HP Universal CMDB

für die Betriebssysteme Windows und Linux

Softwareversion: 9.02

Bereitstellungshandbuch

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

Rechtliche Hinweise

Garantie

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

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

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

Urheberrechtshinweise

Marken

Adobe® und Acrobat® sind Marken von Adobe Systems Incorporated.

AMD und das AMD-Pfeilsymbol sind Marken von Advanced Micro Devices, Inc.

Google™ und Google Maps™ sind Marken von Google Inc.

Intel®, Itanium®, Pentium® und Intel® Xeon® sind Marken der Intel Corporation in den USA und anderen Ländern.

Java™ ist eine in den USA eingetragene Marke von Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, Windows® XP und Windows Vista® sind in den USA eingetragene Marken der Microsoft Corporation.

Oracle ist eine eingetragene Marke der Oracle Corporation und/oder ihren Tochterunternehmen.

UNIX® ist eine eingetragene Marke von The Open Group.

Hinweise

- Dieses Produkt beinhaltet Software, die von der Apache Software Foundation entwickelt wurde (http://www.apache.org/licenses).

- Dieses Produkt beinhaltet OpenLDAP-Code der OpenLDAP Foundation (http://www.openldap.org/foundation/).
- Dieses Produkt beinhaltet GNU-Code der Free Software Foundation, Inc. (http://www.fsf.org/).
- Dieses Produkt beinhaltet JiBX-Code von Dennis M. Sosnoski.
- Dieses Produkt beinhaltet den XPP3 XMLPull-Parser, der mit JiBX vom Indiana University Extreme! Lab vertrieben und im gesamten JiBX-Framework verwendet wird.
- Dieses Produkt beinhaltet die Office Look and Feels-Lizenz von Robert Futrell (http://sourceforge.net/projects/officelnfs).
- Dieses Produkt beinhaltet JEP – Java Expression Parser-Code von Netaphor Software, Inc. (http://www.netaphor.com/home.asp).

Aktualisierte Dokumentation

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

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

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

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

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

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

Alternativ können Sie auf den Link zum Registrieren neuer Benutzer auf der HP Passport-Anmeldeseite klicken.

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

Support

Besuchen Sie die HP Software Support-Website unter:

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

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

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

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

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

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

Weitere Informationen zu Zugriffsebenen finden Sie unter:

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

Inhalt

TEIL II: INSTALLATION DES UCMDB-SERVERS

TEIL VII: NOTFALLWIEDERHERSTELLUNG

TEIL VIII: ERSTE SCHRITTE IN HP UNIVERSAL CMDB

Willkommen bei diesem Handbuch

Willkommen beim HP Universal CMDB – Bereitstellungshandbuch. In diesem Handbuch wird Ihnen HP Universal CMDB vorgestellt. Es bietet Informationen zu den ersten Schritten, beschreibt die Serverinstallation, die Serverhärtung und bietet detaillierte Informationen über die Schritte, die für ein Upgrade notwendig sind.

Dieses Kapitel umfasst die folgenden Themen:

Aufbau dieses Handbuchs

Dieses Handbuch umfasst die folgenden Kapitel:

Teil I Einführung

Stellt die Komponenten vor, die während der HP Universal CMDB-Installation installiert werden. Es enthält einen Ablauf der Installationsschritte und zeigt die verschiedenen Optionen für die Bereitstellung.

Teil II Installation des UCMDB-Servers

Beschreibt die Installationsprozedur des HP Universal CMDB-Servers einschließlich der Datenbankkonfiguration.

Teil III Installation von Data Flow Probe

Beschreibt die Installationsprozedur der Data Flow Probe.

Teil IV Upgrade von HP Universal CMDB Version 8.0x auf Version 9.0x

Erklärt die Schritte, die für ein Upgrade (Migrieren) von HP Universal CMDB auf Version 9.02 und für das Migrieren von Paketen der Version 8.0x auf die Version 9.02 erforderlich sind.

Teil V Hochverfügbarkeit und Kapazitätsplanung

Beschreibt die Schritte der Installation, zum Starten und zum Konfigurieren von HP Universal CMDB, Version 9.02, für die Verwendung in einer Hochverfügbarkeitsumgebung.

Teil VI Härten von HP Universal CMDB

Erklärt die Schritte, die zum Härten des HP Universal CMDB-Servers und der Data Flow Probe erforderlich sind.

Teil VII Notfallwiederherstellung

Beschreibt die Grundsätze und Richtlinien zum Einrichten eines Systems für die Wiederherstellung im Notfall.

Teil VIII Erste Schritte in HP Universal CMDB

Bietet Informationen zum erstmaligen Anmelden an HP Universal CMDB nach Abschluss der Installation sowie über das Startmenü. Zudem finden Sie hier Informationen für den Zugriff auf UCMDB über den IIS-Websever.

Zielgruppe dieses Handbuchs

Dieses Handbuch richtet sich an folgende HP Universal CMDB-Benutzer:

- HP Universal CMDB-Administratoren
- HP Universal CMDB-Plattformadministratoren
- HP Universal CMDB-Applikationsadministratoren
- HP Universal CMDB-Datenverwaltungsadministratoren

Leser dieses Handbuchs sollten sich mit der Verwaltung von Unternehmenssystemen auskennen, mit ITIL-Konzepten vertraut sein und Kenntnisse über HP Universal CMDB besitzen.

HP Universal CMDB-Online-Dokumentation

HP Universal CMDB beinhaltet die folgende Online-Dokumentation:

Readme. Stellt eine Liste mit Versionseinschränkungen und kurzfristigen Updates bereit. Doppelklicken Sie im Stammverzeichnis der HP Universal CMDB-DVD auf **readme.html**. Sie können auch über die HP Software Support-Website auf die aktuelle Readme-Datei zugreifen.

Neuerungen. Enthält eine Liste mit neuen Funktionen und versionsspezifischen Besonderheiten. Wählen Sie in HP Universal CMDB die Menüoption **Hilfe** > **Neues** aus.

Druckerfreundliche Dokumentation. Wählen Sie **Hilfe** > **UCMDB-Hilfe** aus. Die folgenden Handbücher sind nur im PDF-Format verfügbar:

- *HP Universal CMDB – Bereitstellungshandbuch* (PDF). Erläutert die Hardware- und Softwareanforderungen zum Einrichten von HP Universal CMDB und die Vorgehensweise zum Installieren von HP Universal CMDB, zum Härten des Systems und zum Anmelden bei der Anwendung.
- *HP Universal CMDB – Datenbankhandbuch* (PDF). Erläutert die Vorgehensweise zum Einrichten der Datenbank (MS SQL Server oder Oracle), die von HP Universal CMDB benötigt wird.

- *HP Universal CMDB Discovery and Integration Content Guide* (PDF). Erläutert die Vorgehensweise zum Ausführen der Discovery, um die aktiven Applikationen, Betriebssysteme und Netzwerkkomponenten in Ihrem System zu erkennen. Erläutert außerdem die Vorgehensweise zum Erkennen von Daten in weiteren Daten-Repositorys mittels Integration.

Die **HP Universal CMDB-Online-Hilfe** enthält:

- **Modellierungshandbuch**. Ermöglicht das Verwalten des Inhalts Ihres IT Universe-Modells.
- **Handbuch zur Datenflussverwaltung**. Erläutert die Vorgehensweise zum Integrieren von HP Universal CMDB mit weiteren Daten-Repositorys und zum Einrichten von HP Universal CMDB für die Erkennung von Netzwerkkomponenten.
- **Verwaltungshandbuch**. Erläutert die Verwendung von HP Universal CMDB.
- **Entwicklerreferenzhandbuch**. Für Benutzer mit fortgeschrittenen Kenntnissen über HP Universal CMDB. Erläutert die Vorgehensweise zum Definieren und Verwenden von Adaptern und zum Verwenden der APIs für den Zugriff auf die Daten.

Auf die Online-Hilfe können Sie in bestimmten HP Universal CMDB-Fenstern auch zugreifen, indem Sie in das Fenster und dann auf die Schaltfläche **Hilfe** klicken.

Online-Bücher können mithilfe von Adobe Reader angezeigt und ausgedruckt werden. Den Reader können Sie von der Adobe-Website (www.adobe.com) herunterladen.

Thementypen

Alle Themenbereiche in diesem Handbuch sind nach Themen organisiert. Ein Thema enthält ein eigenes Informationsmodul für einen Themenbereich. Die Themen sind im Allgemeinen nach der Art der enthaltenen Informationen geordnet.

Diese Struktur soll den Zugriff auf bestimmte Informationen vereinfachen. Die Dokumentation ist nach den verschiedenen Arten von Informationen aufgeteilt, die Sie jeweils benötigen könnten.

Es gibt drei Hauptthementypen: **Konzepte**, **Aufgaben** und **Referenz**. Diese Thementypen sind durch unterschiedliche Symbole gekennzeichnet.

Thementyp	Beschreibung	Verwendung
Konzepte 	Hintergrund-, beschreibende oder konzeptionelle Informationen.	Allgemeine Informationen zur Arbeitsweise einer Funktion.
Aufgaben 	**Aufgaben mit Anweisungscharakter.** Schrittweise Anleitung als Hilfestellung für Ihre Arbeit mit der Applikation und die Erreichung Ihrer Ziele. Zu einigen Schritten in den Aufgaben gehören Beispiele mit Musterdaten. Die Schritte in den Aufgaben können nummeriert oder auch nicht nummeriert sein: ➤ **Schritte mit Nummerierung.** Aufgaben, bei denen alle Schritte direkt aufeinander folgend ausgeführt werden müssen. ➤ **Schritte ohne Nummerierung.** Eine Liste mit in sich geschlossenen Operationen, die in beliebiger Reihenfolge ausgeführt werden können.	➤ Lernen Sie den Gesamtablauf einer Aufgabe kennen. ➤ Führen Sie in einer Aufgabe mit Nummerierung die einzelnen Schritte durch, um die Aufgabe zu erfüllen. ➤ Führen Sie unabhängige Operationen aus, indem Sie die Schritte in einer Aufgabe ohne Nummerierung durchführen.
	Aufgaben für Verwendungsszenarios. Beispiele zur Ausführung einer Aufgabe für eine bestimmte Situation.	Erfahren Sie, wie eine Aufgabe in einem realistischen Szenario ausgeführt werden könnte.

Thementyp	Beschreibung	Verwendung
Referenz 	**Allgemeine Referenz**. Detaillierte Listen und Erläuterungen des Referenzmaterials.	Hier finden Sie spezielle Referenzinformationen, die in einem bestimmten Kontext relevant sind.
	Referenz zur Benutzeroberfläche. Spezielle Referenzthemen, in denen eine bestimmte Benutzeroberfläche detailliert beschrieben wird. Wenn Sie im Menü "Hilfe" im Produkt die Option **Hilfe zu dieser Seite** auswählen, werden im Allgemeinen die Themen zur Benutzeroberfläche geöffnet.	Hier finden Sie spezielle Informationen zu den notwendigen Eingaben oder zur Verwendung bestimmter Benutzeroberflächenelemente, wie zum Beispiel für ein Fenster, ein Dialogfeld oder einen Assistenten.
Fehlerbehebung und Einschränkungen 	**Fehlerbehebung und Einschränkungen**. Spezielle Referenzthemen, in denen häufig auftretende Probleme mit entsprechenden Lösungen beschrieben und die zu beachtenden Einschränkungen für eine Funktion oder einen Produktbereich aufgeführt werden.	Erhöhen Sie Ihre Sensibilität für wichtige Probleme, bevor Sie mit einer Funktion arbeiten oder wenn Sie auf Probleme mit der Benutzerfreundlichkeit in der Software stoßen.

Zusätzliche Online-Ressourcen

Troubleshooting & Knowledge Base führt Sie zur Fehlerbehebungsseite der HP Software Support-Website, auf der Sie die Self-Solve Knowledge Search verwenden können. Wechseln Sie zu **Hilfe** > **Fehlerbehebung & Wissensdatenbank**. Der URL für diese Website lautet http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software-Unterstützung führt Sie zur HP Software Support-Website. Auf dieser Website können Sie die Self-Solve Knowledge Search verwenden. Darüber hinaus können Sie u. a. Beiträge in Diskussionsforen für Benutzer veröffentlichen und durchsuchen, Support-Anfragen übermitteln sowie Patches und aktualisierte Dokumentationen herunterladen. Wechseln Sie zu **Hilfe** > **HP Software-Unterstützung**. Der URL für diese Website lautet www.hp.com/go/hpsoftwaresupport.

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.

Weitere Informationen zu Zugriffsebenen finden Sie unter:

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

Hier können Sie sich für eine HP Passport-Benutzer-ID registrieren:

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

HP Software-Website führt Sie zur HP Software-Website. Auf dieser Website finden Sie die aktuellsten Informationen zu HP Software-Produkten. Dazu gehören u. a. neue Softwarereleases, Seminare und Messen sowie Kundenservice. Wechseln Sie zu **Hilfe** > **HP Software-Website**. Der URL für diese Website lautet www.hp.com/go/software.

Aktualisierte Dokumentation

HP Software aktualisiert seine Produktdokumentationen ständig mit neuen Informationen.

Auf der folgenden Website zu HP Software-Produkthandbüchern 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.

Teil I

Einführung

1

Einführung in HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

HP Universal CMDB – Übersicht

Im Folgenden erhalten Sie eine Einführung zu HP Universal CMDB, zu den Hauptphasen der HP Universal CMDB-Installation und zum Installationsworkflow. Außerdem erfahren Sie, welche Hardware, Software und Konfigurationsdaten Sie benötigen und welche ersten Schritte Sie durchführen müssen.

Dieser Abschnitt umfasst die folgenden Themen:

Über HP Universal CMDB

HP Universal CMDB besteht aus einem umfassenden Datenmodell für Geschäftsservices, das integrierte Funktionen für die Discovery von Konfigurationselementen (CIs) und Beziehungen zwischen diesen CIs, für die Darstellung und Zuordnung von Geschäftsservices und für die Verfolgung von Konfigurationsänderungen bietet.

Mit HP Universal CMDB können Sie alle CIs in einer „verwalteten Welt“ erfassen. Eine verwaltete Welt bezeichnet eine in sich geschlossene Umgebung, die sich mit einem Topologiemodell beschreiben lässt (definiert mit der TQL-Sprache (Topology Query Language) von HP). Die IT-Infrastruktur eines großen Unternehmens stellt beispielsweise eine solche verwaltete Welt dar, in der die Topologie mehrere Ebenen umfasst, darunter Netzwerke, Protokolle, Datenbanken, Betriebssysteme usw. Durch die Verwaltung von Ansichten können Sie die Informationen genau im richtigen Format anzeigen.

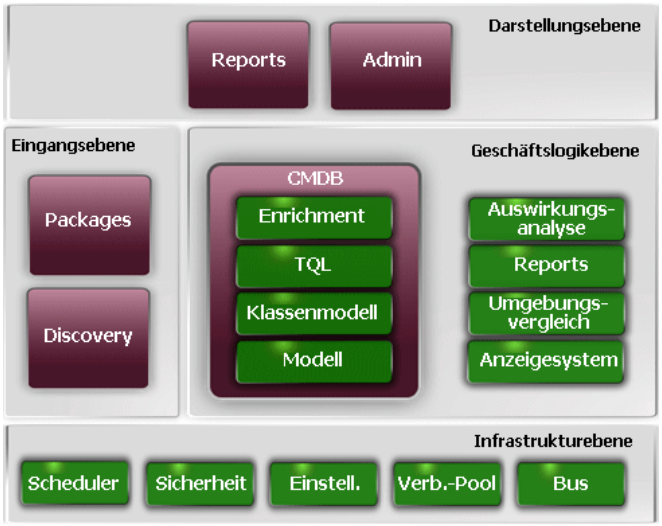
Darüber hinaus werden alle Informationen in den TQL-Ergebnissen automatisch mit den neuesten Daten aktualisiert, die in der CMDB (Configuration Management Database) erfasst werden. Dies bedeutet, dass alle definierten TQLs und Ansichten immer die neuesten Informationen zum Status der verwalteten Welt enthalten. Ansichten werden mit mehreren Ebenen angezeigt, damit Sie wichtige CIs bedarfsgerecht erkennen können. Darüber hinaus lassen sich Reports (in HTML, Excel oder Tabellenformat) mit den Informationen erstellen, die im System erfasst wurden.

HP Universal CMDB eignet sich für die folgenden betrieblichen und funktionalen Anforderungen:

- **Abstimmung von IT-Ressourcen und Applikationen.** Automatische Discovery von IT-Ressourcen und deren wechselseitigen Abhängigkeiten aus der Perspektive der Geschäftsservices.
- **Problemlösung.** Abbildung der kausalen Beziehungen zwischen CIs, um die Ursache von Infrastrukturproblemen zu finden und die Fehlerbehebung zu beschleunigen.
- **Steuerung von Asset- und Änderungsverwaltung.** Automatische Erkennung von Infrastrukturänderungen, um die automatische Aktualisierung aller relevanten Untersysteme zu ermöglichen.
- **Angepasste Statusverwaltung (Leistung, Änderung).** Möglichkeit zur Definition eines CI-Verwaltungsstatus.
- **Leistungsverwaltung und Kapazitätsplanung.**
- **Architektur- und Infrastrukturplanung.**
- **Föderations- und Abstimmungsdaten.** Abgerufen aus vorhandenen Repositorys und anderen CMDBs.

HP Universal CMDB-Systemarchitektur

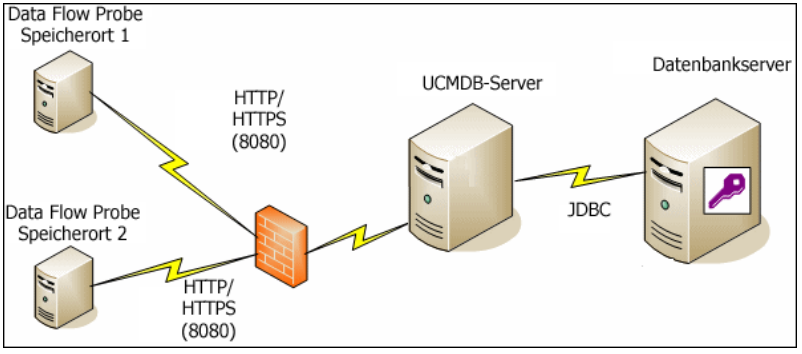
Die folgende Grafik zeigt die Systemarchitektur von HP Universal CMDB im Überblick:



Informationen zum Einrichten einer LDAP-Authentifizierungsmethode für die Anmeldung finden Sie unter "Authentifizierung bei der Anmeldung in HP Universal CMDB" auf Seite 397.

HP Universal CMDB-Bereitstellung

Die folgende Grafik veranschaulicht eine typische Bereitstellung des HP Universal CMDB-Systems.



Die CMDB

Die CMDB (Configuration Management Database) bildet das zentrale Repository für die Konfigurationsdaten, die von HP Universal CMDB und den verschiedenen Applikationen und Tools von Drittanbietern erfasst werden.

Die CMDB enthält CIs und Beziehungen, die automatisch aus dem Discovery-Prozess erstellt oder manuell eingefügt werden. Die CIs und Beziehungen ergeben zusammen das Modell der Komponenten in der IT-Welt Ihres Unternehmens.

Außerdem werden in der CMDB die Infrastrukturdaten gespeichert und verwaltet, die von Data Flow Management erfasst und aktualisiert werden.

Das IT-Modell kann sehr groß sein und Tausende von CIs umfassen. Um die Verwaltung dieser CIs zu vereinfachen, werden die CIs in einer Ansicht dargestellt, die eine Teilmenge aller Komponenten in der IT-Welt abbildet.

Sie verwenden Ansichten (mit HP Universal CMDB bereitgestellte oder in der Topologie-Karte definierte Werk-Ansichten), um die CIs und Beziehungen in der CMDB anzuzeigen und zu verwalten. Durch diese Ansichten können Sie gezielt mit bestimmten IT-Bereichen arbeiten.

Daneben enthält die CMDB auch TQL-Abfragedefinitionen für das Abfragen und Abrufen von Daten aus der CMDB, um diese anzuzeigen in:

- Pattern-Ansichten (Ansichten, die auf TQLs basieren)
- einem CIT-Modell (CIT = Configuration Item Type) (einem Repository für alle CI-Typen und Beziehungsdefinitionen)

Hinweis: Sie können aus anderen HP-Produkten eine Verbindung zur CMDB herstellen. Weitere Informationen dazu finden Sie in der Installationsdokumentation des Produkts.

Data Flow Management-Zuordnung

Der Discovery-Prozess bildet den Mechanismus, mit dem Sie Daten zu Ihrem System erfassen können, indem die IT-Infrastrukturressourcen und ihre wechselseitigen Abhängigkeiten (Beziehungen) erkannt werden. Data Flow Management kann diverse Ressourcen erkennen, wie z. B. Applikationen, Datenbanken, Netzwerkgeräte, verschiedene Servertypen usw. Jede erkannte IT-Ressource wird in der CMDB erfasst und gespeichert und in Form eines verwalteten Konfigurationselements (CI) dargestellt.

TQL (Topology Query Language)

TQL ist eine Sprache und ein Werkzeug zum Erkennen, Organisieren und Verwalten von IT-Infrastrukturdaten. TQL dient zum Erstellen von Abfragen, mit denen sich bestimmte Daten aus der CMDB abrufen und anzeigen lassen.

TQL-Abfragen sorgen dafür, dass die CMDB ständig nach Änderungen durchsucht wird, die sich beim Status der verwalteten Ressourcen ergeben haben, damit die betroffenen Untersysteme aktualisiert werden können.

TQL erweitert die traditionellen Abfragesprachen um zwei wichtige Funktionen:

- Durch TQL kann HP Universal CMDB konzeptbasierte Beziehungen zwischen CIs darstellen, die ihre tatsächlichen Abhängigkeiten widerspiegeln. Mithilfe vordefinierter Operatoren können die unterschiedlichen Verbindungstypen zwischen CIs eingerichtet werden, um den Entwurf und die Leistung der Infrastruktur genauer abzubilden. Diese Darstellung dient als Basis und als Modell für die Ermittlung, Anordnung, Abfrage und Verwaltung komplexer Infrastrukturen.
- TQL beinhaltet grafische Symbole und Syntax, um die Ressourcen und ihre wechselseitigen Verbindungen abzubilden. Diese Visualisierung einer IT-Infrastruktur erleichtert es Ihnen, die IT-Geschäftsvorgänge zu verstehen, zu überwachen und zu verwalten.

Dokumentkonventionen

- Die HP Universal CMDB-Dokumentation geht davon aus, dass der HP Universal CMDB Server und die Data Flow Probe in den Standardverzeichnissen **C:\hp\UCMDB\UCMDBServer** bzw. **C:\hp\UCMDB\DataFlowProbe** installiert sind.
- Anweisungen für den Zugriff auf Komponenten der Applikation beginnen immer vom linken Menü aus. Beispiel für die Anzeige der Topologieabfrage für Active Directory: **Modellieren** > **Modeling Studio** > **Ressourcen** > **Root** > **Application** > **Active Directory**.

