritte Applikation (AppC) von AppA oder AppB zugreift, dann erfolgt der Zugriff unter Verwendung der Benutzernamen die für die Anmeldung bei AppA bzw. AppB verwendet wurden.

- **Identitätsmanager**. Da sie für Authentifizierungszwecke verwendet werden, müssen alle ungeschützten Ressourcen im Identitätsmanager mit der **nonsecureURLs**-Einstellung in der LW-SSO-Konfigurationsdatei konfiguriert werden.
- **LW-SSO-Demomodus.**
  - Der Demomodus sollte nur für Vorführzwecke verwendet werden.
  - Der Demomodus sollte nur in unsicheren Netzwerken verwendet werden.
  - Der Demomodus darf nicht in der Produktionsumgebung verwendet werden. Es sollte keine Kombination aus Demo- und Produktionsmodus verwendet werden.

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden die bekannten Fehler und Einschränkungen beschrieben, die bei der Verwendung der LW-SSO-Authentifizierung auftreten können.

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 ohne den vollqualifizierten Domänennamen (FQDN) im Anmelde-URL auf die Applikation 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 Applikation 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`
  - Das Verhalten von Drittanbieter-Cookies in Internet Explorer:

    Microsoft Internet Explorer 6 enthält ein Modul, das das P3P-Projekt (Platform for Privacy Preferences) unterstützt. Dies bedeutet, dass Cookies von einer Drittanbieterdomäne standardmäßig in der Internet-Sicherheitszone blockiert werden. Sitzungscookies werden von Internet Explorer ebenfalls als Drittanbieter-Cookies betrachtet und daher blockiert. Dies führt dazu, dass LW-SSO nicht mehr ausgeführt wird. Weitere Informationen finden Sie unter `http://support.microsoft.com/kb/323752/en-us`.

Um dieses Problem zu beheben, fügen Sie die gestartete Applikation (oder eine DNS-Untermenge wie *.meinedomäne.com) zur Intranetzone/Zone vertrauenswürdiger Sites auf Ihrem Computer hinzu (wählen Sie in Microsoft Internet Explorer die Optionen **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites > Erweitert** aus). Die Cookies werden daraufhin akzeptiert.

Achtung: Das LW-SSO-Sitzungscookie ist nur eines der Cookies, die von der blockierten Drittanbieterapplikation verwendet werden.

- **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.
- **Demomodus.** Im Demomodus unterstützt LW-SSO zwar Links von einer Applikation auf eine andere, aber nicht die Eingabe eines URL in einem Browserfenster, da in diesem Fall die HTTP-Referrerkopfzeile fehlt.

Kapitel 7

Authentifizierung bei der Anmeldung in HP Universal CMDB

Dieses Kapitel umfasst folgende Themen:

Einrichten einer Authentifizierungsmethode

Eine Authentifizierung können Sie wie folgt ausführen:

- **Über den internen HP Universal CMDB-Service.**
- **Über das Lightweight Directory Access Protocol (LDAP).** Sie können einen dedizierten externen LDAP-Server zum Speichern der Authentifizierungsinformationen verwenden, anstatt den internen HP Universal CMDB-Service zu nutzen. Der LDAP-Server muss sich im selben Subnet wie alle HP Universal CMDB Server befinden.

  Weitere Informationen zu LDAP finden Sie im Abschnitt über die LDAP-Zuordnung im *HP Universal CMDB – Verwaltungshandbuch*.

  Bei der Standardauthentifizierungsmethode wird der interne HP Universal CMDB-Service verwendet. Wenn Sie die Standardmethode nutzen, müssen Sie keine Änderungen im System vornehmen.

  Diese Optionen gelten für Anmeldungen über Webservices sowie über die Benutzeroberfläche.

- **Über LW-SSO.** HP Universal CMDB ist mit LW-SSO konfiguriert. Durch LW-SSO können Sie sich in HP Universal CMDB anmelden und automatisch auf andere konfigurierte Applikationen zugreifen, die in derselben Domäne ausgeführt werden, ohne dass Sie sich in diesen Applikationen anmelden müssen.