HP Universal CMDB auf VMware

Wenn Sie HP Universal CMDB auf einer VMware-Plattform bereitstellen, gelten andere Dimensionierungsrichtlinien als für eine normale Installation. Für eine VMware-Installation gelten die folgenden allgemeinen Beschränkungen und Empfehlungen:

- Die Leistung von HP Universal CMDB auf VMware ist in der Regel niedriger als bei einer normalen Installation. Daher wird eine VMware-Plattform nicht für die Bereitstellung von HP Universal CMDB in Unternehmen empfohlen und wird nur für Standardbereitstellungen unterstützt. Informationen zu den Anforderungen bei der Bereitstellung finden Sie unter "Server-Hardwareanforderungen" auf Seite 36.
- Die Kapazität und Leistung von HP Universal CMDB kann abhängig von den verschiedenen Serverressourcen schwanken, darunter CPU, Speicher und Netzwerkbandbreite, die den HP Universal CMDB-Komponenten zugewiesen wurden.
- Sie sollten ESX Server mit den Versionen 3.5 bis 4.0 verwenden.
- Sie sollten eine Gigabit-Netzwerkkarte verwenden.
- Es wird dringend empfohlen, keinen Datenbankserver mit HP Universal CMDB-Datenbanken auf VMware auszuführen, wenn sich die Datenbankdateien auf einem virtuellen VMware-Datenträger befinden.
- VMware wird als einzige Virtualisierungstechnologie von HP Universal CMDB für Windows unterstützt.

Die folgenden HP Universal CMDB-Komponenten werden auf VMware ESX Server mit den Versionen 3.5 bis 4.0 unterstützt:

- HP Universal CMDB
- Data Flow Probe

Migrieren von früheren Versionen

Informationen zu HP Universal CMDB-Upgrades von Version 8.0x auf 9.02 finden Sie unter "Upgrade für HP Universal CMDB von Version 8.0x auf Version 9.0x" auf Seite 173.

Informationen zu HP Universal CMDB-Upgrades von Version 7.0x und 7.5x auf 8.0x finden Sie in der Dokumentation zu Version 8.04.

Aufgaben

Ändern der Speicherzuweisung für Applets

Hinweis: Dieser Abschnitt ist nur von Bedeutung, wenn Sie die Verbindung zur HP Universal CMDB von einem Clientcomputer mit JRE 6u9 oder früher herstellen.

Für eine ordnungsgemäße Funktion benötigen die HP Universal CMDB-Applets möglicherweise mehr Speicher, als ihnen standardmäßig zugewiesen ist, insbesondere wenn Sie sehr große Topologie-Karten anzeigen oder das Applet über eine längere Zeit verwenden, ohne den Browser neu zu starten.

Zum Ändern der Speicherzuweisung bearbeiten Sie eine Datei auf dem Clientcomputer (auf dem der Benutzer das Applet verwendet):

1. Öffnen Sie auf Windows-Computern die folgende Datei: **...\Dokumente und Einstellungen\%Benutzerprofil%\Anwendungsdaten\Sun\Java\Deployment\deployment.properties**.
2. Ändern Sie die Zeile mit der neuesten Java-Version, indem Sie am Ende den Text **-XmxYYYm** hinzufügen. Dabei steht **YYY** für die Speichermenge (in Megabyte), die dem Java-Applet zugewiesen wird. Beispiel:

   ```
   deployment.javapi.jre.6u10.args=-Xmx256m
   ```

   Dadurch werden dem Applet 256 MB Speicher zugewiesen.

   Der Standardwert (wenn kein Parameter **-Xmx** vorliegt) beträgt 64 MB. Sie können die Werte 128 MB und 256 MB ausprobieren. Es wird empfohlen, nicht mehr als 256 MB zu verwenden. Wenn Java den festgelegten Speicher nicht anfordern kann, wird es nicht geladen. Setzen Sie in diesem Fall den zugewiesenen Speicher auf einen niedrigeren Wert.

Diese Änderung können Sie auch vornehmen, indem Sie **Start** > **Einstellungen** > **Systemsteuerung** auswählen. Doppelklicken Sie auf das Java-Symbol und klicken Sie dann auf die Registerkarte **Java**. Klicken Sie auf die Schaltfläche **Anzeigen** für die verwendeten Laufzeiteinstellungen bei Ausführung eines Applets. Nehmen Sie die Änderungen im Feld **Java-Laufzeitparameter** gemäß den zuvor aufgeführten Anweisungen vor.

Hinweis:

- Aufgrund von technischen Beschränkungen wird beim Wechseln des Modus (z. B. von Admin zu Applikation) oder des Managers, bevor alle Applets in den Browser heruntergeladen wurden, möglicherweise die Meldung **Abbruchfehler** angezeigt. Leeren Sie in diesem Fall den Java-Cache.
- Um den Fortschritt beim Herunterladen der Applet-JAR-Dateien anzuzeigen, geben Sie im Java-Konsolenfenster **5** ein.
- Weitere Informationen zum Installieren oder Aktualisieren von Java auf dem Clientcomputer finden Sie unter "Aktualisieren der Java-Konfiguration" auf Seite 50.

2

HP Universal CMDB – Unterstützungsmatrix

Dieses Kapitel umfasst die folgenden Themen:

Referenz

Referenz

Server-Hardwareanforderungen

Computer/Prozessor	**Windows/Linux:** Um die CPU-Anforderungen zu erfüllen, benötigen Sie einen der folgenden Prozessoren: ➤ Intel Xeon-Doppelkernprozessor mit mindestens 2,4 GHz ➤ AMD Opteron-Doppelkernprozessor mit mindestens 2,4 GHz Zusätzlich zur genannten Anforderung müssen Sie über die folgende Anzahl an CPU-Kernen verfügen, abhängig von Ihrer Bereitstellungskonfiguration: ➤ Kleine Bereitstellung: 1 CPU ➤ Standardbereitstellung: 4 CPUs ➤ Unternehmensbereitstellung: 8 CPUs **Hinweis**: Da die Leistung von HP Universal CMDB von der Prozessorgeschwindigkeit abhängt, sollten Sie einen möglichst schnellen Prozessor einsetzen.
Speicher	**Windows/Linux:** ➤ Kleine Bereitstellung: 4 GB RAM ➤ Standardbereitstellung: 8 GB RAM ➤ Unternehmensbereitstellung: 16 GB RAM

Virtueller Speicher/ Speicher-Swap-Datei	**Windows:** ➤ Kleine Bereitstellung: 6 GB (Unterstützt) ➤ Standardbereitstellung: 12 GB ➤ Unternehmensbereitstellung: 24 GB **Linux:** ➤ Kleine Bereitstellung: 4 GB (Unterstützt) ➤ Standardbereitstellung: 8 GB ➤ Unternehmensbereitstellung: 16 GB **Hinweis:** ➤ Der virtuelle Speicher für Windows sollte mindestens 1,5 Mal so groß wie der physische Speicher sein. ➤ Die Größe der Linux-Swap-Datei sollte der physischen Speichermenge entsprechen.
Freier Festplattenplatz	Mindestens 30 GB (für Protokolle, Speicherauszüge usw.)
Anzeige	**Windows:** Farbpalette mit mindestens 256 Farben (empfohlen: 32.000 Farben)

Server-Softwareanforderungen

Hardware-plattform	Betriebssystemtyp	Betriebssystemversion und -edition	Unterstützt	Empfohlen
x86-64	Windows 2003	Enterprise SP2 und R2 SP2, 64-Bit	Ja	
x86-64	Windows 2008	Enterprise SP2 und R2, 64-Bit	Ja	Ja
x86-64	Red Hat Linux 5	Enterprise/Advanced, 64-Bit	Ja	
Alle	SUSE Linux 9, 10, 11	Enterprise	Nein	
x86	Windows 2000, 2003/2008		Nein	64-Bit erforderlich
Sun SPARC	Solaris 8, 9 oder 10		Nein	
Alle	Red Hat Linux 3, 4	Enterprise	Nein	
Itanium 64	Red Hat Linux 5	Enterprise/Advanced	Nein	

Hinweis:

- Die nicht unterstützten Konfigurationen sind aufgeführt, um sicherzustellen, dass der Umfang der Unterstützungsmatrix eindeutig ist.
- Es wird empfohlen, Dr. Watson im automatischen Modus zu aktivieren und zu konfigurieren (nachdem Dr. Watson, d. h. Drwtsn32.exe, mindestens ein Mal ausgeführt wurde). Zum Einrichten des automatischen Modus suchen Sie in der Windows-Registrierung nach **\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AeDebug** und setzen den Wert für den Parameter **Auto** auf **1**.
- Unabhängig von der Betriebssystemversion werden die gesamte Distribution (mit OEM-Unterstützung) und das neueste empfohlene Patch-Cluster benötigt.

Vom Server unterstützte virtuelle Umgebungen

Virtuelle Umgebung	Betriebssystemversion und -edition	Unterstützt	Empfohlen
VMware ESX 4.0	➤ Windows 2003 Enterprise SP2 und R2 SP2, 64-Bit ➤ Windows 2008 Enterprise SP2 und R2, 64-Bit ➤ Red Hat Linux 5 Enterprise/Advanced, 64-Bit	Ja	Ja
VMware ESX Version 3.5 oder Version 3.x	➤ Windows 2003 Enterprise SP2 und R2 SP2, 64-Bit ➤ Windows 2008 Enterprise SP2 und R2, 64-Bit ➤ Red Hat Linux 5 Enterprise/Advanced, 64-Bit	Ja	Ältere ESX 3.x-Versionen liefern möglicherweise nicht genug Leistung und werden möglicherweise nicht von allen Betriebssystem-versionen unterstützt.
MS Hyper-V Server 2008 v1 und R2	Alle	Nein	
Xen Hypervisor 3.x	Alle	Nein	
ESXi	Alle	Nein	

Server-Datenbankanforderungen

In diesem Abschnitt werden die Datenbankserver beschrieben, die für den Einsatz mit HP Universal CMDB unterstützt werden.

Dieser Abschnitt umfasst die folgenden Themen:

Systemanforderungen für Oracle

In der folgenden Tabelle sind die Oracle-Server aufgeführt, die für den Einsatz mit HP Universal CMDB unterstützt werden. Wird eine Option unterstützt, bedeutet dies, dass die QS-Mitarbeiter von HP erfolgreiche grundlegende Tests für diese Option durchgeführt haben.

Datenbank-Release	
Version	**Systemtyp**
Oracle 10.2 (10.2.0.4 oder höhere, komponentenspezifische Versionsnummer 10.2.0.X) Enterprise Edition	64-Bit
Oracle 10.2 (10.2.0.4 oder höhere, komponentenspezifische Versionsnummer 10.2.0.X) RAC Enterprise Edition	64-Bit
Oracle 11.1.0.7 Enterprise Edition	64-Bit
Oracle 11.2 (11g R2) Standard Edition	64-Bit
Oracle 11.2 (11g R2) Enterprise Edition	64-Bit
Oracle 11.2 (11g R2) RAC Enterprise Edition	64-Bit

Hinweis:

- Es wird dringend empfohlen, die neuesten kritischen Oracle-Patches für Ihr Betriebssystem anzuwenden. Weitere Informationen finden Sie in der Oracle-Dokumentation.
- Hinweise zu unterstützten Plattformen finden Sie in der Oracle-Dokumentation.
- Die Oracle-Partitionierungsoption sollte aktiviert sein.

Beispiele für getestete Bereitstellungen

In der folgenden Tabelle sind die Bereitstellungsumgebungen aufgeführt, für die durch QS-Mitarbeiter von HP strenge Tests durchgeführt wurden.

Datenbank-Release		**Betriebssystem**
Version	**Systemtyp**	
Oracle 11.2 (11g R2) Enterprise Edition	64-Bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) RAC Enterprise Edition	64-Bit	Linux Enterprise Edition RHEL 5
Oracle 10.2.0.4 Enterprise Edition	64-Bit	Linux Enterprise Edition RHEL 5
Oracle 11.2 (11g R2) Enterprise Edition	64-Bit	Solaris 10

Systemanforderungen für Microsoft SQL Server

In der folgenden Tabelle sind die Microsoft SQL Server aufgeführt, die für den Einsatz mit HP Universal CMDB unterstützt werden. Wird eine Option unterstützt, bedeutet dies, dass die QS-Mitarbeiter von HP erfolgreiche grundlegende Tests für diese Option durchgeführt haben.

Datenbank-Release		
Version	**Systemtyp**	**Service Pack**
Microsoft SQL Server 2008 Enterprise Edition	32-Bit	Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64-Bit	Service Pack 1
Microsoft SQL Server 2008 Standard Edition	32-Bit	Service Pack 1
Microsoft SQL Server 2008 Standard Edition	64-Bit	Service Pack 1
Microsoft SQL Server 2005 Enterprise Edition	32-Bit	Service Pack 3
Microsoft SQL Server 2005 Enterprise Edition	64-Bit	Service Pack 3

Hinweis:

- Es dürfen nur unterstützte Service Packs mit den neuesten Patches installiert werden.
- Hinweise zu unterstützten Plattformen finden Sie in der Microsoft-Dokumentation.

Beispiele für getestete Bereitstellungen

In der folgenden Tabelle sind die Bereitstellungsumgebungen aufgeführt, für die durch QS-Mitarbeiter von HP strenge Tests durchgeführt wurden.

Datenbank-Release			**Betriebssystem**
Version	**Systemtyp**	**Service Pack**	
Microsoft SQL Server 2008 Enterprise Edition	32-Bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1
Microsoft SQL Server 2008 Enterprise Edition	64-Bit	Service Pack 1	Windows 2008 Enterprise Edition Service Pack 1 (64-Bit)

Client-Softwareanforderungen

Bildschirmauflösung	Mindestauflösung: 1024 x 768. Sie sollten eine Auflösung von 1280 x 1024 verwenden. Bei Breitbildschirmen (z. B. für Laptops mit 15,4 Zoll) eignet sich am besten die Auflösung 1600 x 1050.
Java Runtime Environment (zur Anzeige von Applets)	**Familie 1.6**: Empfohlen wird Version 6u20 und erforderlich ist Version 6u4 oder höher. 6u19 wird nicht empfohlen, da nach jedem Laden eines Applets in einer Pop-up-Meldung darauf hingewiesen wird, dass das Applet eine Mischung aus signiertem und unsigniertem Code enthält. **Hinweis:** Empfohlen wird die JRE-Version 6u20, die auch auf dem UCMDB Server selbst zum lokalen Herunterladen im Netzwerk enthalten ist. **So ändern Sie die lokal verfügbare JRE:** **1** Legen Sie eine neue ausführbare Datei für die JRE-Bereitstellung im folgenden Verzeichnis ab: **C:\hp\UCMDB\UCMDBServer\deploy\ucmdb-ui\static\JRE** **2** Starten Sie den Server neu. Weitere Informationen zum Arbeiten mit Applets finden Sie unter "Ändern der Speicherzuweisung für Applets" auf Seite 33. Wenn Sie Microsoft Internet Explorer verwenden, können Sie die Sun-JRE von der Java-Website herunterladen (**http://java.com/**). Überprüfen Sie nach der Installation, ob der Browser die richtige Java-Version verwendet. Klicken Sie auf **Extras** > **Internetoptionen** > **Erweitert** und aktivieren Sie das Kontrollkästchen **Java (Sun)**. Klicken Sie auf **OK**, schließen Sie den Browser und öffnen Sie ihn erneut.
Java-Caching	Aktivieren Sie Java-Caching auf dem Clientcomputer: **Systemsteuerung** > **Java** > **Allgemein** > **Temporäre Internet-Dateien** > **Einstellungen** > **Temporäre Dateien auf Computer belassen**.
Applet-Tag-Unterstützung	UCMDB-Applets unterstützen nur Applet-Tag-Bereitstellung. Um die Unterstützung von Applet-Tags durch den Clientcomputer zu überprüfen, öffnen Sie die Java-Systemsteuerung. Klicken Sie auf die Registerkarte **Erweitert** und öffnen Sie **Standard-Java für Browser**. Überprüfen Sie, ob Microsoft Internet Explorer ausgewählt ist.

Flash-Player (zur Anzeige von Diagrammen in Reports)	Acrobat Flash 8 oder höher
Microsoft Excel (zur Anzeige exportierter Daten)	Versionen 2003, 2007 und 2010
Adobe PDF (zur Anzeige exportierter Daten)	Versionen 7.0, 8.1 und 9.1

Client-Browseranforderungen

Browser	Betriebssystemversion und -edition	Unterstützt	Empfohlen
Internet Explorer 7 oder höher	Windows XP 32-/64-Bit Windows Vista 32-/64-Bit Windows 7 32-/64-Bit Windows 2003 32-/64-Bit Windows 2008 32-/64-Bit	Ja	Ja
Internet Explorer 8	Windows XP 32-/64-Bit Windows Vista 32-/64-Bit Windows 7 32-/64-Bit Windows 2003 32-/64-Bit Windows 2008 32-/64-Bit	Ja	
Google Chrome	Windows XP Windows Vista Windows 7	Ja	
Firefox 3.5 oder höher	Windows XP Windows Vista Windows 7 Windows 2003 Linux	Ja	
Safari 4.x	Windows	Nein	
Internet Explorer 6	Windows	Nein	

Kapazitätsplanungsanforderungen

Weitere Informationen finden Sie unter "HP Universal CMDB – Planen großer Kapazitäten" auf Seite 285.

3

Lizenzierungsmodell für HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

Lizenzierungsmodell – Übersicht

Das Lizenzierungsmodell für HP Universal CMDB beruht auf drei komplementären Lizenztypen bzw. Lizenzstufen. Die erste Stufe mit der Bezeichnung UCMDB Foundation-Lizenz wird berechtigten Kunden kostenlos zur Verfügung gestellt. Die anderen beiden Stufen (UCMDB Integration Only-Lizenz und DDM Advanced Edition-Lizenz) sind gebührenpflichtig.

Dieser Abschnitt umfasst die folgenden Themen:

➤ "Lizenzierungsstufen" auf Seite 48

➤ "Maßeinheiten" auf Seite 49

Lizenzierungsstufen

➤ **UCMDB Foundation-Lizenz**

Diese Lizenz gewährt folgende Rechte:

- ➤ Verwendung von UCMDB als Backbone-Komponente für ausgewählte BTO-Produkte
- ➤ Integration von UCMDB-Instanzen mit anderen
- ➤ Integration von BTO-Produkten mit UCMDB unter Nutzung verschiedener Integrationstypen

➤ **UCMDB Integration Only-Lizenz**

Diese Lizenz gewährt das Recht, Produkte von Drittanbietern (Nicht-HP-Produkte) mit UCMDB zu integrieren und dabei verschiedene Integrationstypen zu nutzen.

➤ **DDM Advanced Edition-Lizenz**

Diese Lizenz gewährt folgende Rechte:

➤ Verwendung aller Funktionen von Discovery and Dependency Mapping (DDM) zur UCMDB-Auffüllung

➤ Integration von BTO- und Drittanbieterprodukten (Nicht-HP-Produkten) mit UCMDB unter Nutzung beliebiger Integrationstypen

Die folgende Tabelle enthält eine Übersicht über die mit den einzelnen Lizenzen verbundenen Rechte:

Lizenz/Integration	Integrationen mit anderen BTO-Produkten	Integrationen mit Drittanbieter-produkten	Angepasste Discovery-ähnliche Integrationen	Alle Discovery-Funktionen
UCMDB Foundation	Erlaubt	Nein	Nein	Nein
UCMDB Integration Only	Nein	Erlaubt	Nein	Nein
DDM Advanced Edition	Erlaubt	Erlaubt	Erlaubt	Erlaubt

Maßeinheiten

➤ **Betriebssysteminstanz**

Jede Implementierung des bootfähigen Programms, die auf einem physischen System oder auf einer Partition innerhalb des physischen System installiert werden kann. Ein physisches System kann mehrere Betriebssysteminstanzen umfassen.

➤ **Verwalteter Server**

Ein Computersystem oder eine Computersystem-Partition, auf dem bzw. der ein bootfähiges Programm installiert ist, mit Ausnahme von privaten Computern oder Computern, die hauptsächlich von einer Person genutzt werden.

Hinweis: Drucker und Netzwerkgeräte gelten nicht als verwaltete Server.

UCMDB Foundation-Lizenz

Diese kostenlose Berechtigungslizenz für das UCMDB-Produkt erhalten automatisch alle HP-Kunden, die HP Discovery and Dependency Mapping (DDM), HP Service Manager (SM) oder HP Asset Manager (AM) erwerben.

Dieser Abschnitt umfasst folgende Themen:

Standard-BTO-Integrationen

Durch diese Lizenz sind Sie berechtigt, die folgenden BTO-Produkte mit UCMDB zu integrieren:

- HP Universal CMDB * (unterschiedliche Instanz)
- HP Asset Manager *
- HP Service Manager *
- HP DDM Inventory
- HP Network Node Manager
- HP Storage Essentials
- HP Systems Insight Manager

(*) bidirektionale Integration

Die Datenflüsse zwischen diesen Produkten werden mithilfe von Adaptern implementiert, die standardmäßig mit HP Universal CMDB geliefert oder im Paket der SACM-Lösung bereitgestellt werden. Die meisten Adapter können die Data Flow Probe-Infrastruktur von HP Universal CMDB nutzen. Ausnahme sind die Adapter, die einen Föderationsdatenfluss oder den Push-Datenfluss von UCMDB zu SM unterstützen, da hier eine technische Beschränkung besteht.

Hinweis: Der Datenfluss zwischen UCMDB und Asset Manager beruht auf einem Connect-It-Anschluss, für den AM-Kunden eine kostenlose Lizenz erhalten.

Das Recht zur Integration von BTO-Produkten mit UCMDB, das die UCMDB Foundation-Lizenz gewährt, entbindet den Kunden nicht von der Verpflichtung, für diese Produkte zunächst eine gültige Lizenz zu erwerben.

Andere Integrationen

Durch diese Lizenz sind Sie auch berechtigt, BTO-Produkte wie folgt mit UCMDB zu integrieren:

- Standardintegrationen, die von HP-Partnern bereitgestellt werden (möglicherweise mit zusätzlichen Gebühren verbunden)
- Angepasste Datenaustauschintegrationen (d. h. generische Datenbankadapter, generische Push-Adapter und vom Kunden entwickelte Java-Adapter)
- die HP Universal CMDB-Webservice-API und die HP Universal CMDB-API (Java)
- aber nicht Discovery-ähnliche Integrationen (die mithilfe von Jython-Adaptern erstellt werden)

Anzahl an CIs und Beziehungen

Mit der UCMDB Foundation-Lizenz können eine unbeschränkte Anzahl an CIs und Beziehungen in UCMDB gespeichert oder zwischen UCMDB und anderen BTO-Produkten ausgetauscht werden. Die einzige Beschränkung besteht in der physischen Kapazität und Leistung.

Anzahl an UCMDB-Instanzen

Die UCMDB Foundation-Lizenz erlaubt eine unbegrenzte Anzahl an UCMDB-Instanzen, die in einer Kundenumgebung für die Implementierung von Entwicklungs-, Test-, Produktions-, Hochverfügbarkeits- und/oder Disaster-Recovery-Plattformen bereitgestellt werden können. Bei der Verwaltung und beim Austausch von Daten in einer Installation mit mehreren Instanzen können jedoch technische Beschränkungen bestehen. Server, die von DDM erkannt oder von einem Drittanbieterprodukt bereitgestellt werden, müssen unter der DDM Advanced Edition-Lizenz oder der UCMDB Integration Only-Lizenz nur ein Mal gezählt werden, selbst wenn sie für die betriebliche Verwaltung in mehreren UCMDB-Instanzen angezeigt werden.

Anzahl an Data Flow Probe-Instanzen

Die UCMDB Foundation-Lizenz erlaubt eine unbegrenzte Anzahl an Data Flow Probe-Instanzen, die in einer Kundenumgebung für das Hosting von Discovery- oder Integrationsadaptern bereitgestellt werden können. Bei der maximalen Anzahl an Proben, die sich mit UCMDB verwenden lassen, können jedoch technische Beschränkungen bestehen. Außerdem können manche Adapter, wie bereits zuvor erwähnt, nicht von einer Probe gehostet werden.