  Wenn die Unterstützung für LW-SSO-Authentifizierung aktiviert ist (sie ist standardmäßig deaktiviert), müssen Sie sicherstellen, dass für die anderen Applikationen in der Single Sign-On-Umgebung ebenfalls LW-SSO aktiviert ist und derselbe **initString**-Parameter verwendet wird.

Aktivieren der Anmeldung in HP Universal CMDB mit LW-SSO

Verwenden Sie zum Aktivieren von LW-SSO für HP Universal CMDB die folgende Prozedur:

1. Rufen Sie die JMX-Konsole auf, indem Sie in Ihrem Webbrowser die folgende Adresse eingeben: **http://<Servername>:8080/jmx-console,** wobei **<Servername>** für den Namen des Computers steht, auf dem HP Universal CMDB installiert ist.
2. Klicken Sie unter **UCMDB-UI** auf **name=LW-SSO Configuration**, um die Seite **Operations** zu öffnen.
3. Legen Sie mit der Methode **setInitString** die Init-Zeichenkette fest.
4. Legen Sie mit der Methode **setDomain** den Domänennamen des Computers fest, auf dem UCMDB installiert ist.
5. Rufen Sie die Methode **setEnabledForUI** mit dem Parameterwert **True** auf.
6. **Optional**. Wenn Sie die Funktion für mehrere Domänen nutzen möchten, wählen Sie die Methode **addTrustedDomains** aus, geben Sie die Domänenwerte ein und klicken Sie auf **Invoke**.
7. **Optional.** Wenn Sie mit einem Reverse-Proxy arbeiten möchten, wählen Sie die Methode **updateReverseProxy** aus, setzen Sie den Parameter **Is reverse proxy enabled** auf **True** und geben Sie einen URL für den Parameter **Reverse proxy full server URL** ein. Klicken Sie anschließend auf **Invoke**. Wenn Sie sowohl direkt als auch über einen Reverse-Proxy auf UCMDB zugreifen möchten, nehmen Sie die folgende zusätzliche Konfiguration vor: Wählen Sie die Methode **setReverseProxyIPs** aus, geben Sie die IP-Adresse für den Parameter **ip/s** des Reverse-Proxy ein und klicken Sie auf **Invoke**.
8. **Optional**. Wenn Sie über einen externen Authentifizierungspunkt auf UCMDB zugreifen möchten, wählen Sie die Methode **setValidationPointHandlerEnable** aus, setzen Sie den Parameter **Is validation point handler enabled** auf **True** und geben Sie den URL für den Authentifizierungspunkt in den Parameter **Authentication point server** ein. Klicken Sie anschließend auf **Invoke.**
9. Um die LW-SSO-Konfiguration so anzuzeigen, wie sie im Einstellungsmechanismus gespeichert ist, rufen Sie die Methode **retrieveConfigurationFromSettings** auf.
10. Um die tatsächlich geladene LW-SSO-Konfiguration anzuzeigen, rufen Sie die Methode **retrieveConfiguration** auf.

Hinweis: LW-SSO kann nicht über die Benutzeroberfläche aktiviert werden.

Einrichten einer sicheren Verbindung mit dem SSL-Protokoll

Da beim Anmeldeprozess vertrauliche Informationen zwischen HP Universal CMDB und dem LDAP-Server übertragen werden, sollten Sie diese Inhalte schützen. Dazu aktivieren Sie SSL-Kommunikation auf dem LDAP-Server und konfigurieren HP Universal CMDB für die Verwendung von SSL.

HP Universal CMDB unterstützt SSL mit Verwendung eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben wurde.

Die meisten LDAP-Server, einschließlich Active Directory, können einen sicheren Port für eine SSL-basierte Verbindung bereitstellen. Wenn Sie Active Directory mit einer privaten Zertifizierungsstelle verwenden, müssen Sie Ihre Zertifizierungsstelle zu den vertrauenswürdigen Zertifizierungsstellen in JRE hinzufügen.