Sonderfall BSM

Kunden, die HP Application Performance Manager (APM) Version 9.0x oder höher erwerben, erhalten automatisch eine kostenlose Lizenz, um die integrierte UCMDB-Komponente mit der Bezeichnung „Run-time Service Model“ (RTSM) zu verwenden und um BTO-Produkte mit RTSM zu integrieren. Folglich besitzen und benötigen APM-Kunden keine UCMDB Foundation-Lizenz.

Hinweis: APM wurde früher als HP Business Availability Center Version 8.0x (BAC) und RTSM als Operational Database (ODB) bezeichnet.

UCMDB Integration Only-Lizenz

Diese Lizenz basiert auf der Maßeinheit der verwalteten Server (Informationen hierzu finden Sie unter "Maßeinheiten" auf Seite 49). Kunden, die Drittanbieterprodukte mit UCMDB integrieren möchten, müssen die richtige Anzahl dieser Lizenzen erwerben.

Dieser Abschnitt umfasst folgende Themen:

Lizenzierungsrichtlinie

Für jeden verwalteten Server, der in einem Drittanbieterprodukt definiert ist und dessen Definition anschließend in UCMDB kopiert wird, um in Form von CIs erfasst zu werden, muss eine sogenannte „License to Use“ (LTU) erworben werden. Die UCMDB Integration Only-Lizenz erfordert einen anfänglichen Erwerb von mindestens 100 LTUs.

Gültige Integrationstypen

Mit dieser Lizenz können Sie Drittanbieterprodukte wie folgt mit UCMDB integrieren:

- Standardintegrationen, die von HP bereitgestellt werden
- Standardintegrationen, die von HP-Partnern bereitgestellt werden (möglicherweise mit zusätzlichen Gebühren verbunden)
- Angepasste Datenaustauschintegrationen (d. h. generische Datenbankadapter, generische Push-Adapter und vom Kunden entwickelte Java-Adapter)

- die HP Universal CMDB-Webservice-API und die HP Universal CMDB-API (Java)
- aber nicht Discovery-ähnliche Integrationen (die mithilfe von Jython-Adaptern erstellt werden)

Hinweis: HP Universal CMDB bietet Standardadapter für Drittanbieterprodukte, darunter Microsoft SCCM und BMC Atrium CMDB.

DDM Advanced Edition-Lizenz

Diese Lizenz basiert auf der Maßeinheit der Betriebssysteminstanzen (Informationen hierzu finden Sie unter "Maßeinheiten" auf Seite 49). Kunden, die alle Discovery- und Abhängigkeitszuordnungs-Funktionen von DDM nutzen möchten, müssen die richtige Anzahl dieser Lizenzen erwerben.

Dieser Abschnitt umfasst folgende Themen:

Lizenzierungsrichtlinie

Für jede Betriebssysteminstanz, die von DDM erkannt und in UCMDB in Form von CIs erfasst wird, muss eine LTU erworben werden. Die DDM Advanced Edition-Lizenz erfordert einen anfänglichen Erwerb von mindestens 100 LTUs.

Beispiel: Ein VMware ESX Server, der einen virtuellen Computer hostet, erfordert zwei LTUS.

Server, die sowohl von DDM erkannt als auch von einem Drittanbieterprodukt bereitgestellt werden (um zusätzliche Daten zu erfassen), müssen unter der UCMDB Integration Only-Lizenz nicht mitgezählt werden. Die DDM Advanced Edition-Lizenz deckt dieses Nutzungsszenario ab.

Discovery and Dependency Mapping

Mit dieser Lizenz können Sie die Discovery-Systemsteuerung und andere zugehörige Funktionen verwenden, um alle Discovery-Inhalte direkt zu nutzen. Darüber hinaus können Sie neue Jython-Adapter erstellen, um weitere Ressourcen zu erkennen.

Integrations

Mit dieser Lizenz können Sie das Integration Studio verwenden, um Integrationspunkte mit BTO und Drittanbieterprodukten zu erstellen und dabei Discovery-ähnliche Integrationen zu nutzen (angepasste Jython-Adapter).

Kostenlose DDM Inventory-Berechtigung mit DDM Advanced Edition

Für jede LTU, die Sie unter der DDM Advanced Edition-Lizenz für einen bestimmten Server erwerben, erhalten Sie eine kostenlose DDM Inventory-Lizenz, um Inventardaten auf diesem Server zu erfassen.

Aufgaben

Upgrade auf die Integration Only- oder DDM Advanced Edition-Lizenz

Wenn Sie HP Universal CMDB installieren, erhalten Sie die Universal CMDB Foundation-Lizenz. Um die erforderliche Datei für das Upgrade auf die Integration Only- oder DDM Advanced Edition-Lizenz zu erhalten, müssen Sie sich an HP Software Support wenden und anschließend die folgende Prozedur ausführen:

So führen Sie ein Upgrade Ihrer Lizenz durch:

1. Fordern Sie die entsprechende Datei von HP Software Support an.
2. Ersetzen Sie die Datei **ucmdb_license.xml** im Ordner C:\hp\UCMDB\UCMDBServer\conf\. Der Name der Datei muss ucmdb_license.xml lauten.
3. Erzwingen Sie mit der JMX-Konsole eine Lizenzänderung:
   a. Starten Sie den Webbrowser und geben Sie die Serveradresse wie folgt ein: **http://<UCMDB Server-Hostname oder -IP>:8080/jmx-console**.
   b. Geben Sie die Anmeldeinformationen für die Authentifizierung an der JMX-Konsole ein, wenn Sie dazu aufgefordert werden (falls Ihnen diese Anmeldeinformationen nicht vorliegen, wenden Sie sich an Ihren Systemadministrator). Die Standardwerte für Benutzername und Kennwort lauten **sysadmin**/**sysadmin**.
   c. Klicken Sie unter **UCMDB** auf **service=Server Services**, um die Seite **Operations** zu öffnen.
   d. Suchen Sie **getLicense** und geben Sie die folgenden Informationen ein:

      Geben Sie für den Parameter **customerID** den Wert **1** ein.

      Klicken Sie auf **Invoke**.

      Es werden Informationen zum Lizenztyp, der Kundenname, die erlaubten Packages und Hinweise auf blockierte Applikationen angezeigt.

Referenz

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden die Fehlerbehebung und Einschränkungen für die UCMDB-Lizenzierung erläutert.

- **Problem**: Bei der Integration von UCMDB mit HP Storage Essentials kann der Job zur SE-Integration über SQL mit der Foundation-Lizenz nicht ausgeführt werden.

  Lösung: Führen Sie die Prozedur aus, die im *HP Universal CMDB Discovery and Integration Content Guide* (PDF) unter "Discover the SE Oracle Database" beschrieben wird.

- **Problem**: Bei der Integration von UCMDB mit HP Network Node Manager (NNMi) kann der Job für Ebene 2 über NNM mit der Foundation-Lizenz nicht ausgeführt werden.

  Lösung: Weitere Informationen finden Sie im Abschnitt "Network Node Manager i (NNMi) Integration" im *HP Universal CMDB Discovery and Integration Content Guide* (PDF).

4

Erste Schritte in HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Planung vor der Bereitstellung

Die Bereitstellung von HP Universal CMDB in einer Unternehmensnetzwerkumgebung ist ein Prozess, der eine Ressourcenplanung, einen Systemarchitekturentwurf und eine durchdachte Bereitstellungsstrategie erfordert. Die folgende Checkliste enthält einige grundlegende Aspekte, die vor der Installation berücksichtigt werden müssen. Eine umfassende Dokumentation der Best Practices für die Bereitstellungsplanung erhalten Sie von HP Professional Services.

Prüfen Sie anhand der folgenden Checkliste die grundlegenden Aspekte, die Ihr Unternehmen bei der Planung der Bereitstellung von HP Universal CMDB beachten muss.

✔	**Schritt**
	Definieren Sie die Ziele des Projekts.
	Definieren Sie die Protokolle, die für Data Flow Management (DFM) verwendet werden, und stellen Sie die Verfügbarkeit dieser Protokolle sicher.
	Überprüfen Sie, ob Sie über Zugriffsrechte für die Protokolle verfügen, die für DFM verwendet werden sollen. Fragen Sie den Systemadministrator nach dem Benutzernamen und Kennwort für die relevanten Protokolle.
	Definieren Sie die Geschwindigkeit und Auslastung der Netzwerk-Subnets, die erkannt werden sollen. Möglicherweise stellen Sie fest, dass Sie die Zeitüberschreitungen für bestimmte Protokolle erhöhen müssen.
	Prüfen Sie, ob die folgenden Applikationen die Standardports verwenden. Falls sie nicht die Standardports verwenden, bestimmen Sie, welche Ports sie verwenden. ➤ FTP ➤ IBM HTTP Server ➤ IIS ➤ Microsoft SQL Server ➤ Oracle Server ➤ SAP ➤ SNMP ➤ Siebel ➤ WebLogic ➤ WebSphere
	Bestimmen Sie die Komponenten, die erkannt werden sollen: ➤ Serverhardwareplattform ➤ Serverbetriebssystem mit Version ➤ Netzwerkgerätetypen

✔	**Schritt**
	Installieren Sie die folgenden Tools und Dienstprogramme, um die Analyse der Discovery-Prozesse zu unterstützen: ➤ SNMP-Tool ➤ WMI-Tool ➤ LDAP-Browser ➤ Überwachungstool für Protokolldateien (z. B. BareTail für Windows oder ein UNIX-Überwachungsprogramm)
	Legen Sie fest, wofür Sie HP Universal CMDB einsetzen möchten: ➤ Zuordnung von Systemkomponenten ➤ Ursachenanalyse ➤ Auswirkungsanalyse ➤ Verlegung/Konsolidierung von Rechenzentren
	Analysieren Sie die IT-Prozesse und die Unternehmensstruktur und -kultur, die sich auf die Bereitstellung auswirken können oder auf die sich die Bereitstellung auswirken kann.
	Analysieren Sie die Unternehmensziele und bestimmen Sie die wichtigen IT-gestützten Geschäftsprozesse zum Erreichen dieser Ziele.
	Bestimmen Sie die betroffenen Benutzer (mit maßgeblichem Interesse an den Geschäftsprozessen), darunter Führungskräfte, Spartenleiter, Applikationseigentümer, Systemadministratoren und Sicherheitsbeauftragte.
	Stimmen Sie das Projekt mit den derzeitigen Leistungsverwaltungsverfahren ab.
	Definieren Sie die Projektergebnisse, z. B. in Form von erwarteten Messwerten, Funktionen, Bereitstellungsumfang und Reifegraden.
	Bestimmen Sie die geeignete HP Universal CMDB-Funktionalität.
	Erstellen Sie eine Roadmap für die Bereitstellung.
	Definieren Sie Erfolgskriterien für das Projekt.
	Entscheiden Sie, wie oft Sie DFM ausführen möchten. Weiter Informationen finden Sie unter "Dialogfeld "Discovery-Scheduler"" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

Aufgaben

Erste Schritte

Dieser Abschnitt enthält eine grundlegende, schrittweise Einführung in das Arbeiten mit HP Universal CMDB.

1 Informieren Sie sich, wo Sie Hilfe erhalten.

Lernen Sie die verschiedenen Unterstützungsquellen kennen, darunter HP Professional Services und HP Software Support sowie die HP Universal CMDB-Dokumentation. Weitere Informationen finden Sie unter "Willkommen bei diesem Handbuch" auf Seite 15.

2 Informieren Sie sich über die HP Universal CMDB-Komponenten.

Lernen Sie die Komponenten kennen, aus denen das HP Universal CMDB-System besteht. Weitere Informationen finden Sie unter "HP Universal CMDB – Übersicht" auf Seite 26.

3 Planen Sie Ihre HP Universal CMDB-Bereitstellung.

Erstellen Sie einen vollständigen Bereitstellungsplan, bevor Sie HP Universal CMDB installieren. Verwenden Sie die Checkliste zur Planung vor der Bereitstellung. Ausführliche Best Practices für die Bereitstellungsplanung erhalten Sie von Ihrem Ansprechpartner bei HP Professional Services. Weitere Informationen finden Sie unter "Planung vor der Bereitstellung" auf Seite 60.

4 Installieren Sie die HP Universal CMDB-Komponenten.

Installieren Sie den Server (auf einem Windows- oder Linux-System) und die Data Flow Probe. Weitere Informationen finden Sie in Teil II, "Installation des UCMDB-Servers".

5 Melden Sie sich in HP Universal CMDB an.

Starten Sie HP Universal CMDB. Weitere Informationen finden Sie unter "Zugreifen auf HP Universal CMDB" auf Seite 441.

6 Beginnen Sie mit der Systemverwaltung.

Richten Sie das HP Universal CMDB-System ein. Weiter Informationen finden Sie unter "Verwaltung" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Grundlegende Verwaltungsaufgaben

Dieser Abschnitt enthält eine Checkliste für grundlegende Verwaltungs- und Konfigurationsaufgaben. Mithilfe dieser Checkliste können Sie die grundlegenden Verwaltungsaufgaben prüfen, die zum Einrichten des HP Universal CMDB-Systems erforderlich sind.

1 Richten Sie Data Flow Management (DFM) ein.

Lizenzierte DDM-Benutzer können den Discovery-Prozess ausführen, um IT-Ressourcen in der Netzwerkinfrastruktur zu ermitteln. Weitere Informationen finden Sie im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

2 Fordern Sie beim Einrichten von DFM die folgenden Informationen vom Systemadministrator an:

- Anmeldeinformationen für das Betriebssystem
- Anmeldeinformationen für Netzwerkprotokolle
- Anmeldeinformationen für Applikationen

3 Richten Sie die Benutzer ein.

Definieren Sie Berechtigungen für Ansichten. Durch Berechtigungen wird Benutzern der Zugriff auf Ansichten, TQLs und andere Komponenten gewährt oder verweigert. Weitere Informationen finden Sie in den Abschnitten "Einrichten von und Arbeiten mit Benutzern" und "Security Manager" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

4 Konfigurieren Sie die Empfänger geplanter Reports, einschließlich Bereitstellungsmethode.

Weiter Informationen finden Sie unter "Reports" im *HP Universal CMDB – Modellierungshandbuch* (PDF).

5 Erstellen Sie manuell Ihr IT Universe-Modell, indem Sie CIs (Konfigurationselemente) und CI-Beziehungen im Modell definieren.

Unterteilen Sie das Modell in Ansichten, die logische Teilbereiche des Gesamtmodells abbilden. Fügen Sie CIs anhand erkannter Netzwerkressourcen hinzu oder definieren Sie Infrastrukturkomponenten manuell.

Weitere Informationen finden Sie unter:

- "IT Universe Manager" im *HP Universal CMDB – Modellierungshandbuch* (PDF)
- "Modeling Studio" im *HP Universal CMDB – Modellierungshandbuch* (PDF)

Teil II

Installation des UCMDB-Servers

5

Installationsprozedur

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Konzepte

Installationsprozedur – Übersicht

Während der Installation werden die folgenden HP Universal CMDB-Komponenten installiert:

- HP Universal CMDB Server
- CMDB-Datenbank (Configuration Management Database)
- History-Datenbank
- HP Universal CMDB-Packages
- Data Flow Management-Probe (falls eine geeignete Lizenz vorliegt – weitere Informationen finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47)

Wichtig: HP Universal CMDB darf **nur** ein Mal auf einem Server installiert werden, selbst wenn die Instanzen in verschiedenen Ordnern installiert werden oder verschiedene Versionen aufweisen.

Installationsphasen

Der Installationsworkflow besteht aus den folgenden Hauptphasen:

1 Einrichten der CMDB- und History-Datenbanken.

Die Einrichtung von HP Universal CMDB erfolgt entweder unter Microsoft SQL Server oder unter Oracle Server.

Weitere Informationen finden Sie unter "Bereitstellen und Verwalten der Microsoft SQL Server-Datenbank" und "Bereitstellen und Verwalten der Oracle Server-Datenbank" im *HP Universal CMDB – Datenbankhandbuch* (PDF).

2 Anfordern der geeigneten HP Universal CMDB-Lizenz.

Speichern Sie die Lizenz auf einem Computer, auf den Sie von dem Computer aus zugreifen können, auf dem Sie HP Universal CMDB installieren.

Weitere Informationen finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.

3 Installieren von HP Universal CMDB Server.

Weitere Informationen finden Sie unter "Installieren von HP Universal CMDB auf einer Windows-Plattform" auf Seite 73 oder "Installieren von HP Universal CMDB auf einer Linux-Plattform" auf Seite 89.

Am Ende der Serverinstallation wird die Installationsprozedur direkt mit der Installation der Datenbanken (CMDB und History) fortgesetzt. Sie können eine neue Datenbank (Microsoft SQL Server) oder ein neues Schema (Oracle Server) erstellen oder eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herstellen. Weitere Informationen finden Sie unter "UCMDB-Serverkonfiguration" auf Seite 105.

Hinweis: Werk-Packages werden automatisch nur ein Mal beim ersten Starten des Servers bereitgestellt.

---

4 Installieren der Collectors (Data Flow Probes). Weitere Informationen finden Sie unter "Installieren der Data Flow Probe auf der Windows-Plattform" auf Seite 137 oder "Installieren der Data Flow Probe auf der Linux-Plattform" auf Seite 157.

5 Einrichten der Zugriffsberechtigungen für UCMDB Server und die Data Flow Probe.

Weitere Informationen finden Sie in Teil VI, "Härten von HP Universal CMDB".

6 Einrichten der Authentifizierungsberechtigungen für den UCMDB Server-Service.

7 Starten von HP Universal CMDB.

Weitere Informationen finden Sie unter "Zugriffsbefehle für den UCMDB-Server" auf Seite 131.

6

Installieren von HP Universal CMDB auf einer Windows-Plattform

Wichtig: Wenn Sie eine Service-Pack-Version installieren (z. B. 9.02), finden Sie die aktuellen Anweisungen in den Versionshinweisen.

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Installationsvoraussetzungen

Beachten Sie vor dem Installieren von HP Universal CMDB folgende Punkte:

- Es wird dringend empfohlen, dass Sie gründlich die Einführung in diesem Handbuch lesen, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter "Einführung in HP Universal CMDB" auf Seite 25.
- Installieren Sie HP Universal CMDB nicht auf einem Laufwerk, das einer Netzwerkressource zugeordnet ist.
- Aufgrund von Webbrowser-Beschränkungen dürfen die Namen von Servercomputern, auf denen der HP Universal CMDB Server ausgeführt wird, nur aus alphanumerischen Zeichen (a-z, A-Z, 0-9), Bindestrichen (-) und Punkten (.) bestehen.

  Wenn die Namen der Computer, auf denen HP Universal CMDB Server ausgeführt wird, Unterstriche enthalten, können Sie sich möglicherweise nicht in HP Universal CMDB anmelden. In diesem Fall müssen Sie die IP-Adresse des Computers anstatt des Computernamens verwenden.
- **Wichtig:** HP Universal CMDB darf **nur** ein Mal auf einem Server installiert werden, selbst wenn die Instanzen in verschiedenen Ordnern installiert werden oder verschiedene Versionen aufweisen.
- Namen von Datenbankbenutzern und Kennwörter dürfen alphanumerische Zeichen aus dem Zeichensatz der Datenbank sowie Unterstriche enthalten. Namen müssen mit einem alphabetischen Zeichen beginnen und dürfen maximal 30 Zeichen lang sein.
- Das HP Universal CMDB-Programmverzeichnis darf nur englische Zeichen enthalten.
- Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.
- Informationen zur Fehlerbehebung bei der Anmeldung finden Sie unter "Verfügbare Fehlerbehebungsressourcen" auf Seite 459.

- **Wichtig:** Wenn Sie ein Upgrade Ihrer aktuellen Version auf 9.02 durchführen, lesen Sie das Kapitel "Upgrade für HP Universal CMDB von Version 8.0x auf Version 9.0x" auf Seite 173, bevor Sie Ihre aktuelle Version deinstallieren. In diesem Kapitel wird im Abschnitt "Durchführen der Prozeduren nach dem Upgrade" auf Seite 179 erklärt, wie Sie den Verlust der Adapterkonfigurationsdateien vermeiden.
- Halten Sie die folgenden Informationen bereit, bevor Sie mit der Installation beginnen:
  - Informationen zum Festlegen der Parameter für die CMDB- und CMDB History-Datenbanken. Wenn Sie diese Datenbankeneinstellungen während der Servereinrichtung vornehmen möchten, finden Sie unter "UCMDB-Serverkonfiguration" auf Seite 105 weitere Informationen.
  - Wenn Sie den UCMDB Server auf einer gehärteten Plattform (einschließlich Verwendung des HTTPS-Protokolls) ausführen möchten, lesen Sie die Härtungsprozeduren in Teil VI, "Härten von HP Universal CMDB".
  - E-Mail-Adresse des Administrators. (Optional)
  - Name des SMTP-Mailservers. (Optional)
  - SMTP-Absendername. Dieser Name wird in Alerts angezeigt, die UCMDB sendet. (Optional)

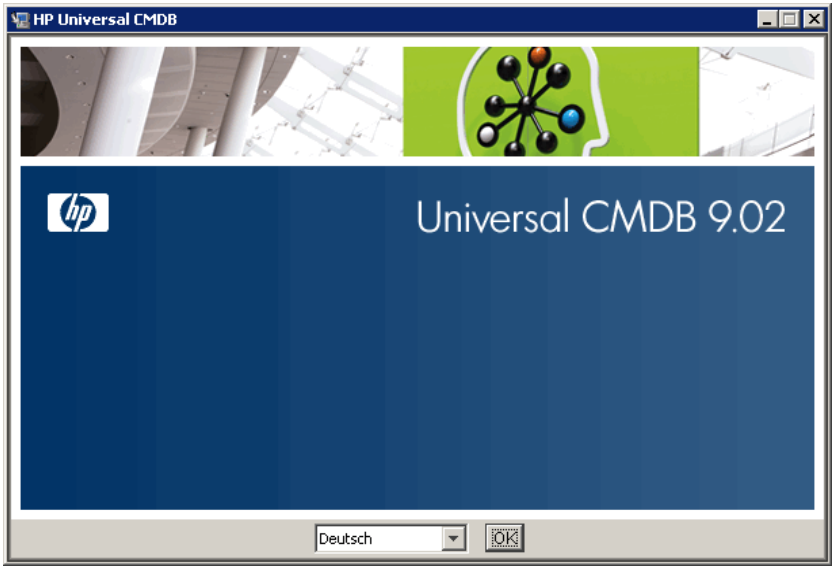
Aufgaben

Installieren von UCMDB

In der folgenden Prozedur wird erklärt, wie Sie HP Universal CMDB installieren.

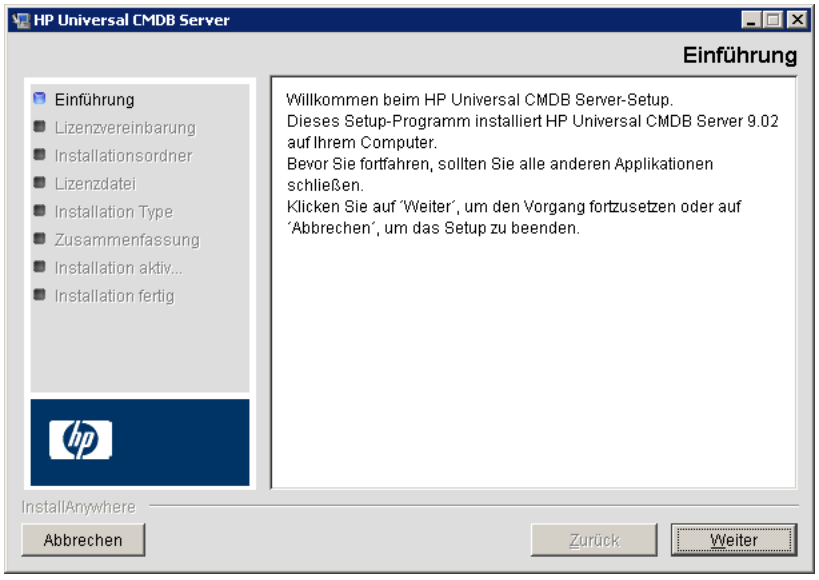
1. Wenn Sie von einem Netzwerklaufwerk aus installieren, stellen Sie eine Verbindung zu diesem Laufwerk her.
2. Suchen Sie die ausführbare Datei für UCMDB: **HPUCMDB_Server_902.exe**.
3. Doppelklicken Sie auf die Datei, um den Startbildschirm zu öffnen.

   Wenn die digitale Signatur gültig ist, wird der Startbildschirm geöffnet:

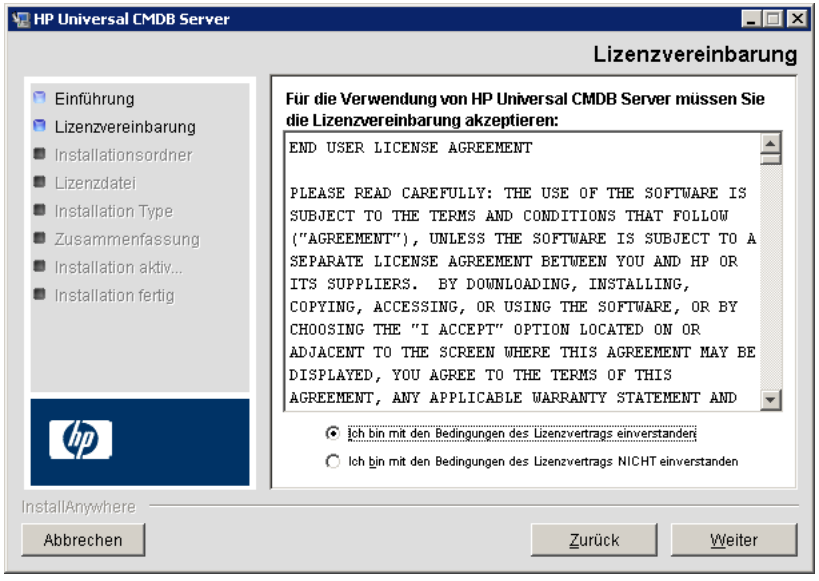


4. Wählen Sie die Gebietssprache aus und klicken Sie auf **OK**.

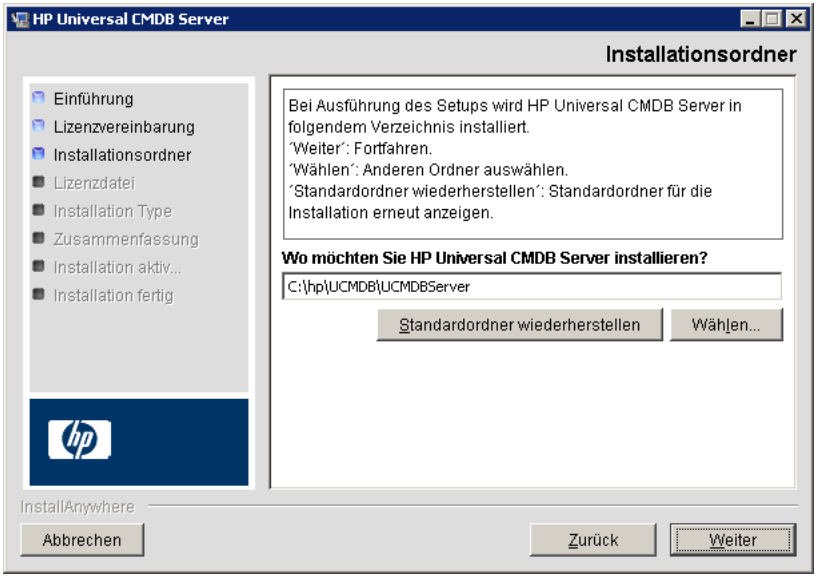
Das Dialogfeld **Einführung** wird geöffnet.



5 Klicken Sie auf **Weiter**, um das Dialogfeld **Lizenzvereinbarung** zu öffnen.



Akzeptieren Sie die Bedingungen der Lizenz und klicken Sie auf **Weiter**, um das Dialogfeld **Installationsordner** zu öffnen.

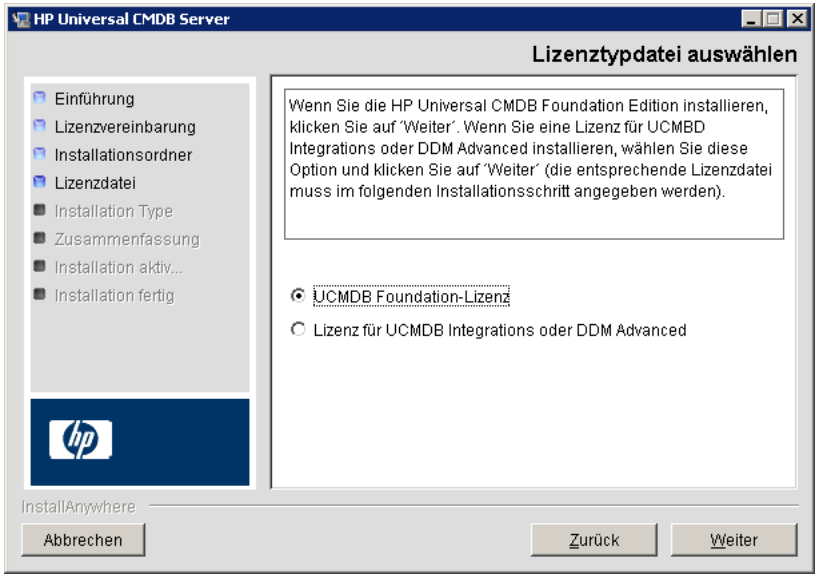


Übernehmen Sie die Standardeinstellung oder klicken Sie auf **Auswählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Zum Installieren in einem anderen Verzeichnis suchen Sie den entsprechenden Installationsorder und wählen ihn aus. Der Installationspfad darf keine Leerzeichen enthalten.

Tipp: Um wieder den Standardinstallationsordner anzuzeigen, klicken Sie auf **Standardordner wiederherstellen**.

---

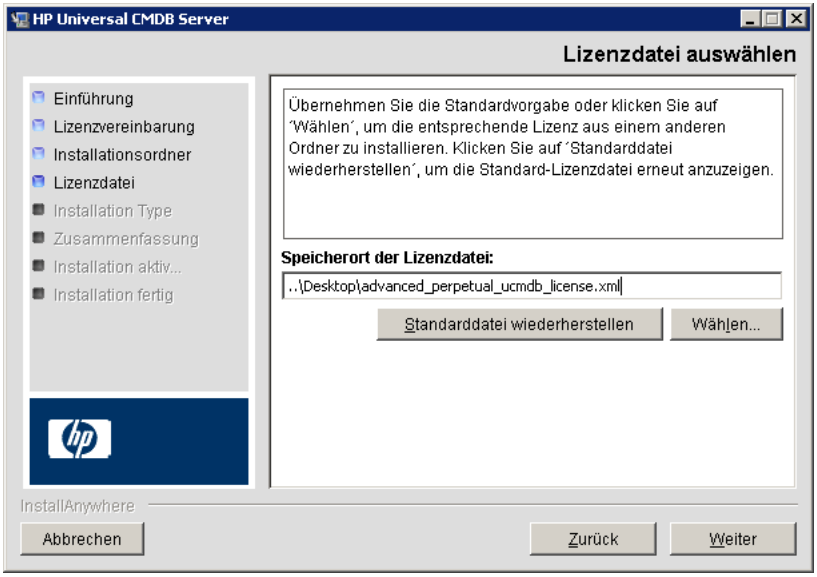
6 Klicken Sie auf **Weiter**, um das Dialogfeld **Lizenztypdatei wählen** zu öffnen.



Übernehmen Sie zum Installieren der Foundation-Lizenz die Standardeinstellung. Um die Integrations- oder DDM Advanced-Lizenz zu installieren, wählen Sie die entsprechende Option aus. Weitere Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.

Wenn Sie die UCMDB Foundation-Lizenz auswählen, fahren Sie mit Schritt 7 auf Seite 81 fort.

Wenn Sie die UCMDB Integrations- oder DDM Advanced-Lizenz ausgewählt haben, klicken Sie auf **Weiter**, um das Dialogfeld **Lizenzdatei wählen** zu öffnen.

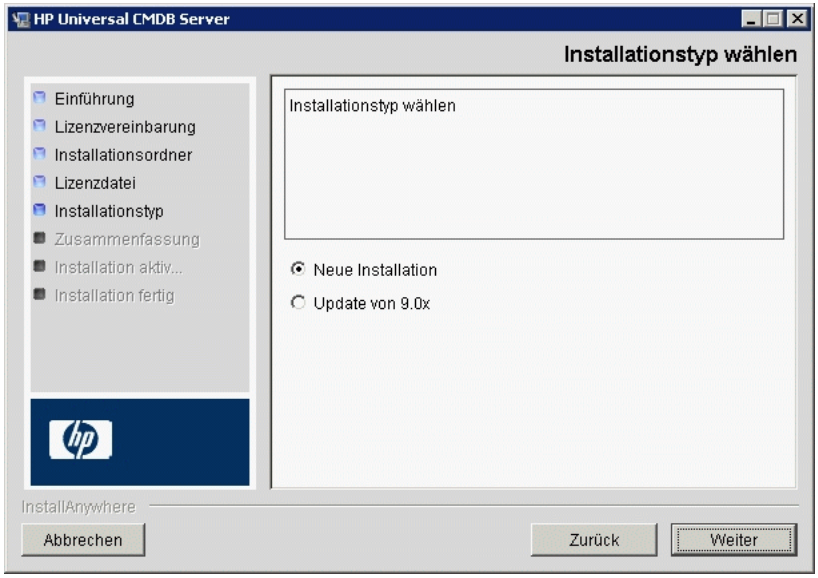


Übernehmen Sie die Standardeinstellung oder klicken Sie auf **Auswählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Suchen Sie den Ordner mit der Lizenzdatei und wählen Sie ihn aus. Wählen Sie die Lizenzdatei (**ucmdb_license.xml**) aus.

Tipp: Um wieder die Standardinstallationsdatei anzuzeigen, klicken Sie auf **Standarddatei wiederherstellen**.

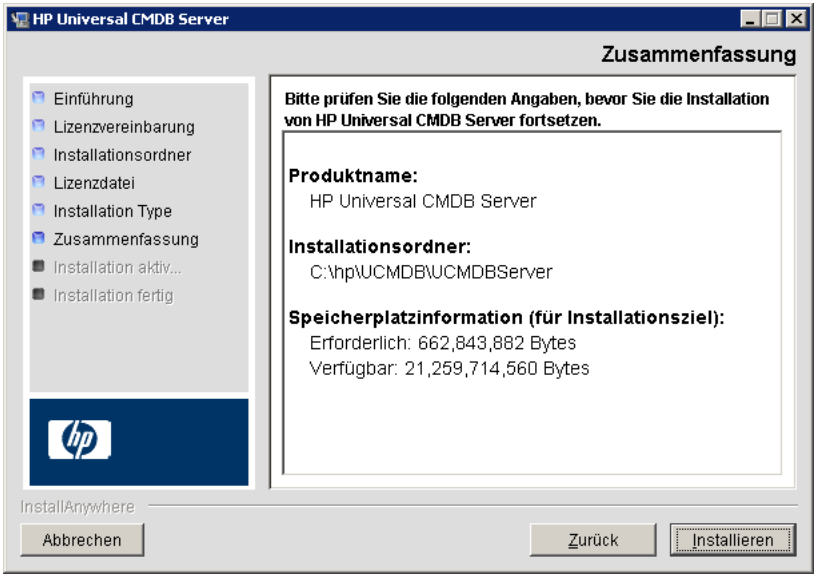
---

7 Klicken Sie auf **Weiter**, um das Dialogfeld **Installationstyp wählen** zu öffnen.



Wählen Sie **Neue Installation** aus, wenn Sie eine vollständige Produktinstallation durchführen. Wählen Sie **Update von 9.0x** aus, wenn Sie eine Patchinstallation durchführen.

8 Klicken Sie auf **Weiter**, um das Dialogfeld **Zusammenfassung** zu öffnen, in dem die ausgewählten Installationsoptionen aufgeführt sind.



9 Wenn die Zusammenfassung korrekt ist, klicken Sie auf **Installieren**. Eine Meldung zeigt an, dass die Installation durchgeführt wird.

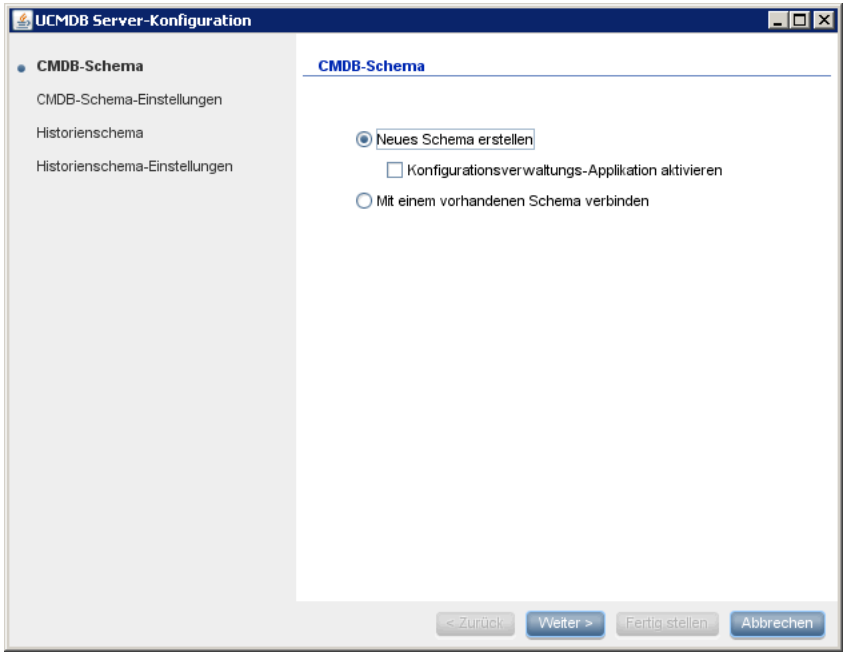
10 Nach Abschluss der Installation wird die Meldung **HP Universal CMDB Server konfigurieren** angezeigt:

In der nächsten Phase der Prozedur wird der UCMDB Server-Konfigurationsassistent gestartet (um die Datenbank oder das Schema einzurichten). Klicken Sie auf **Ja**, um mit der Konfiguration fortzufahren.

Wenn Sie ein Upgrade von Version 8.0x auf 9.02 durchführen, klicken Sie auf **Nein** und fahren Sie mit der Prozedur unter "Installieren der Data Flow Probe für Version 9.02" auf Seite 180 fort.

Sie können die Datenbank oder das Schema auch später einrichten. Rufen Sie dazu den UCMDB Server-Konfigurationsassistenten über das Windows-Startmenü auf.

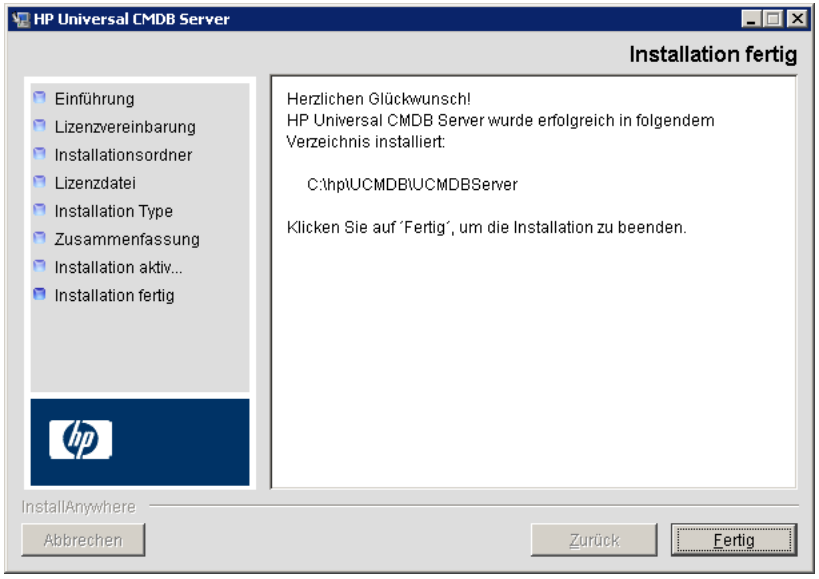
Das Dialogfeld **UCMDB Server-Konfiguration** wird geöffnet.



In den folgenden Phasen wählen Sie aus, ob Sie eine neue Datenbank oder ein neues Schema (Microsoft SQL Server oder Oracle Server) erstellen möchten oder ob Sie eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herstellen möchten. In der Regel erstellen Sie eine neue Datenbank oder ein neues Schema für eine neue Installation von HP Universal CMDB, während Sie eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herstellen, wenn Sie einen Server erneut installieren oder einen zusätzlichen Server installieren.

- Eine Einführung zum Erstellen einer Datenbank bzw. zum Verbinden mit einer Datenbank finden Sie unter "Auswählen der Datenbank oder des Schemas" auf Seite 106.
- Die Prozedur zum Erstellen einer Microsoft SQL Server-Datenbank finden Sie unter "Erstellen einer Microsoft SQL Server-Datenbank" auf Seite 110.
- Die Prozedur zum Erstellen eines Oracle-Schemas finden Sie unter "Erstellen eines Oracle-Schemas" auf Seite 116.
- Die Prozedur zum Verbinden mit einer vorhandenen Microsoft SQL Server-Datenbank finden Sie unter "Verbinden mit einer vorhandenen Microsoft SQL Server-Datenbank" auf Seite 121.
- Die Prozedur zum Verbinden mit einem vorhandenen Oracle-Schema finden Sie unter "Verbinden mit einem vorhandenen Oracle-Schema" auf Seite 121.

11 Wenn Sie die Konfiguration im Konfigurationsassistenten beendet haben, wird das Dialogfeld **Installation fertig** geöffnet.



12 Klicken Sie auf **Fertig**, um die Installation abzuschließen.

Konfigurieren des UCMDB-Mailservers

Führen Sie diese Prozedur nach der Installation von HP Universal CMDB durch.

So konfigurieren Sie den UCMDB-Mailserver:

1 Wählen Sie die Kategorie **Verwaltung** > **Infrastructure Settings Manager** > **Maileinstellungen** aus.

2 Definieren Sie die Einstellung **SMTP-Server**: Geben Sie den Namen des SMTP-Servers ein.

3 Bearbeiten Sie die Einstellung **SMTP-Server-Port**: Der Standardwert lautet 25.

4 Als Backup für den primären SMTP-Server können Sie Informationen zu einem alternativen Server eingeben. Wiederholen Sie die Schritte 2 und 3 und geben Sie dabei unter **Alternativer SMTP-Server** sowie unter **Port des alternativen SMTP-Servers** die entsprechenden Angaben ein.

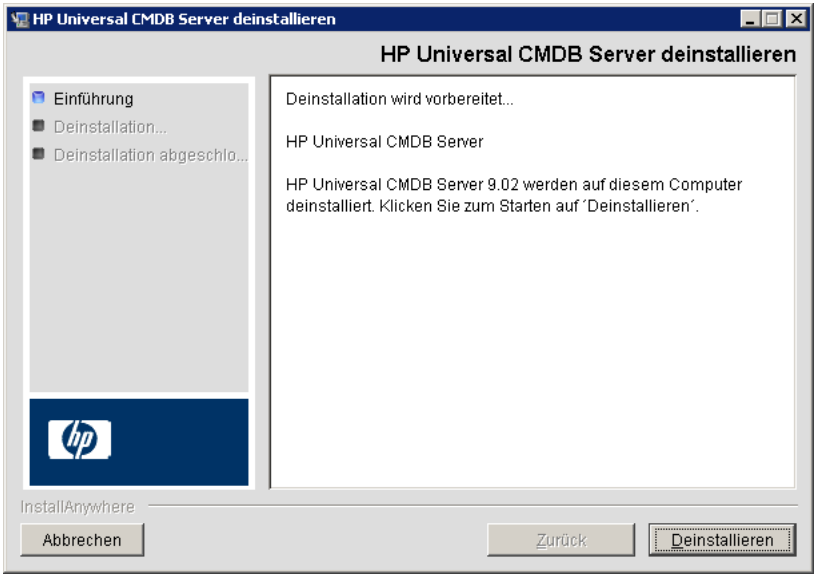
5 Ändern Sie die Einstellung für **E-Mail-Absender** in den Namen, der in von HP Universal CMDB gesendeten Reports angezeigt werden soll.

6 Damit Benutzer den Namen unter **E-Mail-Absender** in Mailformularen bearbeiten können, ändern Sie den Wert für **Absender kann bearbeitet werden** in **True**. Andernfalls belassen Sie den Wert auf **False**.

Deinstallieren von HP Universal CMDB

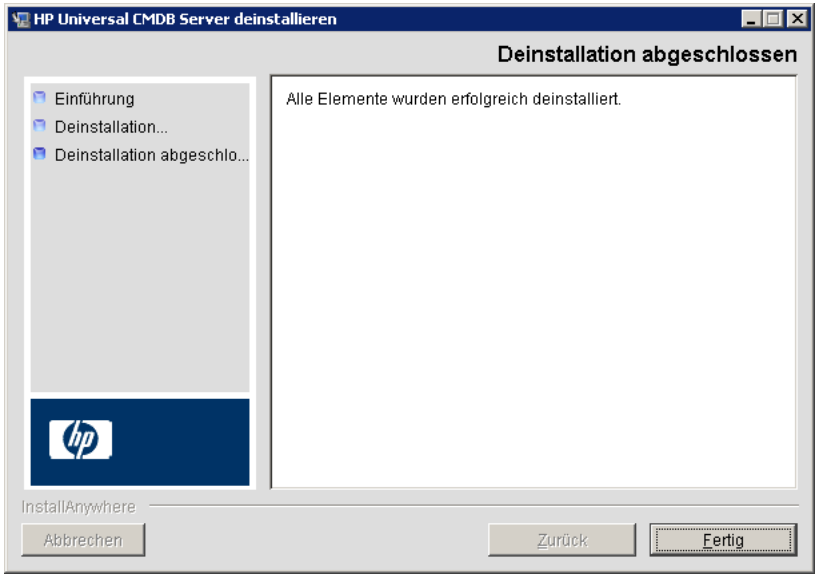
In der folgenden Prozedur wird erklärt, wie Sie HP Universal CMDB deinstallieren.

1 Wählen Sie im Startmenü **Alle Programme** > **HP UCMDB** > **HP Universal CMDB Server starten** > **HP Universal CMDB Server deinstallieren** aus. Das Dialogfeld **HP Universal CMDB Server deinstallieren** wird geöffnet.



2 Klicken Sie auf **Deinstallieren**.

Nach Abschluss der Deinstallation wird eine Bestätigungsmeldung angezeigt:



3 Klicken Sie auf **Fertig**.

7

Installieren von HP Universal CMDB auf einer Linux-Plattform

Wichtig: Wenn Sie eine Service-Pack-Version installieren (z. B. 9.02), finden Sie die aktuellen Anweisungen in den Versionshinweisen.