Weitere Informationen zum Konfigurieren der HP Universal CMDB-Plattform für die Kommunikation über SSL finden Sie unter "Aktivieren der SSL-Kommunikation" auf Seite 18.

So fügen Sie eine Zertifizierungsstelle zu den vertrauenswürdigen Zertifizierungsstellen hinzu, um einen sicheren Port für eine SSL-basierte Verbindung bereitzustellen:

1. Exportieren Sie ein Zertifikat aus Ihrer Zertifizierungsstelle und importieren Sie es in die JVM, die HP Universal CMDB verwendet. Gehen Sie dabei wie folgt vor:

   a. Rufen Sie auf dem UCMDB Server-Computer den Ordner **UCMDBServer\bin\JRE\bin** auf.

   b. Führen Sie folgenden Befehl aus:

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

   Beispiel:

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

2. Wählen Sie die Kategorie **Verwaltung > Infrastructure Settings Manager > LDAP - Allgemein** aus.

   Hinweis: Diese Einstellungen können auch mit der JMX-Konsole konfiguriert werden. Weitere Informationen finden Sie unter "Konfigurieren der LDAP-Einstellungen über die JMX-Konsole" auf der nächsten Seite.

3. Suchen Sie die Einstellung **LDAP-Server-URL** und geben Sie den LDAP-URL-Wert im folgenden Format ein:

   ```
   ldaps://<LDAP-Host>[:<Port>]/[<Basis-DN>][??Umfang]
   ```

   Beispiel:

   ```
   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

   Achten Sie auf das **s** in **ldaps**.

4. Klicken Sie auf **Speichern**, um den neuen Wert zu speichern, oder auf **Standardeinstellung**, um den Eintrag durch den Standardwert (einen leeren URL) zu ersetzen.

Verwenden der JMX-Konsole zum Testen von LDAP-Verbindungen

In diesem Abschnitt wird eine Methode zum Testen der LDAP-Authentifizierungskonfiguration über die JMX-Konsole beschrieben.

1. Öffnen Sie den Browser und geben Sie die folgende Adresse ein: **http://<Servername>:8080/jmx-console,** wobei **<Servername>** für den Namen des Computers steht, auf dem HP Universal CMDB installiert ist.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

2. Klicken Sie unter **UCMDB** auf **UCMDB-UI:name=LDAP Settings**, um die Seite **Operations** zu öffnen.

3. Suchen Sie **testLDAPConnection**.

4. Geben Sie in das Feld **Value** für den Parameter **customer id** die Kunden-ID ein.

5. Klicken Sie auf **Invoke**.

   Auf der Seite **JMX MBEAN Operation Result** wird angegeben, ob die LDAP-Verbindung erfolgreich hergestellt wurde. Ist die Verbindung erfolgreich, werden auf der Seite auch die LDAP-Stammgruppen angezeigt.

Konfigurieren der LDAP-Einstellungen über die JMX-Konsole

In diesem Abschnitt wird beschrieben, wie Sie die LDAP-Authentifizierungseinstellungen über die JMX-Konsole konfigurieren.

So konfigurieren Sie LDAP-Authentifizierungseinstellungen:

1. Öffnen Sie den Browser und geben Sie die folgende Adresse ein: **http://<Servername>:8080/jmx-console,** wobei **<Servername>** für den Namen des Computers steht, auf dem HP Universal CMDB installiert ist.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

2. Klicken Sie unter **UCMDB** auf **UCMDB-UI:name=LDAP Settings**, um die Seite **Operations** zu öffnen.

3. Zum Anzeigen der derzeitigen LDAP-Authentifizierungseinstellungen suchen Sie die Methode **getLDAPSettings**. Klicken Sie auf **Invoke**. Eine Tabelle mit allen LDAP-Einstellungen und den zugehörigen Werten wird angezeigt.

4. Zum Ändern der Werte für die LDAP-Authentifizierungseinstellungen suchen Sie die Methode **configureLDAP**. Geben Sie die Werte für die betreffenden Einstellungen ein und klicken Sie auf **Invoke**. Auf der Seite **JMX MBEAN Operation Result** wird angegeben, ob die LDAP-

Authentifizierungseinstellungen erfolgreich aktualisiert wurden.

Hinweis: Wenn Sie für eine Einstellung keinen Wert eingeben, behält die Einstellung den derzeitigen Wert bei.

5. Nach dem Konfigurieren der LDAP-Einstellungen können Sie die Anmeldeinformationen der LDAP-Benutzer prüfen. Suchen Sie die Methode **verifyLDAPCredentials**. Geben Sie die Kunden-ID, den Benutzernamen und das Kennwort ein und klicken Sie auf **Invoke**. Auf der Seite **JMX MBEAN Operation Result** wird angegeben, ob die LDAP-Authentifizierung des Benutzers erfolgreich war.

Aktivieren und Definieren der LDAP-Authentifizierungsmethode

Sie können die LDAP-Authentifizierungsmethode für ein HP Universal CMDB-System aktivieren und definieren.

So aktivieren und definieren Sie die LDAP-Authentifizierungsmethode:

1. Wählen Sie die Kategorie **Verwaltung > Infrastructure Settings Manager > LDAP - Allgemein** aus.
2. Wählen Sie **LDAP-Server-URL** aus und geben Sie den LDAP-URL-Wert im folgenden Format ein:

   ldap://<LDAP-Host>[:<Port>]/[<Basis-DN>][??Umfang]

   Beispiel:

   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub

3. Wählen Sie die Kategorie **LDAP-Gruppendefinition** aus und geben Sie dann in der Einstellung **Gruppen-Basis-DN** den Distinguished Name (DN) der allgemeinen Gruppe ein.
4. Geben Sie in der Einstellung **Basis-DN der Stammgruppe** den Distinguished Name (DN) der Stammgruppe ein.
5. Wählen Sie die Kategorie **LDAP - Allgemein** aus und überprüfen Sie in der Einstellung **Benutzersynchronisierung aktivieren**, ob der Wert auf **True** festgelegt ist.
6. Wählen Sie die Kategorie **LDAP - Allgemeine Authentifizierung** aus und geben Sie in der Einstellung **Kennwort für Benutzer mit Suchberechtigung** das Kennwort ein.