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Installationsvoraussetzungen

Beachten Sie vor dem Installieren von HP Universal CMDB folgende Punkte:

- Es wird dringend empfohlen, dass Sie gründlich die Einführung in diesem Handbuch lesen, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter "Einführung in HP Universal CMDB" auf Seite 25.
- Aufgrund von Webbrowser-Beschränkungen dürfen die Namen von Servercomputern, auf denen der HP Universal CMDB Server ausgeführt wird, nur aus alphanumerischen Zeichen (a-z, A-Z, 0-9), Bindestrichen (-) und Punkten (.) bestehen.

  Wenn die Namen der Computer, auf denen HP Universal CMDB Server ausgeführt wird, Unterstriche enthalten, können Sie sich möglicherweise nicht in HP Universal CMDB anmelden. In diesem Fall müssen Sie die IP-Adresse des Computers anstatt des Computernamens verwenden.
- **Wichtig:** HP Universal CMDB darf **nur** ein Mal auf einem Server installiert werden, selbst wenn die Instanzen in verschiedenen Ordnern installiert werden oder verschiedene Versionen aufweisen.
- Wenden Sie die folgende Konfiguration auf den Linux-Computer an:
  - /etc/sysctl.conf. Fügen Sie den Wert für **fs.file-max** hinzu oder ändern Sie ihn in
    fs.file-max = 300000
  - /etc/security/limits.conf. Fügen Sie am Ende der Datei Folgendes hinzu:
    *** soft nofile 20480**
    *** soft nofile 20480**

Hinweis: Sie benötigen vermutlich die entsprechenden Berechtigungen zum Ändern dieser Dateien. Sie müssen den Linux-Computer möglicherweise neu starten, damit die Änderungen wirksam werden.

- Namen von Datenbankbenutzern und Kennwörter dürfen alphanumerische Zeichen aus dem Zeichensatz der Datenbank sowie Unterstriche enthalten. Namen müssen mit einem alphabetischen Zeichen beginnen und dürfen maximal 30 Zeichen lang sein.
- Das HP Universal CMDB-Programmverzeichnis darf nur englische Zeichen enthalten.
- Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.
- Informationen zur Fehlerbehebung bei der Anmeldung finden Sie unter "Verfügbare Fehlerbehebungsressourcen" auf Seite 459.
- Halten Sie die folgenden Informationen bereit, bevor Sie mit der Installation beginnen:
  - Informationen zum Festlegen der Parameter für die CMDB- und CMDB History-Datenbanken. Wenn Sie diese Datenbankeneinstellungen während der Servereinrichtung vornehmen möchten, finden Sie unter "UCMDB-Serverkonfiguration" auf Seite 105 weitere Informationen.
  - Wenn Sie den UCMDB Server auf einer gehärteten Plattform (einschließlich Verwendung des HTTPS-Protokolls) ausführen möchten, lesen Sie die Härtungsprozeduren in Teil VI, "Härten von HP Universal CMDB".

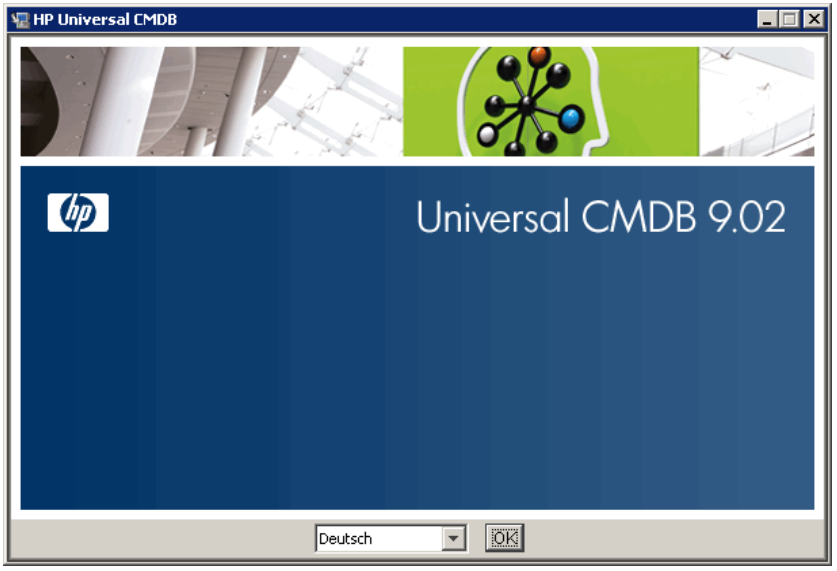
Aufgaben

Installieren von HP Universal CMDB

In der folgenden Prozedur wird erklärt, wie Sie HP Universal CMDB installieren.

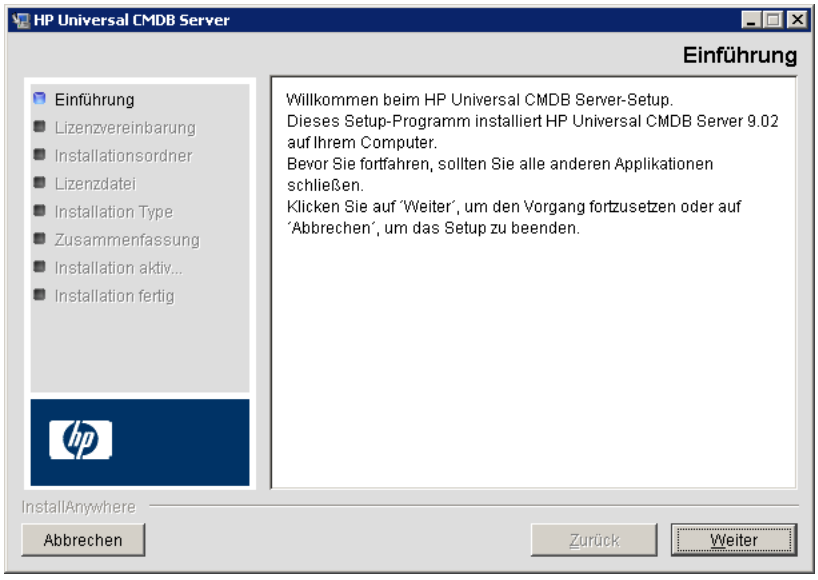
1. Bei der Installation von HP Universal CMDB unter Linux handelt es sich um eine grafikbasierte Installation. Bevor Sie das Installationsprogramm ausführen, konfigurieren Sie die Umgebungsvariable **DISPLAY** so, dass sie auf eine ausgeführte Instanz eines X Windows-Servers verweist.
2. Suchen Sie die ausführbare Datei für UCMDB: **HPUCMDB_Server_902.bin**.
3. Führen Sie die folgende Datei aus: **sh <Pfad zur Installationsdatei>/HPUCMDB_Server_902.bin**.

   Der Startbildschirm wird angezeigt:

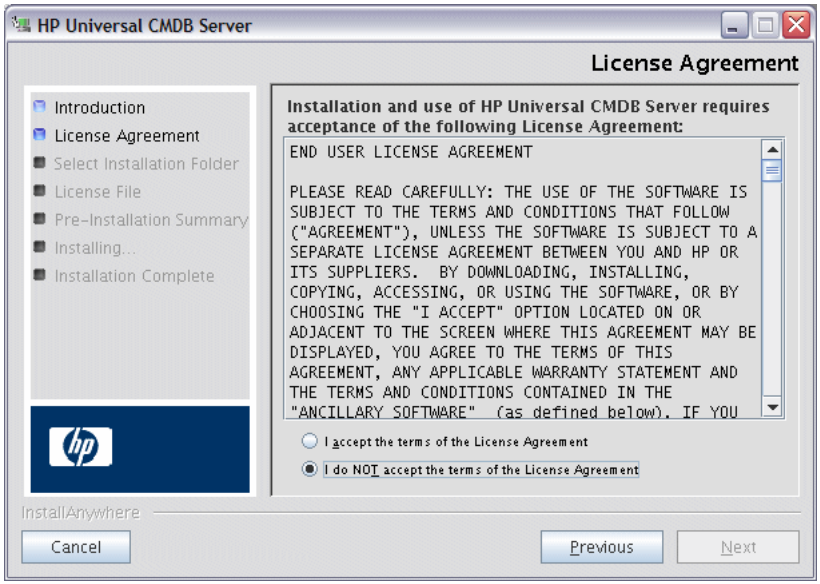


4. Wählen Sie die Gebietssprache aus und klicken Sie auf **OK**.

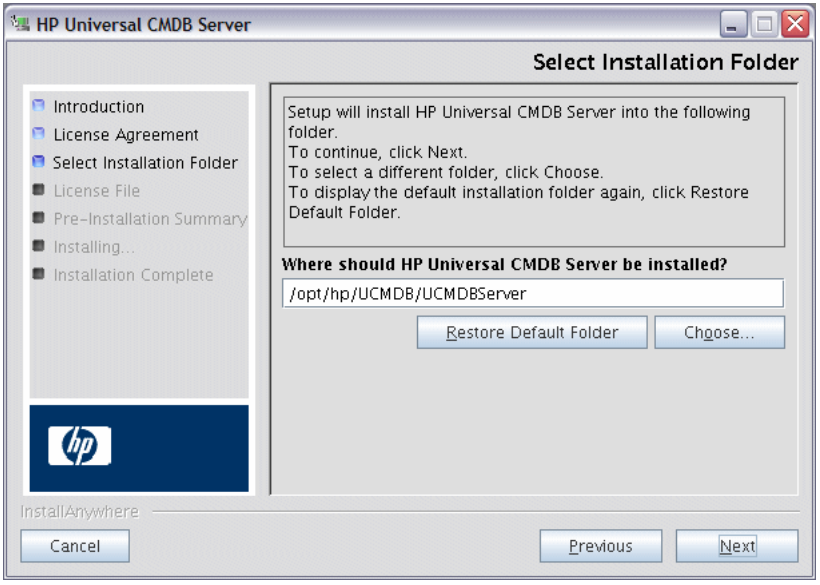
Das Dialogfeld **Einführung** wird geöffnet.



5 Klicken Sie auf **Weiter**, um das Dialogfeld **Lizenzvereinbarung** zu öffnen.



Akzeptieren Sie die Bedingungen der Lizenz und klicken Sie auf **Weiter**, um das Dialogfeld **Installationsordner** zu öffnen.

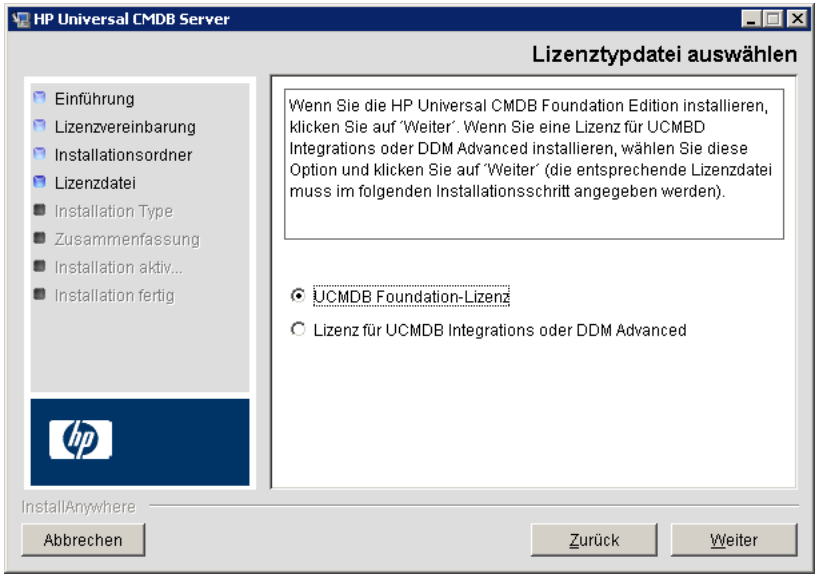


Geben Sie einen anderen Pfad ein oder klicken Sie auf **Auswählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Zum Installieren in einem anderen Verzeichnis suchen Sie den entsprechenden Installationsorder und wählen ihn aus. Der Installationspfad darf keine Leerzeichen enthalten.

Tipp: Um wieder den Standardinstallationsordner anzuzeigen, klicken Sie auf **Standardordner wiederherstellen**.

---

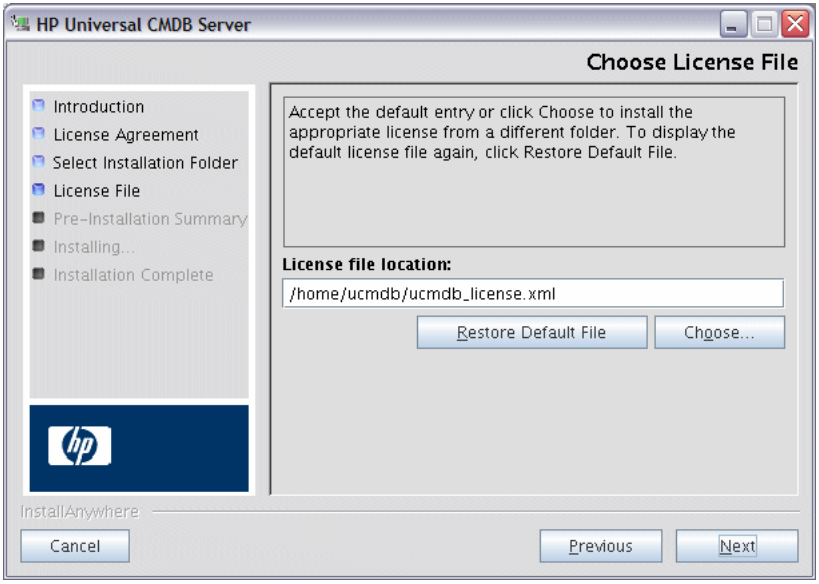
6 Klicken Sie auf **Weiter**, um das Dialogfeld **Lizenztypdatei wählen** zu öffnen.



Übernehmen Sie zum Installieren der Foundation-Lizenz die Standardeinstellung. Um die Integrations- oder DDM Advanced-Lizenz zu installieren, wählen Sie die entsprechende Option aus. Weitere Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.

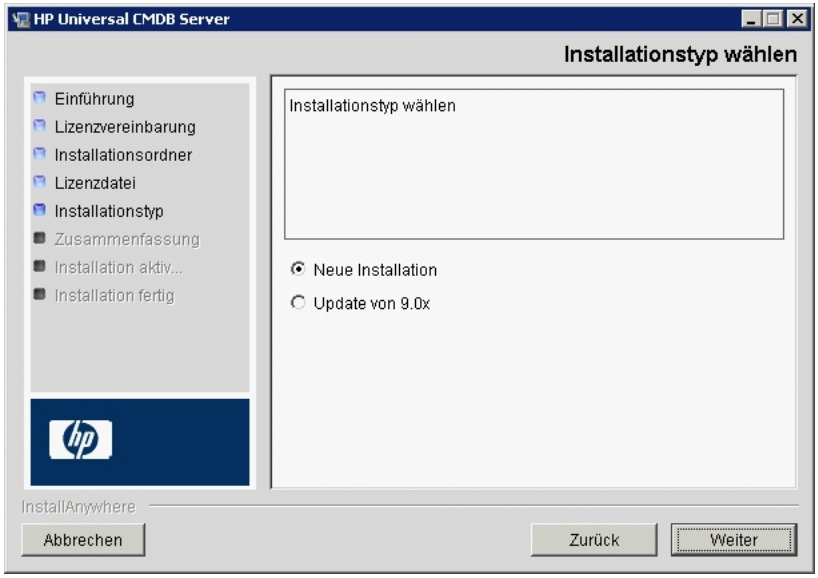
Wenn Sie die UCMDB Foundation-Lizenz auswählen, fahren Sie mit Schritt 8 fort.

Wenn Sie die UCMDB Integrations- oder DDM Advanced-Lizenz ausgewählt haben, klicken Sie auf **Weiter**, um das Dialogfeld **Lizenzdatei wählen** zu öffnen.



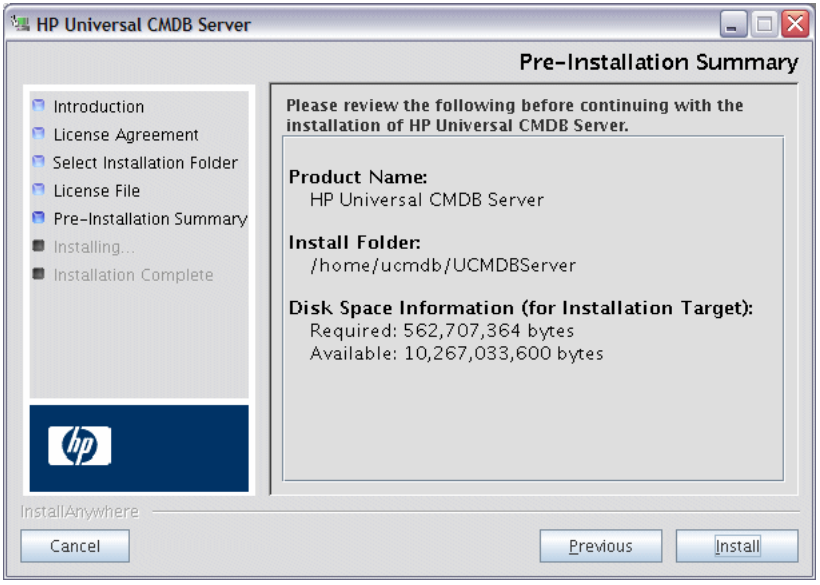
Klicken Sie auf **Auswählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Suchen Sie den Ordner mit der Lizenzdatei und wählen Sie ihn aus. Wählen Sie die Lizenzdatei (**ucmdb_license.xml**) aus.

7 Klicken Sie auf **Weiter**, um das Dialogfeld **Installationstyp wählen** zu öffnen.



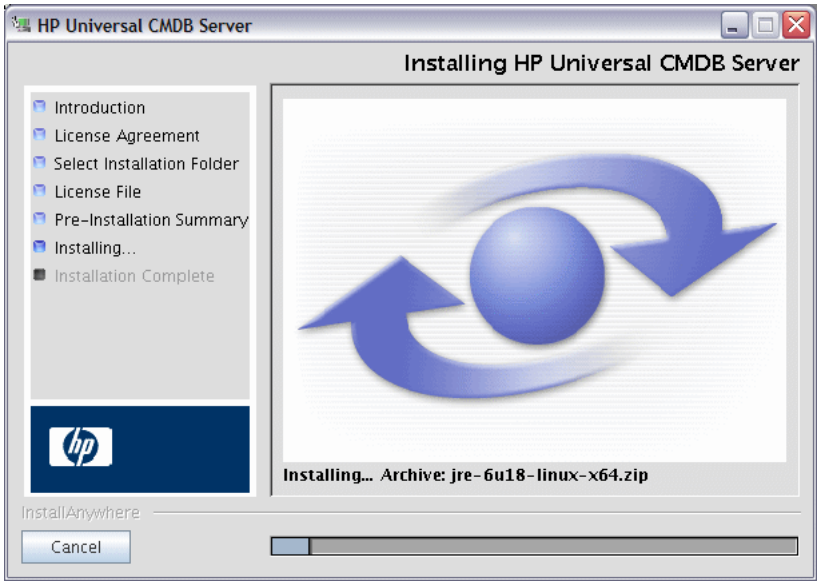
Wählen Sie **Neue Installation** aus, wenn Sie eine vollständige Produktinstallation durchführen. Wählen Sie **Update von 9.0x** aus, wenn Sie eine Patchinstallation durchführen.

8 Klicken Sie auf **Weiter**, um das Dialogfeld **Zusammenfassung** zu öffnen, in dem die ausgewählten Installationsoptionen aufgeführt sind.

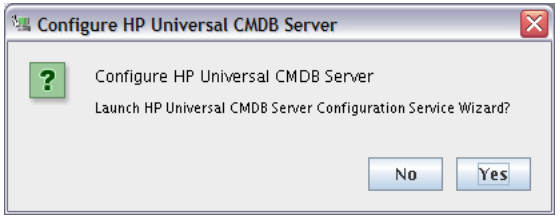


Wenn die Zusammenfassung korrekt ist, klicken Sie auf **Installieren**.

9 Eine Meldung zeigt an, dass die Installation durchgeführt wird.



Die Meldung **HP Universal CMDB Server konfigurieren** wird angezeigt:

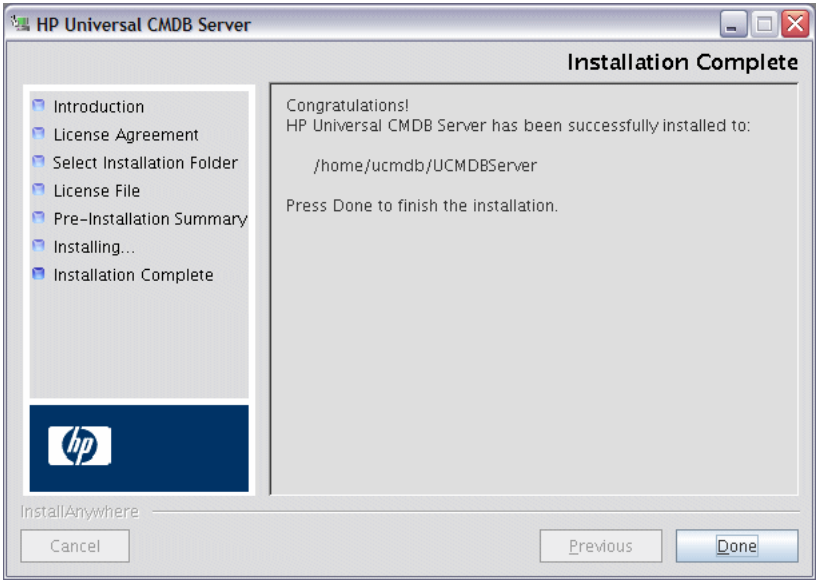


10 Klicken Sie auf **Ja**, um mit der Konfiguration fortzufahren und das Dialogfeld zur HP Universal CMDB Server-Konfiguration zu öffnen.

Sie können die Datenbank oder das Schema aber auch später einrichten. Führen Sie in diesem Fall das Skript **configure.sh** aus, das sich im Unterordner **bin** des Installationsordners befindet.

11 In den folgenden Phasen wählen Sie aus, ob Sie eine neue Datenbank oder ein neues Schema (Microsoft SQL Server oder Oracle Server) erstellen möchten oder ob Sie eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herstellen möchten. In der Regel erstellen Sie eine neue Datenbank oder ein neues Schema für eine neue Installation von HP Universal CMDB, während Sie eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herstellen, wenn Sie einen Server erneut installieren oder einen zusätzlichen Server installieren. Eine Einführung zum Erstellen einer Datenbank bzw. zum Verbinden mit einer Datenbank finden Sie unter "Auswählen der Datenbank oder des Schemas" auf Seite 106.

12 Wenn Sie die Konfiguration im Konfigurationsassistenten beendet haben, wird das Dialogfeld **Installation fertig** geöffnet. Klicken Sie auf **Fertig**, um die Installation abzuschließen.