7. Wählen Sie die Kategorie **LDAP-Optionen für Klassen und Attribute** aus, suchen Sie die Einstellung **Gruppenklassenobjekt** und tragen Sie den Objektklassennamen ein (**group** für Microsoft Active Directory und **groupOfUniqueNames** für Oracle Directory Server).
8. Suchen Sie die Einstellung **Gruppenmitgliedsattribut** und tragen Sie den Attributnamen ein (**member** für Microsoft Active Directory und **uniqueMember** für Oracle Directory Server).
9. Suchen Sie die Einstellung **Benutzerobjektklasse** und tragen Sie den Objektklassennamen

ein (**user** für Microsoft Active Directory und **inetOrgPerson** für Oracle Directory Server).

10. Suchen Sie die Einstellung **UUID-Attribut** und tragen Sie das eindeutige identifizierende Attribut für einen Benutzer in Ihrem Verzeichnisserver ein. Das Attribut muss in Ihrem Verzeichnisserver eindeutig sein. Wenn Sie beispielsweise SunOne/Oracle Directory Server verwenden, ist das UID-Attribut nicht eindeutig. Geben Sie in diesem Fall entweder die E-Mail-Adresse oder den Distinguished Name als eindeutiges Attribut an. Die Verwendung eines nicht eindeutigen Attributs in UCMDB kann bei der Anmeldung zu einem inkonsistenten Verhalten führen.
11. Speichern Sie die neuen Werte. Um einen Eintrag durch den Standardwert zu ersetzen, klicken Sie auf **Standardeinstellung**.
12. Wenn die Infrastruktureinstellung **Unterscheidung nach Groß-/Kleinschreibung bei der LDAP-Authentifizierung erzwingen** unter **LDAP - Allgemein** auf **True** gesetzt ist, wird bei der Authentifizierung zwischen Groß- und Kleinschreibung unterschieden.

    Achtung: Wird der Wert dieser Infrastruktureinstellung geändert, müssen alle externen Benutzer manuell vom UCMDB-Administrator gelöscht werden.
13. Ordnen Sie LDAP-Benutzergruppen zu UCMDB-Benutzergruppen zu. Weitere Informationen finden Sie unter "Authentifizierung bei der Anmeldung in HP Universal CMDB" auf Seite 88.
14. Wenn Sie einen Standardberechtigungssatz für Benutzer in einer LDAP-Gruppe definieren möchten, die keine Gruppenzuordnung aufweist, wählen Sie die Kategorie **LDAP - Allgemein** aus, suchen Sie die Einstellung **Automatisch zugewiesene Benutzergruppe** und geben Sie den Gruppennamen ein.

Das Standardprotokoll für die Kommunikation mit dem LDAP-Server lautet TCP, aber Sie können das Protokoll in SSL ändern. Weitere Informationen finden Sie unter "Einrichten einer sicheren Verbindung mit dem SSL-Protokoll" auf Seite 90.

Hinweis: Für jeden LDAP-Benutzer werden Vorname, Nachname und E-Mail-Adresse im lokalen Repository gespeichert. Wenn der Wert eines dieser auf dem LDAP-Server gespeicherten Parameter von dem Wert im lokalen Repository abweicht, werden die lokalen Werte bei jeder Anmeldung mit den Werten des LDAP-Servers überschrieben.

Abrufen der derzeitigen LW-SSO-Konfiguration in einer verteilten Umgebung

Wenn UCMDB in einer verteilten Umgebung integriert ist, beispielsweise in einer BSM-Bereitstellung, führen Sie die folgende Prozedur aus, um die derzeitige LW-SSO-Konfiguration auf dem Verarbeitungscomputer abzurufen.

So rufen Sie die derzeitige LW-SSO-Konfiguration ab:

1. Öffnen Sie einen Browser und geben Sie die folgende Adresse ein:
   `http://localhost.<Domänenname>:8080/jmx-console`

   Eventuell müssen Sie einen Benutzernamen und ein Kennwort eingeben.

2. Suchen Sie **UCMDB:service=Security Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.
3. Suchen Sie den Vorgang **retrieveLWSSOConfiguration**.
4. Klicken Sie auf **Invoke**, um die Konfiguration abzurufen.

Kapitel 8

Confidential Manager

Dieses Kapitel umfasst folgende Themen:

Confidential Manager – Übersicht

Der Confidential Manager bildet das Framework, mit dem das Problem der Verwaltung und Verteilung sensibler Daten für HP Universal CMDB und andere Produkte von HP Software gelöst wird.

Confidential Manager besteht aus zwei Hauptkomponenten: dem Client und dem Server. Diese zwei Komponenten sind für eine sichere Datenübertragung verantwortlich.

- Beim Confidential Manager-Client handelt es sich um eine Bibliothek, die von Applikationen für den Zugriff auf sensible Daten verwendet wird.
- Der Confidential Manager-Server erhält Anfragen von Confidential Manager-Clients oder von Drittanbieterclients und führt die erforderlichen Aufgaben aus. Der Confidential Manager-Server ist für das sichere Speichern der Daten verantwortlich.

Confidential Manager verschlüsselt Anmeldeinformationen während der Übertragung, im Client-Cache, im persistenten Speicher und im Arbeitsspeicher. Confidential Manager verwendet symmetrische Kryptographie für die Übertragung von Anmeldeinformationen zwischen dem Confidential Manager-Client und dem Confidential Manager-Server und nutzt dabei einen gemeinsamen geheimen Schlüssel. Confidential Manager verwendet verschiedene geheime Schlüssel zur Verschlüsselung des Cache, des persistenten Speichers und der Übertragung, je nach Konfiguration.

Ausführliche Richtlinien zum Verwalten der Verschlüsselung von Anmeldeinformationen auf der Data Flow Probe finden Sie unter "Verwalten der Data Flow-Anmeldeinformationen" auf Seite 43.

Sicherheitsaspekte

- Sie können die folgenden Schlüsselgrößen für den Sicherheitsalgorithmus verwenden: 128, 192 und 256 Bit. Mit dem kleineren Schlüssel wird der Algorithmus schneller ausgeführt, ist aber nicht so sicher. Die Sicherheit des 128-Bit-Schlüssels reicht in den meisten Fällen aus.

- Um die Systemsicherheit zu erhöhen, verwenden Sie MAC: Legen Sie für **useMacWithCrypto** den Wert **true** fest. Weitere Informationen finden Sie unter "Verschlüsselungseigenschaften" auf Seite 98.
- Um Provider für hohe Kundensicherheit zu nutzen, können Sie den JCE-Modus verwenden.

Konfigurieren von HP Universal CMDB Server

Wenn Sie mit HP Universal CMDB arbeiten, sollten Sie den geheimen Schlüssel und die Krypto-Eigenschaften der Verschlüsselung mit den folgenden JMX-Methoden konfigurieren:

1. Starten Sie auf dem HP Universal CMDB Server-Computer den Webbrowser und geben Sie die folgende Serveradresse ein: **http://<Hostname oder IP-Adresse des UCMDB-Servers>:8080/jmx-console**.

   Eventuell müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden.

2. Klicken Sie unter **UCMDB** auf **UCMDB:service=Security Services**, um die Seite **Operations** zu öffnen.

3. Zum Abrufen der derzeitigen Konfiguration suchen Sie den Vorgang **CMGetConfiguration**.

   Klicken Sie auf **Invoke**, um die XML-Datei mit der Konfiguration des Confidential Manager-Servers anzuzeigen.

4. Um die Konfiguration zu ändern, kopieren Sie die im vorherigen Schritt aufgerufene XML-Datei in einen Texteditor. Nehmen Sie die Änderungen gemäß der Tabelle unter "Verschlüsselungseigenschaften" auf Seite 98 vor.

   Suchen Sie den Vorgang **CMSetConfiguration**. Kopieren Sie die aktualisierte Konfiguration in das Feld **Value** und klicken Sie auf **Invoke**. Die neue Konfiguration wird auf den UCMDB Server geschrieben.

5. Wenn Sie Benutzer für Autorisierung und Replizierung zum Confidential Manager hinzufügen möchten, suchen Sie den Vorgang **CMAddUser**. Dieser Prozess eignet sich auch für den Replizierungsvorgang. Bei der Replizierung sollte der Server-Slave über einen privilegierten Benutzer mit dem Server-Master kommunizieren.

   - **username**. Der Benutzername.
   - **customer.** Die Standardeinstellung lautet ALL_CUSTOMERS.
   - **resource.** Der Ressourcenname. In der Standardeinstellung ist der Stammordner ausgewählt.
   - **permission.** Wählen Sie zwischen ALL_PERMISSIONS, CREATE, READ, UPDATE und DELETE aus. In der Standardeinstellung sind alle Berechtigungen ausgewählt.

   Klicken Sie auf **Invoke**.

6. Starten Sie HP Universal CMDB bei Bedarf neu.

   Hinweis: In den meisten Fällen muss der Server nicht neu gestartet werden. Der Server muss möglicherweise neu gestartet werden, wenn Sie eine der folgenden Ressourcen ändern:

- Speichertyp
- Name oder Spaltennamen der Datenbanktabelle