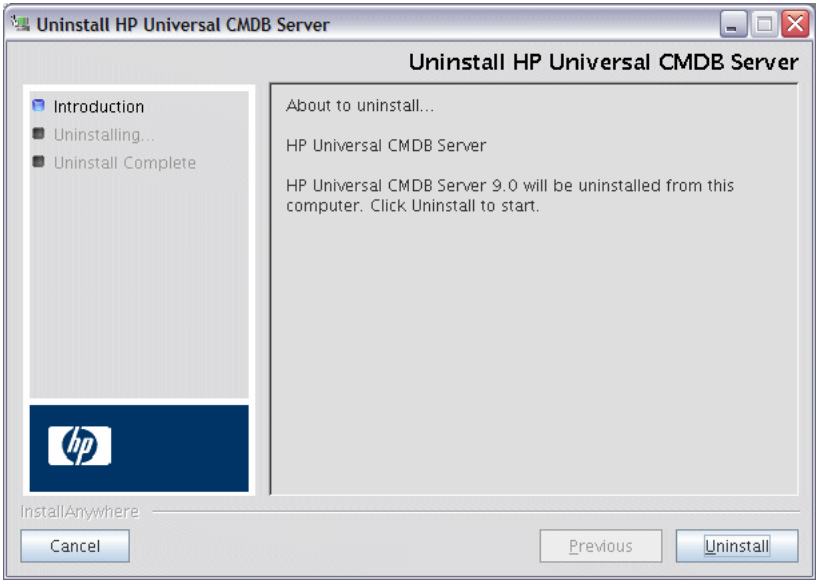
Konfigurieren des UCMDB-Mailservers

1. Wählen Sie die Kategorie **Verwaltung** > **Infrastructure Settings Manager** > **Maileinstellungen** aus.
2. Definieren Sie die Einstellung **SMTP-Server**: Geben Sie den Namen des SMTP-Servers ein.
3. Bearbeiten Sie die Einstellung **SMTP-Server-Port**: Der Standardwert lautet 25.
4. Als Backup für den primären SMTP-Server können Sie Informationen zu einem alternativen Server eingeben. Wiederholen Sie die Schritte 2 und 3 und geben Sie dabei unter **Alternativer SMTP-Server** sowie unter **Port des alternativen SMTP-Servers** die entsprechenden Angaben ein.
5. Ändern Sie die Einstellung für **E-Mail-Absender** in den Namen, der in von HP Universal CMDB gesendeten Reports angezeigt werden soll.
6. Damit Benutzer den Namen unter **E-Mail-Absender** in Mailformularen bearbeiten können, ändern Sie den Wert für **Absender kann bearbeitet werden** in **True**. Andernfalls belassen Sie den Wert auf **False**.

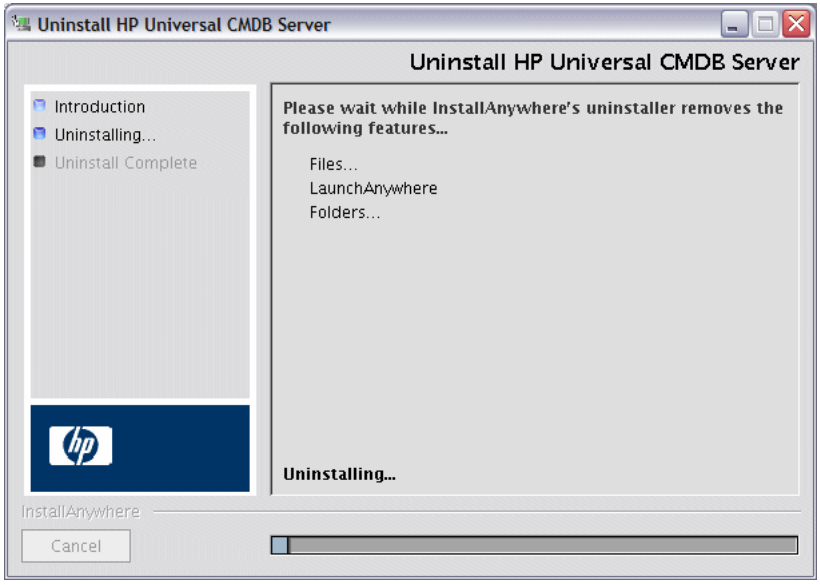
Deinstallieren von UCMDB

Die folgende Prozedur dient zum Deinstallieren von UCMDB.

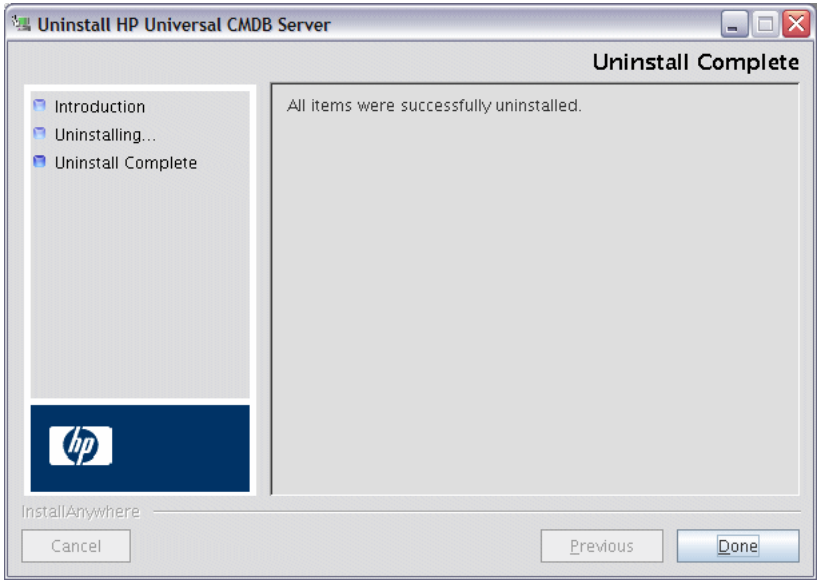
1 Führen Sie das Skript **Uninstall_UCMDBServer** aus dem Unterordner **UninstallerData** des Installationsordners aus.



2 Wählen Sie im selben Ordner **Deinstallieren** aus, um HP Universal CMDB Server zu deinstallieren.



3 Klicken Sie auf **Fertig**, um die Deinstallation abzuschließen.



8

UCMDB-Serverkonfiguration

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Auswählen der Datenbank oder des Schemas

Im Folgenden wird die zweite Phase der Installationsprozedur beschrieben, die das Starten des UCMDB Server-Konfigurationsassistenten beinhaltet (um die Datenbank oder das Schema einzurichten). Weitere Informationen zur ersten Phase der Installation finden Sie unter "Installieren von HP Universal CMDB auf einer Windows-Plattform" auf Seite 73 oder "Installieren von HP Universal CMDB auf einer Linux-Plattform" auf Seite 89.

Hinweis: Es wird dringend empfohlen, dass Sie gründlich die Einführung in diesem Handbuch lesen, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter "Einführung in HP Universal CMDB" auf Seite 25.

Während der Installation müssen Sie entscheiden, ob Sie die Datenbankbenutzer erstellen oder vordefinierte Benutzer verwenden möchten. Diese Entscheidung treffen Sie bei HP Universal CMDB zum selben Zeitpunkt, an dem Sie auch die Datenbank auswählen, auf der die Applikation ausgeführt werden soll:

Entscheiden Sie sich in den folgenden Fällen für das Erstellen eines Datenbank- oder Schemabenutzers:

- Es sind keine Datenbankbenutzer vorhanden.
- Es sind Datenbankbenutzer vorhanden, aber Sie möchten die Standardinhalte der Datenbank initialisieren.

Entscheiden Sie sich in den folgenden Fällen für das Verbinden mit einem vorhandenen Datenbank- oder Schemabenutzer:

- Sie möchten ein Upgrade auf eine neuere Version von HP Universal CMDB durchführen und die Datenbankinhalte aus der vorherigen Version von HP Universal CMDB verwenden.

- Sie möchten die Standardinhalte der Datenbank nicht ändern, z. B. weil Ihre Datenbank oder Ihr Schema Daten aus einer früheren Installation desselben Release enthält. In diesem Fall werden die erforderlichen Serverkonfigurationsdateien bei der Einrichtung mit den Datenbankdetails aktualisiert; die Konfigurationsdatei für Datenbankskripts wird ebenfalls aktualisiert. Weitere Informationen finden Sie im *HP Universal CMDB – Datenbankhandbuch* (PDF).
- Von Ihrem Datenbankadministrator erhalten Sie Anweisungen für das Erstellen der Datenbankbenutzer vorab im Einklang mit der Unternehmensrichtlinie. Informationen zum manuellen Erstellen von Microsoft SQL Server-Datenbanken oder Oracle-Schemas finden Sie im *HP Universal CMDB – Datenbankhandbuch* (PDF).

Erforderliche Informationen zum Festlegen von Datenbankparametern

Bevor Sie Parameter für die CMDB- und CMDB History-Datenbanken festlegen, müssen Sie die in den folgenden Abschnitten beschriebenen Informationen vorbereiten.

Bereitstellen von Microsoft SQL Server

Sie benötigen die folgenden Informationen, um neue Datenbanken zu erstellen und eine Verbindung zu vorhandenen Datenbanken herzustellen:

- **Hostname.** Der Name des Computers, auf dem Microsoft SQL Server installiert ist. Wenn Sie eine Verbindung zu einer Nicht-Standardinstanz von Microsoft SQL Server herstellen, geben Sie Folgendes ein: <Hostname>\<Instanzname>
- **Port.** Der TCP/IP-Port von Microsoft SQL Server. HP Universal CMDB zeigt automatisch den Standardport **1433** an.
- **Datenbankname (Schemaname).** Der Name der vorhandenen Datenbank oder der Name, den Sie der neuen Datenbank zuweisen (z. B. UCMDB_History).

➤ **Benutzername und Kennwort.** (Wenn Sie Microsoft SQL Server-Authentifizierung verwenden.) Der Benutzername und das Kennwort eines Benutzers mit Administratorrechten unter Microsoft SQL Server. Der Standard-Benutzername des Microsoft SQL Server-Administrators lautet **sa**. Beachten Sie, dass ein Kennwort eingegeben werden muss.

Sie können eine Datenbank erstellen oder eine Verbindung zu einer Datenbank herstellen, indem Sie Windows-Authentifizierung anstelle von Microsoft SQL Server-Authentifizierung verwenden. Dazu müssen Sie sicherstellen, dass der Windows-Benutzer, der den HP Universal CMDB-Service ausführt, die erforderlichen Zugriffsberechtigungen für die Microsoft SQL Server-Datenbank besitzt. Weitere Informationen zum Zuweisen eines Windows-Benutzers für die Ausführung des HP Universal CMDB-Services finden Sie unter "Ändern des HP Universal CMDB Server-Servicebenutzers" auf Seite 301. Weitere Informationen zum Hinzufügen eines Windows-Benutzers zu Microsoft SQL Server finden Sie unter "Verwenden der Windows-Authentifizierung für den Zugriff auf Microsoft SQL Server-Datenbanken" im *HP Universal CMDB – Datenbankhandbuch* (PDF).

Bereitstellen von Oracle Server

Stellen Sie vor dem Festlegen von Parametern für die CMDB- und CMDB History-Datenbanken sicher, dass Sie mindestens einen Standard-Tablespace für jedes Benutzerschema erstellt haben, um Datenpersistenz zu erzielen, und dass jedem Benutzerschema mindestens ein temporärer Tablespace zugewiesen wurde.

Sowohl zum Erstellen eines neuen Benutzerschemas als auch zum Verbinden mit einem vorhandenen Benutzerschema benötigen Sie die folgenden Informationen:

➤ **Hostname.** Der Name des Hostcomputers, auf dem Oracle Server installiert ist.

➤ **Port.** Der Oracle-Listener-Port. HP Universal CMDB zeigt automatisch den Standardport **1521** an.

➤ **SID.** Der Oracle-Instanzname zur eindeutigen Erkennung der Oracle-Datenbankinstanz, die von HP Universal CMDB verwendet wird.

➤ **Schemaname and Schemakennwort.** Der Name und das Kennwort des vorhandenen Benutzerschemas oder der Name, den Sie dem neuen Benutzerschema zuweisen (z. B. UCMDB_FOUNDATION).

Wenn Sie ein neues Benutzerschema erstellen, benötigen Sie die folgenden Zusatzinformationen:

➤ **Administratorname und Administratorkennwort** (um eine Verbindung als Administrator herzustellen). Der Name und das Kennwort eines Benutzers mit Administratorrechten unter Oracle Server (z. B. ein System-Benutzer).

➤ **Standard-Tablespace.** Der Name des Standard-Tablespace, den Sie für das Benutzerschema erstellt haben. Weitere Informationen zum Erstellen eines HP Universal CMDB-Tablespace finden Sie unter "Manuelles Erstellen der Oracle Database Server-Schemas" im *HP Universal CMDB – Datenbankhandbuch* (PDF).

➤ **Temporärer Tablespace.** Der Name des temporären Tablespace, den Sie dem Benutzerschema zugewiesen haben. Der temporäre Standard-Tablespace für Oracle lautet **temp**.

Hinweis: Zum Erstellen eines neuen Benutzerschemas benötigen Sie Berechtigungen für das Erstellen von Benutzern.

Aufgaben

Aufrufen des UCMDB Server-Konfigurationsassistenten

Wenn Sie die Datenbank oder das Schema nicht während der Installation eingerichtet haben, können Sie es einrichten, indem Sie den UCMDB Server-Konfigurationsassistenten aufrufen. Wählen Sie dazu im Windows-Startmenü **Start > Alle Programme > HP UCMDB > Konfigurationsassistenten für HP Universal CMDB Server starten** aus.

Erstellen einer Microsoft SQL Server-Datenbank

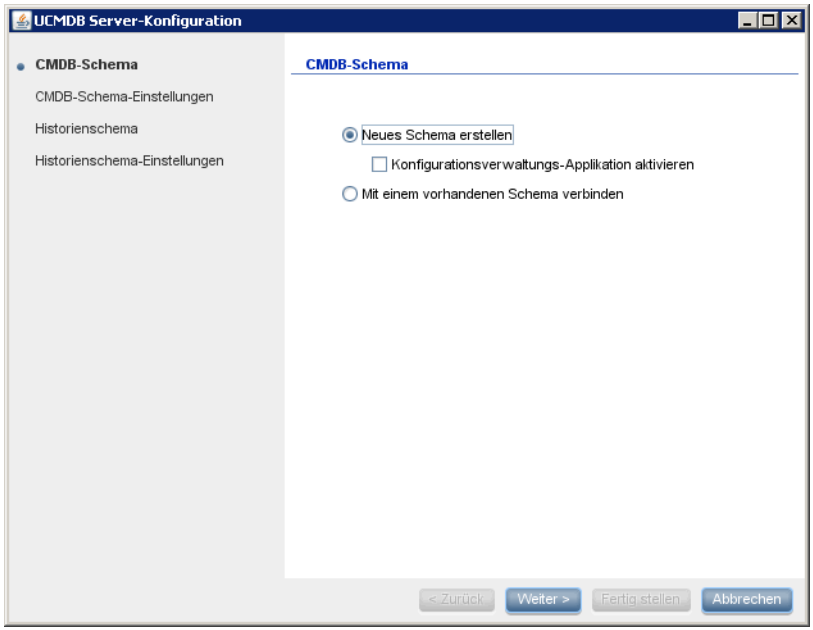
In diesem Abschnitt wird erklärt, wie Sie die Microsoft SQL Server-Datenbank einrichten. Diese Installationsphase besteht aus zwei Teilen, nämlich dem Einrichten der CMDB-Datenbank und der CMDB History-Datenbank.

Hinweis: In UCMDB Version 9.00 oder höher sind die Foundations- und CMDB-Datenbanken kombiniert. Informationen zu Upgrades finden Sie unter "Upgrade für HP Universal CMDB von Version 8.0x auf Version 9.0x" auf Seite 173.

So richten Sie die Microsoft SQL Server-Datenbank ein:

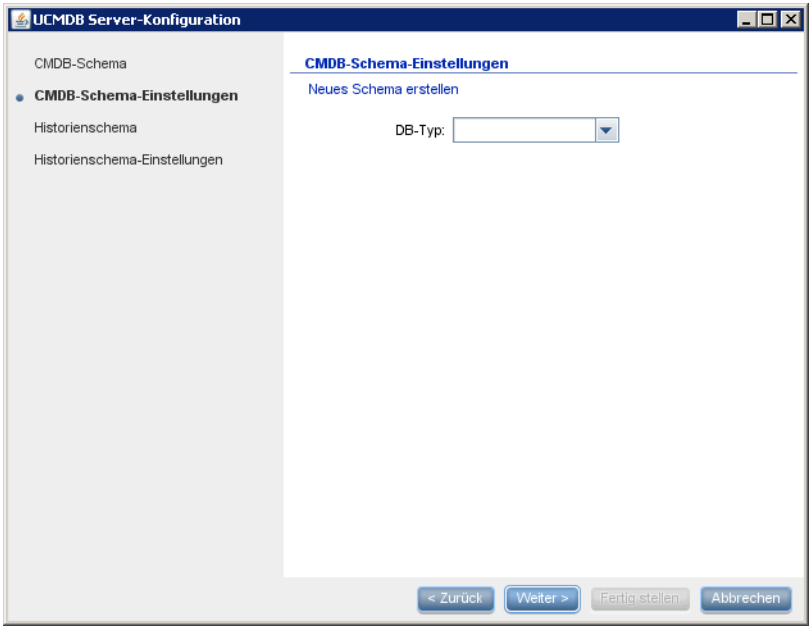
1 Klicken Sie nach der Installation auf **Weiter**, um das Dialogfeld **CMDB-Schema** zu öffnen.

Hinweis: Nach beendeter Installation können Sie den UCMDB Server-Konfigurationsassistenten über das Windows-Startmenü aufrufen. Weitere Informationen finden Sie unter "Aufrufen des UCMDB Server-Konfigurationsassistenten" auf Seite 110.



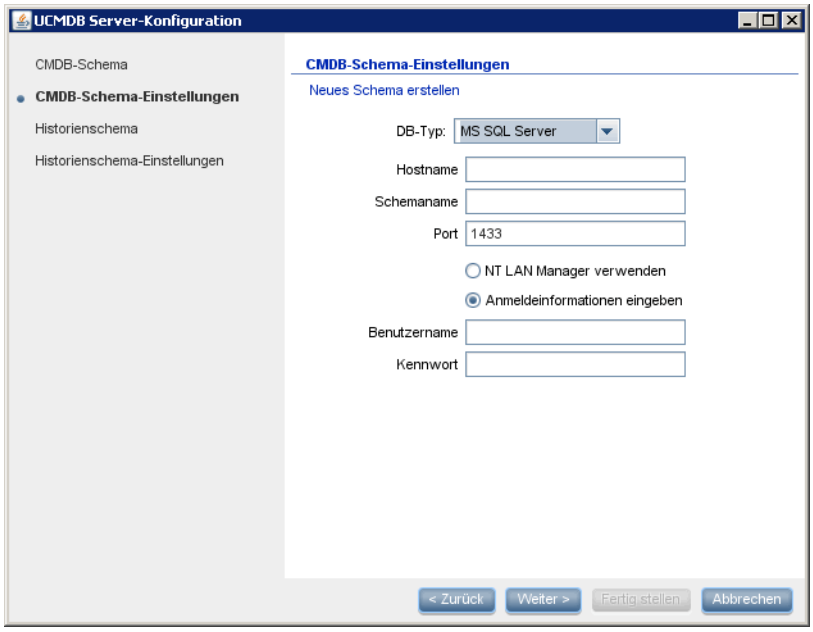
Wählen Sie **Neues Schema erstellen** aus.

2 Klicken Sie auf **Weiter**, um das Dialogfeld **CMDB-Schema-Einstellungen** zu öffnen.



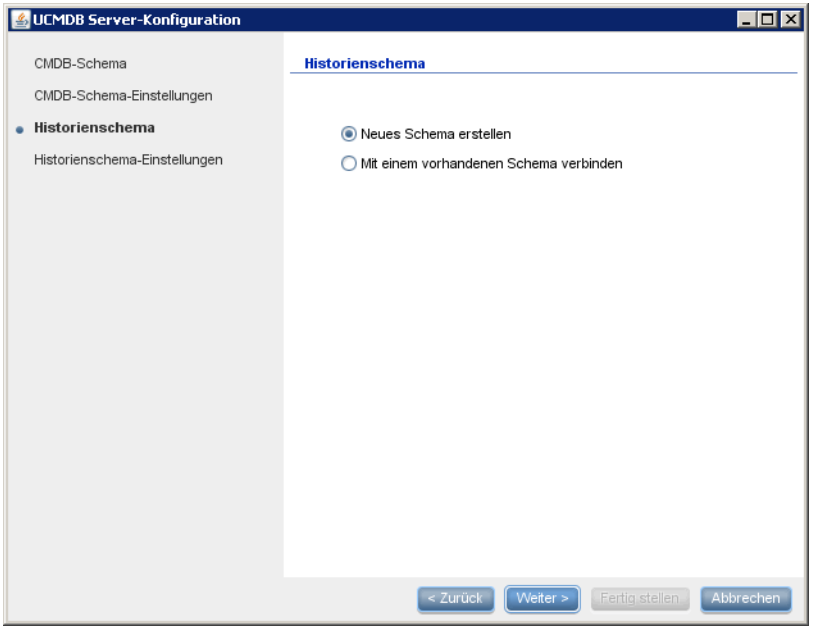
Wählen Sie **MS SQL Server** aus.

3 Im Dialogfeld werden zusätzliche Felder angezeigt.



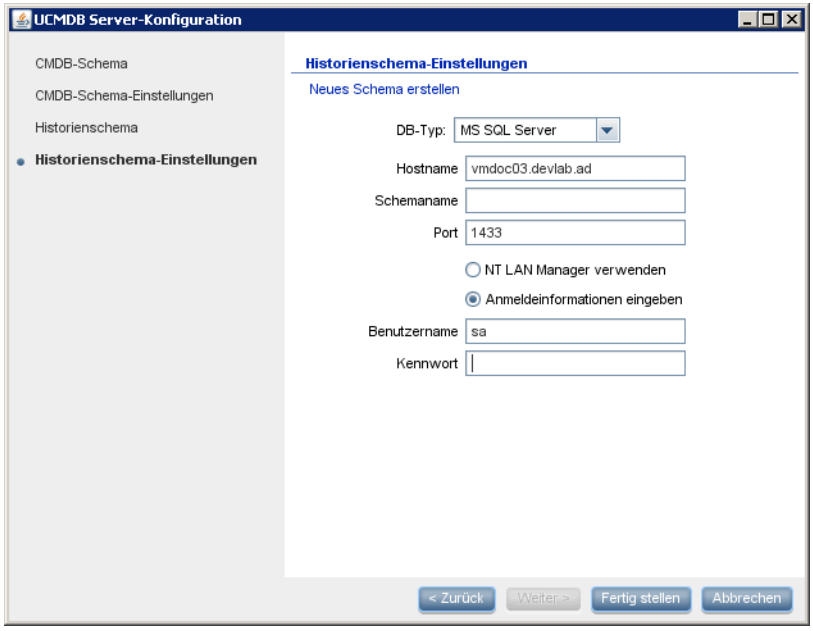
4 Geben Sie den Hostnamen und Datenbanknamen ein und entscheiden Sie, welche Authentifizierung HP Universal CMDB für die Verbindung zum Datenbankserver verwenden soll. Weitere Informationen zur Windows-Authentifizierung finden Sie unter "Verwenden der Windows-Authentifizierung für den Zugriff auf Microsoft SQL Server-Datenbanken" im *HP Universal CMDB – Datenbankhandbuch* (PDF).

5 Klicken Sie auf **Weiter**. Die CMDB-Datenbank wird erstellt. Das Dialogfeld **Historienschema** wird angezeigt.



Wählen Sie **Neues Schema erstellen** aus.

6 Klicken Sie auf **Weiter**, um das Dialogfeld **Historienschema-Einstellungen** zu öffnen.



Wählen Sie **MS SQL Server** aus. Die Werte, die Sie für die CMDB-Einstellungen eingegeben haben, werden im Dialogfeld angezeigt.

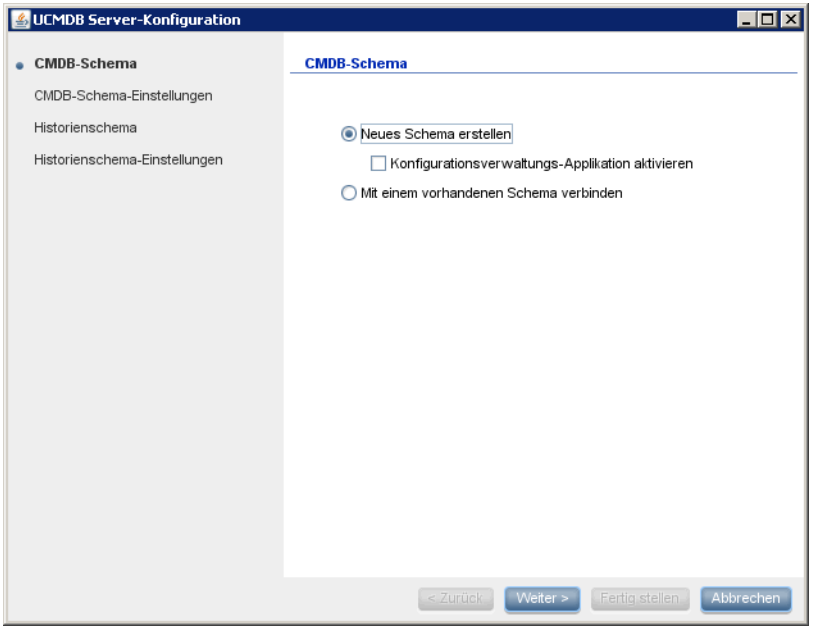
7 Klicken Sie auf **Fertig stellen**. Die CMDB History-Datenbank wird erstellt.

Erstellen eines Oracle-Schemas

In diesem Abschnitt wird erklärt, wie Sie das Oracle-Schema einrichten. Diese Installationsphase besteht aus zwei Teilen, nämlich dem Einrichten des CMDB-Schemas und des CMDB History-Schemas.

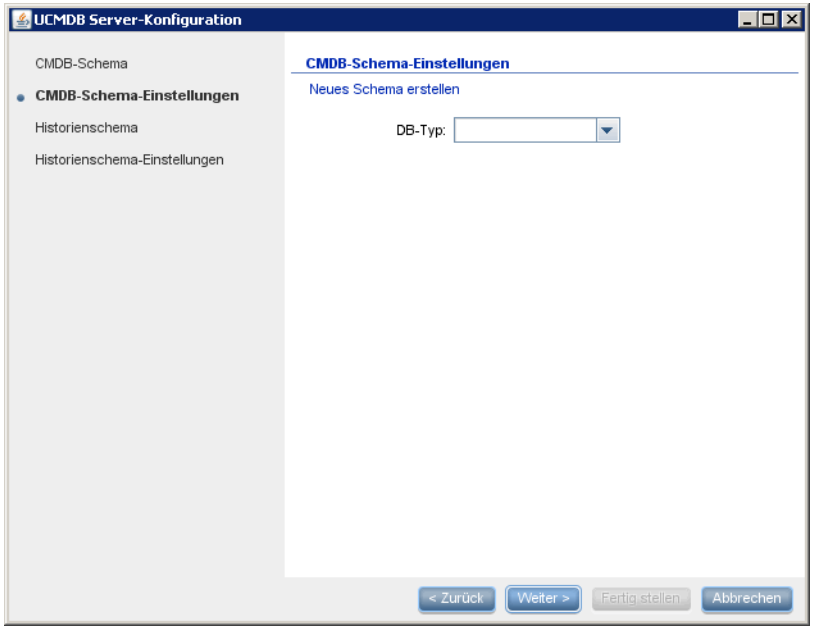
So richten Sie das Oracle-Schema ein:

1 Klicken Sie nach der Installation auf **Weiter**, um das Dialogfeld **CMDB-Schema** zu öffnen.



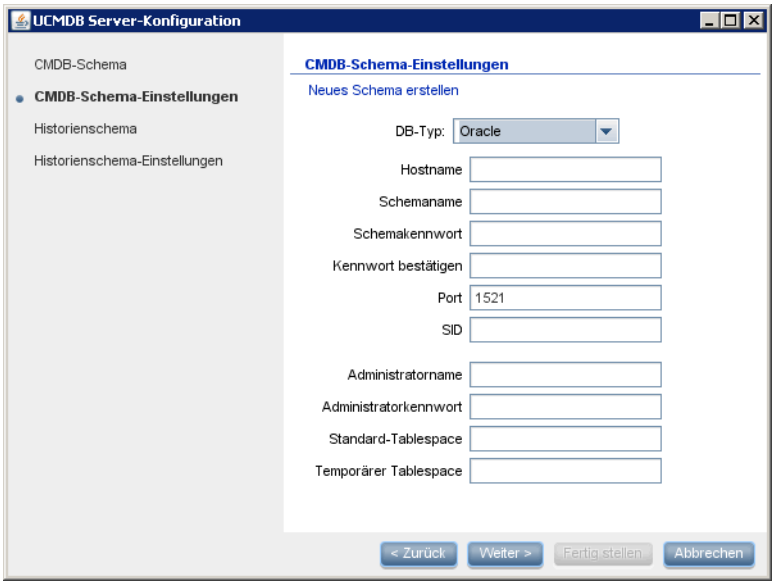
Wählen Sie **Neues Schema erstellen** aus.

2 Klicken Sie auf **Weiter**, um das Dialogfeld **CMDB-Schema-Einstellungen** zu öffnen.



Wählen Sie **Oracle** aus.

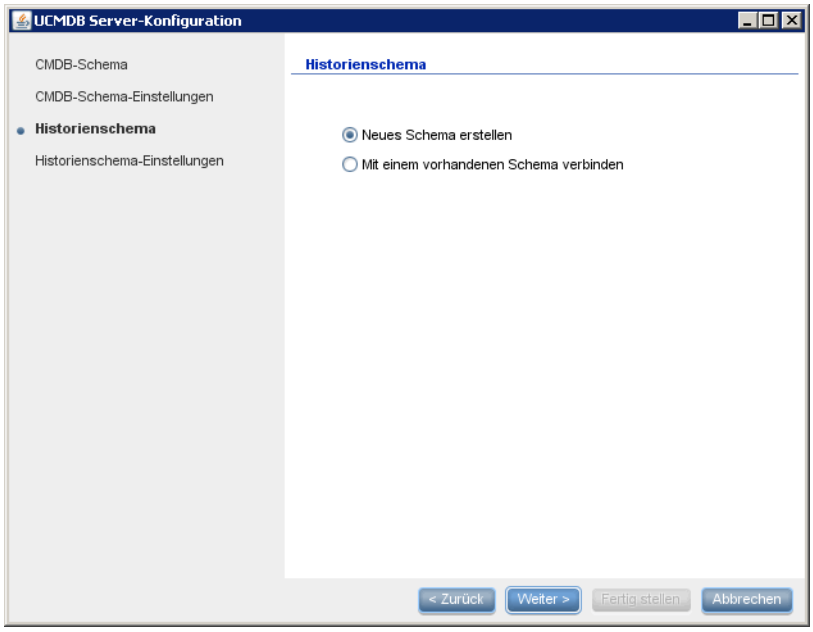
3 Im Dialogfeld werden zusätzliche Felder angezeigt.



Geben Sie die Details des Schemas ein.

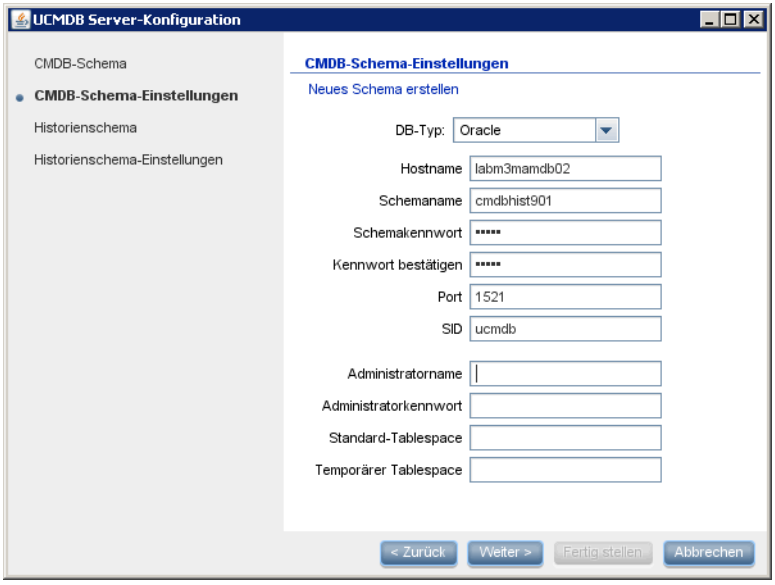
- **Schemaname.** Der Schemaname muss eindeutig sein.
- **Standard-Tablespace.** Aktualisieren Sie dieses Feld.
- **Temporärer Tablespace.** Falls Ihr Datenbankadministrator einen temporären Nicht-Standard-Tablespace erstellt hat, geben Sie diesen Namen ein. Andernfalls geben Sie **temp** ein.

4 Klicken Sie auf **Weiter**, um das Dialogfeld **Historienschema** zu öffnen.



Wählen Sie **Neues Schema erstellen** aus.

5 Klicken Sie auf **Weiter**, um das Dialogfeld **Historienschema-Einstellungen** zu öffnen.



Wählen Sie **Oracle** aus. Die Werte, die Sie für die CMDB-Einstellungen eingegeben haben, werden im Dialogfeld angezeigt.

6 Klicken Sie auf **Fertig stellen**. Die CMDB History-Datenbank wird erstellt.

Verbinden mit einer vorhandenen Microsoft SQL Server-Datenbank

In diesem Abschnitt wird erklärt, wie Sie eine Verbindung zu einer vorhandenen Microsoft SQL Server-Datenbank herstellen. Diese Installationsphase besteht aus zwei Teilen, nämlich dem Verbinden mit der CMDB-Datenbank und der CMDB History-Datenbank.

Befolgen Sie die Anweisungen zum Erstellen einer Microsoft SQL Server-Datenbank, mit Ausnahme der folgenden Schritte:

- Wählen Sie in Schritt 1 auf Seite 111 die Option **Mit einem vorhandenen Schema verbinden** aus und klicken Sie auf **Weiter**.
- Wählen Sie in Schritt 5 auf Seite 114 die Option **Mit einem vorhandenen Schema verbinden** aus und klicken Sie auf **Weiter**.

Verbinden mit einem vorhandenen Oracle-Schema

In diesem Abschnitt wird erklärt, wie Sie eine Verbindung zu einem vorhandenen Oracle Server-Schema herstellen. Diese Installationsphase besteht aus zwei Teilen, nämlich dem Verbinden mit dem CMDB-Schema und dem CMDB History-Schema.

Befolgen Sie die Anweisungen zum Erstellen eines Oracle Server-Schemas, mit Ausnahme der folgenden Schritte:

- Wählen Sie in Schritt 1 auf Seite 116 die Option **Mit einem vorhandenen Schema verbinden** aus und klicken Sie auf **Weiter**.
- Wählen Sie in Schritt 4 auf Seite 119 die Option **Mit einem vorhandenen Schema verbinden** aus und klicken Sie auf **Weiter**.

Neustarten des Servers

Wenn Sie den UCMDB Server-Konfigurationsassistenten als Teil der HP Universal CMDB Server-Installation ausgeführt haben, dürfen Sie HP Universal CMDB auf dem Server erst starten, wenn Sie die Parameter für alle Datenbanken erfolgreich festgelegt haben.

Wenn Sie den UCMDB Server-Konfigurationsassistenten ausgeführt haben, um zuvor definierte Datenbanktypen oder Verbindungsparameter zu ändern, starten Sie den HP Universal CMDB Server und die Data Flow Probe neu, nachdem Sie die Parameter erfolgreich geändert haben.

9

HP Universal CMDB-Services

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Referenz

Aufgaben

Anzeigen des Status des HP Universal CMDB Server-Services

Wählen Sie **Start** > **Alle Programme** > **HP UCMDB** > **HP Universal CMDB Server-Status** aus. Der Status und der detaillierte Status aller Services werden angezeigt:

Status

Customer Name	Customer ID	Status
Default Client	1	Up
Test Customer	2	Up
Test 3nd customer	3	Up
New Customer - con	4	Up

Detailed Status

Component	Process	Customer 1	Customer 2	Customer 3	Customer 4
autodiscovery	master	Up	Up	Up	Up
classModel	master	Up	Up	Up	Up
cmdb_mod_not	master	Up	Up	Up	Up
cmdb_sys_tqls	master	Up	Up	Up	Up
cmdb_view	master	Up	Up	Up	Up
configuration	master	Up	Up	Up	Up
content-install	master	Up	Up	Up	Up
correlation	master	Up	Up	Up	Up
data-acquisition	master	Up	Up	Up	Up

In der Spalte **Customer** wird angezeigt, ob alle HP Universal CMDB-Services ausgeführt werden (**Up**) oder ob manche davon nicht ausgeführt werden ().

Hinweis: Werden manche Services nicht ausgeführt, wenden Sie sich an HP Software Support, um das Problem zu beheben.

Starten und Anhalten des HP Universal CMDB Server-Services

Rufen Sie das Windows-Dialogfeld **Dienste** auf und suchen Sie den Service **UCMDB_Server**. Öffnen Sie das Dialogfeld **Eigenschaften von UCMDB_Server (Lokaler Computer)** und starten Sie den Service. Ändern Sie den Starttyp bei Bedarf in **Automatisch**.

Weitere Informationen zum Starten und Anhalten von UCMDB Server finden Sie unter "Zugriffsbefehle auf der Windows-Plattform" auf Seite 132 oder "Zugriffsbefehle auf der Linux-Plattform" auf Seite 133.

Referenz

HP Universal CMDB-Services

Die HP Universal CMDB Server-Services sind in der folgenden Tabelle beschrieben:

Servicename	Servicebeschreibung
autodiscovery	Verantwortlich für Services, die sich auf die Data Flow Management beziehen.
classModel	Verantwortlich für die Verwaltung des Klassenmodells in der CMDB.
cmdb_mod_not	Verantwortlich für Benachrichtigungen über Änderungen in der CMDB.
cmdb_sys_tqls	Verantwortlich für die Bedingungen, die auf TQL-Knoten angewendet werden, und für die Bedingungsergebnisse, die in der System-TQL gespeichert werden.
cmdb_view	Verantwortlich für die Berechnung von Ansichtsdefinitionen über TQL-Ergebnisse (die Umwandlung von Diagrammen in Strukturen erfolgt mit der Ansichtsdefinition).
configuration	Verantwortlich für Baselines, CI-Änderungsabfragen und TQL-Abfragen bzw. Abfragen der Ansichtshistorie.
content-install	
data-acquisition	
enrichment	Verantwortlich für die Ausführung von Ad-hoc- und aktiven Enrichments.
fcmdb	Verantwortlich für die Steuerung der Adapter, der Auffüllung und Daten-Push-Flüsse, der Datenföderation und der Discovery von einem Modul der obersten Ebene aus.

Servicename	Servicebeschreibung
fcmdb-config	Ein Cache-Mechanismus für föderierte Daten, der grundlegende FCMDB-Services ermöglicht, bevor die FCMDB vollständig geladen ist.
fcmdb-management	Verantwortlich für die Verwaltung der Adapter, der Föderation und des Daten-Push-Flusses.
folders	Verantwortlich für die Verwaltung der Ordnerhierarchie für alle Ressourcentypen.
framework	
grouping	Verantwortlich für die Verwaltung der verschiedenen Bundles, die die Klassifizierung von Ressourcen ermöglichen.
historyDB	
impact	Verantwortlich für die HP Universal CMDB-Untersysteme für Auswirkung, Ursache und Korrelation.
mapping-engine	
model	Verantwortlich für die Zuordnung von CIs aus externen Datenquellen zu lokalen CMDB-CIs.
model_update	Verantwortlich für die Verwaltung von Aktualisierungen für das Klassenmodell in der CMDB.
packaging	Verantwortlich für Packages. Packages sind zip-Dateien mit Ressourcen, die in organisierten, vordefinierten Unterverzeichnissen strukturiert sind.
reconciliation	Der Abstimmungsservice für die CMDB-Datenauffüllung. Verantwortlich für die Abstimmungs-Engine von HP Universal CMDB.
report	Verantwortlich für HP Universal CMDB-Reportservices, darunter das Hinzufügen, Bearbeiten und Löschen von Systemreports, Assetberechnungs-Reports oder Knotenabhängigkeits-Reports.
scheduler	
security	

Servicename	Servicebeschreibung
state_management	
tql	Verantwortlich für TQL -Berechnungen.
tql_res_utils	Verantwortlich für die Verwaltung von TQL-Ergebnissen (aktiv) und das Abrufen von Layouts.
view	Verantwortlich für einen Teil der Geschäftslogik des Modeling Studio, einschließlich "watch".
world	Ein zentrales Repository für Konfigurationsdaten, die aus den unterschiedlichen Applikationen und Tools von HP Universal CMDB sowie von Drittanbietern erfasst wurden. Diese Daten werden zum Erstellen von HP Universal CMDB-Ansichten verwendet. **Hinweis**: Der CMDB-Service wird nicht notwendigerweise vom Prozess mercury_as ausgeführt.

Fehlerbehebung und Einschränkungen

Problem: UCMDB wird nach dem Neustart des Systems nicht automatisch gestartet.

Lösung:

1. Wählen Sie **Start** > **Alle Programme** > **HP UCMDB** > **HP Universal CMDB Server starten** aus.
2. Öffnen Sie das Windows-Dialogfeld **Dienste** und wählen Sie den Service **UCMDB_Server** aus.
3. Öffnen Sie das Dialogfeld **Eigenschaften von UCMDB_Server (Lokaler Computer)**.
4. Stellen Sie auf der Registerkarte **Allgemein** Folgendes sicher:
   - Im Feld **Pfad zur EXE-Datei** ist der richtige Speicherort angegeben.
   - Der Service ist für automatisches Starten konfiguriert (die Option für **Starttyp** lautet **Automatisch**).

5 Stellen Sie auf der Registerkarte **Anmeldung** Folgendes sicher:

➤ Der Service verwendet für die Anmeldung den richtigen Benutzer. Weitere Informationen zum Ändern des Servicebenutzers finden Sie unter "Ändern des HP Universal CMDB Server-Servicebenutzers" auf Seite 301.

6 Stellen Sie auf der Registerkarte **Abhängigkeiten** Folgendes sicher:

➤ Der Service ist ohne Abhängigkeiten konfiguriert (<**Keine Abhängigkeiten**>).

10

Zugriffsbefehle für den UCMDB-Server

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Aufgaben

Zugriffsbefehle auf der Windows-Plattform

Während der Installation von HP Universal CMDB wird ein Startmenü zu den Einstellungen des Computers hinzugefügt, auf dem Sie UCMDB installieren. Sie können den UCMDB Server starten und anhalten, den Datenbankkonfigurations-Assistenten aufrufen, den Servicestatus des Servers anzeigen and den Server deinstallieren.

Hinweis: Weitere Informationen zum Starten und Anhalten von UCMDB Server als Service finden Sie unter "Starten und Anhalten des HP Universal CMDB Server-Services" auf Seite 125.

Zum Aufrufen des HP Universal CMDB-Startmenüs wählen Sie **Start** > **Programme** > **HP UCMDB** aus. Das Menü enthält die folgenden Optionen:

- **Konfigurationsassistenten für HP Universal CMDB Server starten.** Mit dieser Option können Sie den Assistenten ausführen, um eine Verbindung zu einer vorhandenen Datenbank bzw. zu einem vorhandenen Schema herzustellen oder um eine neue Datenbank oder ein neues Schema zu erstellen. Weitere Informationen finden Sie unter "Auswählen der Datenbank oder des Schemas" auf Seite 106.
- **HP Universal CMDB Server starten.** Mit dieser Option starten Sie den Serverservice.
- **HP Universal CMDB Server anhalten.** Mit dieser Option stoppen Sie den Serverservice.
- **HP Universal CMDB Server-Status.** Mit dieser Option öffnen Sie eine Webseite mit Informationen zum Server. Weitere Informationen finden Sie unter "HP Universal CMDB-Services" auf Seite 126.
- **HP Universal CMDB Server deinstallieren.** Mit dieser Option deinstallieren Sie den Server.

Zugriffsbefehle auf der Linux-Plattform

Führen Sie die folgenden Befehle aus, um den UCMDB Server zu starten und anzuhalten, den Datenbankkonfigurations-Assistenten aufzurufen, den Servicestatus des Servers anzuzeigen und den Server zu deinstallieren.

Hinweis:

- Weitere Informationen zum Starten und Anhalten von UCMDB Server als Service finden Sie unter "Starten und Anhalten des HP Universal CMDB Server-Services" auf Seite 125.
- Die folgenden Befehle setzen voraus, dass UCMDB im Standardpfad **/opt/hp** installiert wurde. Wenn der Server in einem anderen Verzeichnis installiert wurde, ersetzen Sie **/opt/hp** durch den betreffenden Pfad.

- So starten Sie den HP Universal CMDB Server:

```
/opt/hp/UCMDB/UCMDBServer/bin/server.sh start
```

- So halten Sie den HP Universal CMDB Server an:

```
/opt/hp/UCMDB/UCMDBServer/bin/server.sh stop
```

- So rufen Sie den HP Universal CMDB Server-Konfigurationsassistenten auf:

```
/opt/hp/UCMDB/UCMDBServer/bin/configure.sh
```

➤ Um die Webseite mit dem UCMDB Server-Status anzuzeigen, öffnen Sie einen Browser und geben den folgenden URL ein: **http://<UCMDB Server-Hostname oder -IP>:8080/status**.

Hinweis: Sie können die Statusseite auf jedem Computer aufrufen, d. h. nicht nur auf dem Linux-Computer, der den UCMDB Server hostet.

➤ So deinstallieren Sie den UCMDB Server:

```
/opt/hp/UCMDB/UCMDBServer/UninstallerData/Uninstall_UCMDBServer
```

Teil III

Installation von Data Flow Probe

11

Installieren der Data Flow Probe auf der Windows-Plattform

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Referenz

Aufgaben

Installieren der Data Flow Probe

Hinweis: Es wird dringend empfohlen, dass Sie gründlich das Kapitel "Einführung in HP Universal CMDB" auf Seite 25 lesen, bevor Sie mit der Installation beginnen. Weitere Informationen zu Data Flow Management finden Sie unter "Einführung in Data Flow Management" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

In der folgenden Prozedur wird beschrieben, wie Sie die Data Flow Probe auf einer Windows-Plattform installieren.

Die Probe kann vor oder nach der Installation von HP Universal CMDB Server installiert werden. Sie müssen jedoch während der Installation der Probe den Servernamen angeben, sodass es sich empfiehlt, den Server vor der Probe zu installieren.

Stellen Sie sicher, dass genug Festplattenplatz verfügbar ist, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter "Data Flow Probe – Installationsanforderungen" auf Seite 153.