- Ersteller der Datenbankverbindung
- Die Eigenschaften der Verbindung zur Datenbank (d. h. URL, Benutzer, Kennwort, Treiberklassenname)
- Datenbanktyp

Hinweis:

- Der UCMDB Server und seine Clients müssen dieselben Krypto-Eigenschaften für die Übertragung aufweisen. Werden diese Eigenschaften auf dem UCMDB Server geändert, müssen Sie sie auch auf allen Clients ändern. (Dies gilt nicht für die Data Flow Probe, da sie durch denselben Prozess ausgeführt wird wie der UCMDB-Server und daher keine Krypto-Konfiguration für die Übertragung erfordert.)
- Die Confidential Manager-Replizierung ist standardmäßig nicht konfiguriert, kann aber bei Bedarf konfiguriert werden.
- Wird die Confidential Manager-Replizierung aktiviert und die Übertragungseinstellung **initString** oder eine andere Krypto-Eigenschaft des Master geändert, müssen die Änderungen auch für alle Slaves durchgeführt werden.

Definitionen

Krypto-Eigenschaften für die Speicherung. Diese Konfiguration bestimmt, wie Daten auf dem Server gespeichert und verschlüsselt werden (in Datenbank oder Datei, mit welchen Krypto-Eigenschaften die Daten ver- oder entschlüsselt werden usw.), wie Anmeldeinformationen sicher gespeichert werden, wie die Verschlüsselung verarbeitet wird und gemäß welcher Konfiguration.

Krypto-Eigenschaften für die Übertragung. Die Übertragungskonfiguration bestimmt, wie der Server und die Clients die gegenseitige Übertragung verschlüsseln, welche Konfiguration verwendet wird, wie Anmeldeinformationen sicher übertragen werden, wie die Verschlüsselung verarbeitet wird und gemäß welcher Konfiguration. Sie müssen dieselben Krypto-Eigenschaften für die Ver- und Entschlüsselung der Übertragung auf dem Server und den Clients verwenden.

Replizierungen und Krypto-Eigenschaften für die Replizierung. Die sicher von Confidential Manager gespeicherten Daten werden auf sichere Weise zwischen mehreren Servern repliziert. Diese Eigenschaften bestimmen, wie die Daten zwischen Slave-Server und Master-Server übertragen werden.

Hinweis:

- Die Datenbanktabelle mit der Konfiguration des Confidential Manager-Servers hat den folgenden Namen: **CM_CONFIGURATION.**
- Die Standardkonfigurationsdatei des Confidential Manager-Servers befindet sich in **app-infra.jar** und heißt **defaultCMServerConfig.xml**.

Verschlüsselungseigenschaften

In der folgenden Tabelle sind die Verschlüsselungseigenschaften beschrieben. Weitere Informationen zur Verwendung dieser Parameter finden Sie unter "Konfigurieren von HP Universal CMDB Server" auf Seite 96.

Parameter	Beschreibung	Empfohlener Wert
encryptTransportMode	Verschlüsselung der übertragenen Daten: true, false	true
encryptDecrypt InitString	Kennwort für die Verschlüsselung	Länger als 8 Zeichen
cryptoSource	Bibliothek für die Umsetzung der Verschlüsselung: • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Unterstützung für schwache Kryptographie vorheriger Versionen: • true • false	true
cipherType	Der von Confidential Manager verwendete Verschlüsselungstyp. Confidential Manager unterstützt nur einen Wert: **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • Null (keine Verschlüsselung)	AES
algorithmModeName	Modus des Blockverschlüsselungsalgorithmus: • CBC	CBC
algorithmPaddingName	Auffüllstandards: • PKCS7Padding • PKCS5Padding	PKCS7Padding

Parameter	Beschreibung	Empfohlener Wert
keySize	Abhängig vom Algorithmus (was **engineName** unterstützt)	256
pbeCount	Wie oft der Hash ausgeführt wird, um den Schlüssel aus **encryptDecryptInitString** zu erstellen. Beliebige positive Zahl.	1000
pbeDigestAlgorithm	Hashing-Typ: • SHA1 • SHA256 • MD5	SHA256
encodingMode	ASCII-Darstellung des verschlüsselten Objekts: • Base64 • Base64Url	Base64Url
useMacWithCrypto	Bestimmt, ob MAC mit der Kryptographie verwendet wird: • true • false	false
macType	Typ des Message Authentication Code (MAC): • hmac	hmac
macKeySize SHA256	Abhängig vom MAC-Algorithmus	256
macHashName	Der Hash-MAC-Algorithmus: • SHA256	SHA256


Java™
COMPATIBLE