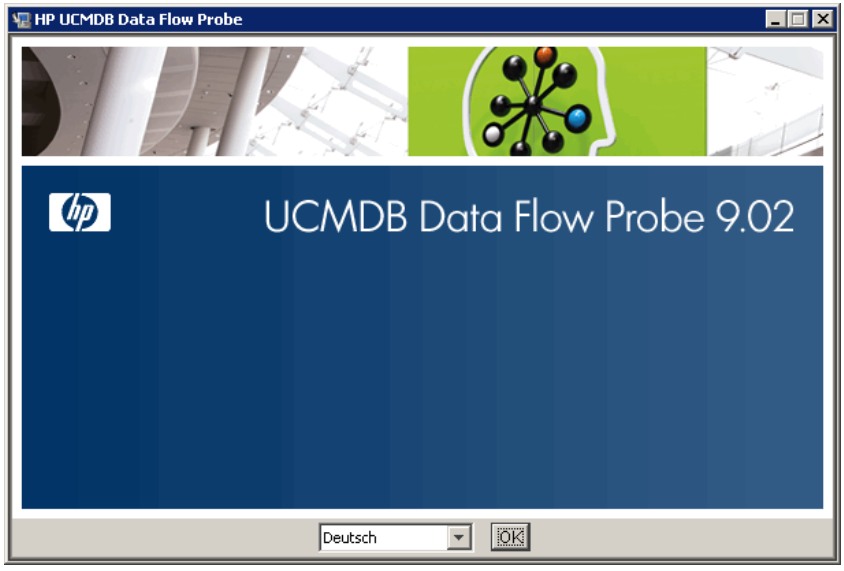
Hinweis: Weitere Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.

So installieren Sie die UCMDB Data Flow Probe:

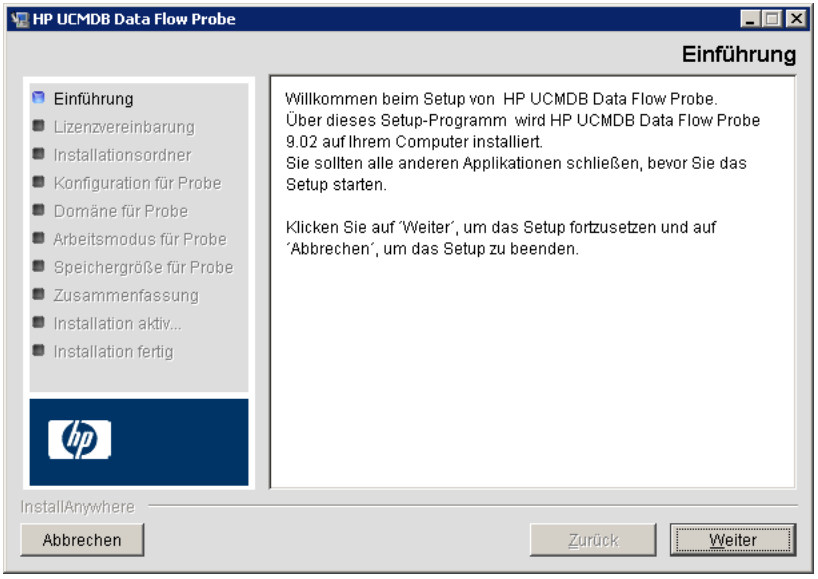
1 Legen Sie die DVD **HP Universal CMDB9.02 Setup Windows** in das Laufwerk ein, von dem aus Sie die Probe installieren. Wenn Sie von einem Netzwerklaufwerk aus installieren, stellen Sie eine Verbindung zu diesem Laufwerk her.

2 Doppelklicken Sie auf die Datei **<DVD-Stammverzeichnis>\UCMDB902\HPUCMDB_DataFlowProbe_902.exe**.

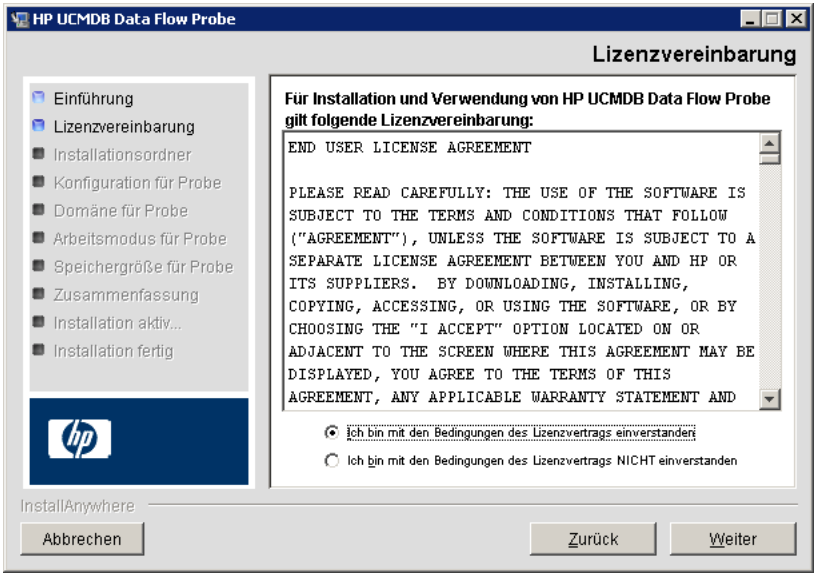
Eine Statusleiste wird angezeigt. Nachdem der Initialisierungsprozess abgeschlossen ist, wird der Startbildschirm angezeigt.



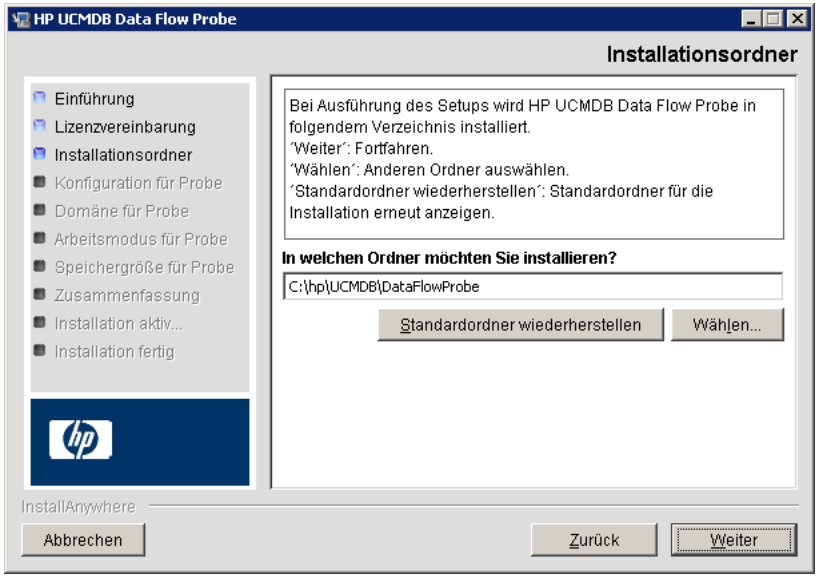
3 Wählen Sie die Gebietssprache aus und klicken Sie auf **OK**, um das Dialogfeld **Einführung** zu öffnen.



4 Klicken Sie auf **Weiter**, um mit der Lizenzvereinbarung fortzufahren.



5 Akzeptieren Sie die Bedingungen der Vereinbarung und klicken Sie auf **Weiter**, um das Dialogfeld **Installationsordner** zu öffnen.

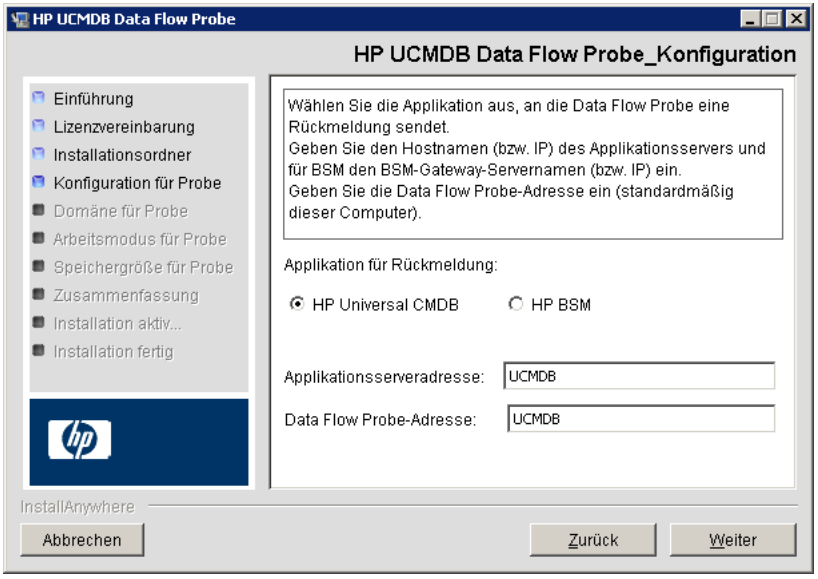


6 Übernehmen Sie die Standardeinstellung oder klicken Sie auf **Wählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Zum Installieren in einem anderen Verzeichnis suchen Sie den entsprechenden Installationsorder und wählen ihn aus.

Hinweis: Zum Wiederherstellen des Standardinstallationsverzeichnisses, nachdem Sie im Dialogfeld **Durchsuchen** ein Verzeichnis ausgewählt haben, klicken Sie auf **Standardordner wiederherstellen**.

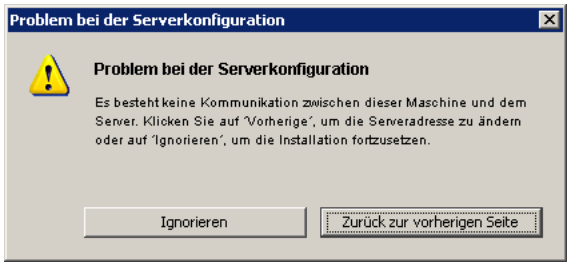
---

7 Klicken Sie auf **Weiter**, um das Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe zu öffnen.

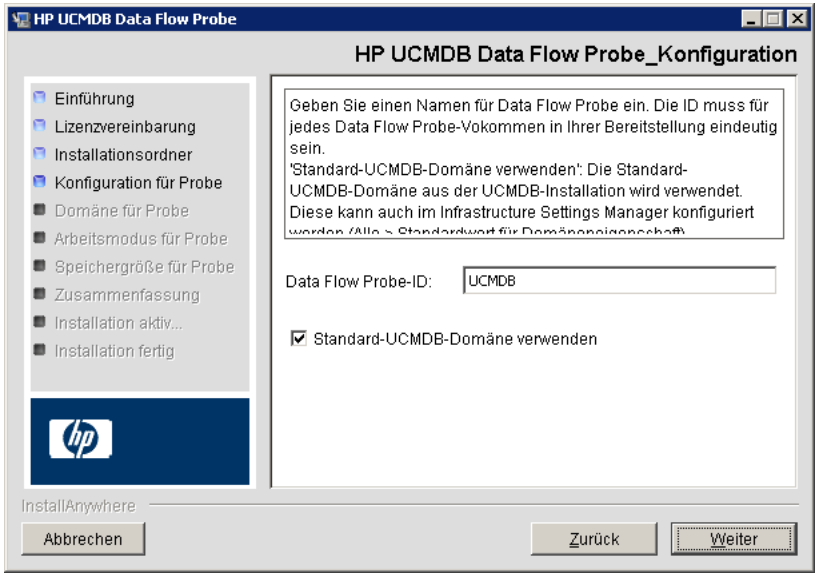


- **Applikation für Rückmeldung.** Wählen Sie den Applikationsserver aus, mit dem Sie arbeiten. Sie können die Probe entweder mit HP Universal CMDB oder mit Business Service Management verwenden.
  - Wenn Sie **HP Universal CMDB** auswählen, geben Sie im Feld **Applikationsserveradresse** den Namen oder die IP-Adresse des HP Universal CMDB-Servers ein, mit dem die Probe verbunden werden soll.
  - Wenn Sie **HP BSM** auswählen, geben Sie im Feld **Applikationsserveradresse** die IP oder den DNS-Namen des Gateway-Servers ein.
- Geben Sie im Feld **Data Flow Probe-Adresse** die IP-Adresse oder den DNS-Namen des Computers ein, auf dem Sie gerade die Probe installieren, oder übernehmen Sie die Standardeinstellung.

8 Wenn Sie die Adresse des Applikationsservers nicht eingeben, wird eine Meldung angezeigt. Sie können auswählen, ob Sie die Installation der Probe ohne Adresseingabe fortsetzen möchten oder ob Sie zur vorherigen Seite zurückkehren und die Adresse hinzufügen möchten.



9 Klicken Sie auf **Weiter**, um das Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe zu öffnen.



➤ Geben Sie im Feld **Data Flow Probe-ID** einen Namen ein, mit dem die Probe in Ihrer Umgebung erkannt wird.

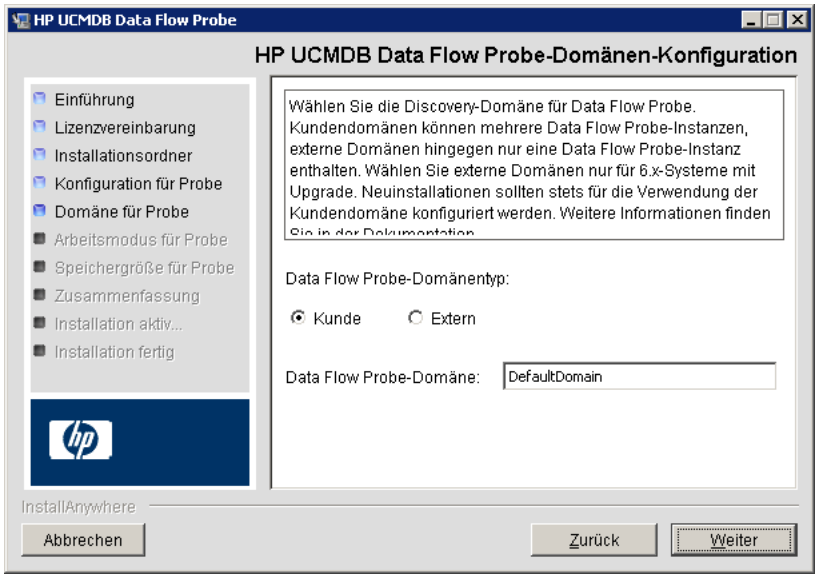
Wichtig:

- Jede UCMDB-Probe in Ihrer Bereitstellung muss eine eindeutige ID erhalten.
- Wenn Sie die Probe im separaten Modus installieren, d. h., wenn Probe Gateway und Probe Manager auf verschiedenen Computern installiert werden, müssen das Probe Gateway and alle Manager denselben Namen erhalten. Dieser Name wird in UCMDB als ein einziger Probenknoten angezeigt. Wenn der Name nicht übereinstimmt, werden manche Jobs möglicherweise nicht ausgeführt.

- Wählen Sie **Standard-UCMDB-Domäne verwenden** aus, um die Standard-UCMDB-IP-Adresse oder den Standard-UCMDB-Computernamen zu verwenden, wie in der UCMDB Server-Installation definiert.

  Die Standard-UCMDB-Domäne kann auch über die Infrastruktureinstellungen konfiguriert werden, die nach der HP Universal CMDB-Installation verfügbar sind (**Verwaltung** > **Infrastructure Settings Manager** > **Klassenmodell-Einstellungen** > **Standardwert für Domäneneigenschaft**).

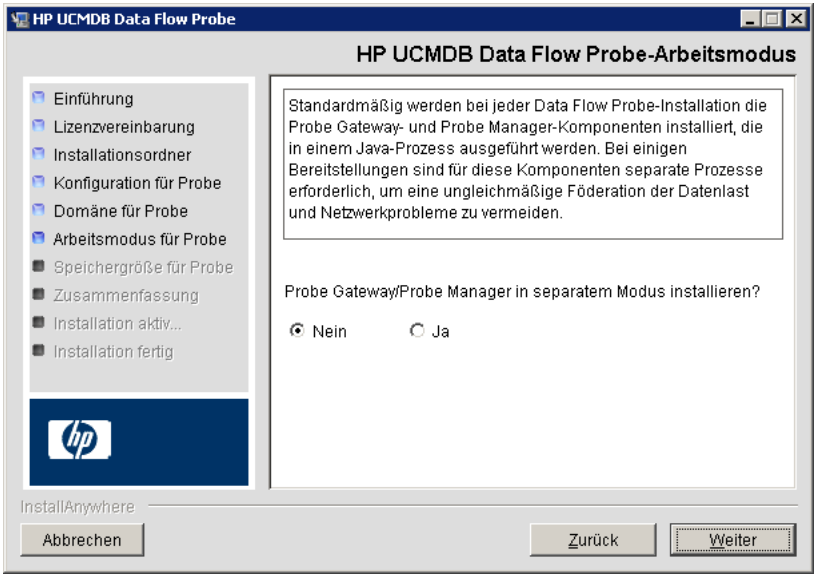
10 Klicken Sie auf **Weiter**. Wenn Sie das Kontrollkästchen **Standard-UCMDB-Domäne verwenden** im Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe deaktiviert haben, wird das Dialogfeld für die Domänenkonfiguration der HP UCMDB Data Flow Probe angezeigt.



- **Data Flow Probe-Domänentyp**. Wählen Sie **Kunde** oder **Extern** aus, abhängig vom Typ der Domäne, unter der die Probe ausgeführt werden soll:
  - **Kunde.** Wählen Sie diese Option aus, wenn Sie eine oder mehrere Proben in Ihrer Bereitstellung installieren.
  - **Extern.** Wählen Sie diese Option aus, wenn Sie ein Upgrade von Systemen mit Version 6.x durchführen.

  Wichtig: Wählen Sie bei neuen Installationen immer **Kunde** aus.
- **Data Flow Probe-Domäne**. Wenn Sie nicht die in UCMDB definierte Standarddomäne verwenden, geben Sie hier den Domänennamen ein.

11 Klicken Sie auf **Weiter**, um das Dialogfeld für den Arbeitsmodus der HP UCMDB Data Flow Probe zu öffnen.

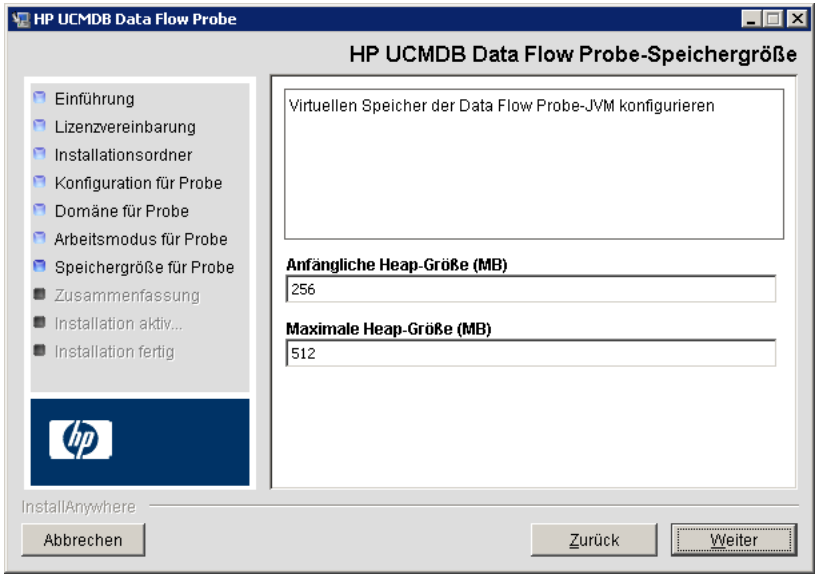


Sie können Probe Gateway und Probe Manager als einen einzigen Java-Prozess oder als separate Prozesse ausführen. Die Ausführung als separate Prozesse empfiehlt sich für Bereitstellungen, die ein besseres Load Balancing erfordern oder bei denen Netzwerkprobleme entstehen können.

Klicken Sie auf **Nein**, um Probe Gateway und Probe Manager als einen einzigen Prozess auszuführen.

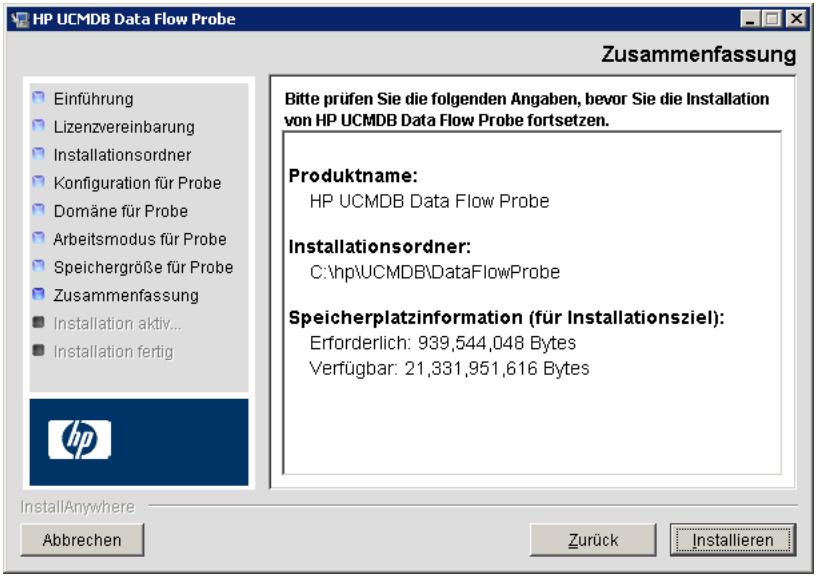
Klicken Sie auf **Ja**, um Probe Gateway und Probe Manager als zwei Prozesse auszuführen. Weitere Informationen zu dieser Prozedur finden Sie unter "Ausführen von Probe Manager und Probe Gateway auf separaten Computern" auf Seite 149.

12 Klicken Sie auf **Weiter**, um das Dialogfeld für die Speichergröße der HP UCMDB Data Flow Probe zu öffnen.



Definieren Sie den minimalen und maximalen Speicherplatz, der der Probe zugewiesen wird. Die Werte werden in Megabyte angegeben.

13 Klicken Sie auf **Weiter**, um das Dialogfeld **Zusammenfassung** zu öffnen und die ausgewählten Optionen zu überprüfen.



14 Klicken Sie auf **Installieren**, um die Installation der Probe abzuschließen. Nach beendeter Installation wird die Seite **Installation abgeschlossen** angezeigt.

Alle Fehler, die möglicherweise während der Installation auftreten, werden in der folgenden Datei erfasst: **C:\hp\UCMDB\DataFlowProbe\HP_UCMDB_Data_Flow_Probe_Install Log.log**.

15 Klicken Sie auf **Fertig**. Im Windows-Menü **Start** wird folgende Verknüpfung hinzugefügt:

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

16 Aktivieren Sie die Probe, indem Sie die Verknüpfung auswählen.

Sie können die Probe in einer Konsole ausführen. Weitere Informationen finden Sie unter "Starten der Probe in einer Konsole" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

Die Probe wird in HP Universal CMDB angezeigt: Rufen Sie **Data Flow Management** > **Data Flow Probe einrichten** auf. Weitere Informationen finden Sie unter "Data Flow Probe – Installationsanforderungen" auf Seite 153.

Upgrade der Probe

In dieser Aufgabe wird beschrieben, wie Sie ein Upgrade der Data Flow Probe durchführen.

1 Deinstallieren der alten Probe

Deinstallieren Sie alle vorhandenen Proben. Wenn eine Probe gerade ausgeführt wird, halten Sie sie vor dem Deinstallieren an:

Start > **Alle Programme** > **HP UCMDB** > **Data Flow Probe deinstallieren**.

2 Installieren der neuen Probe

Sie sollten die neue Probe mit derselben Konfiguration installieren, d. h., verwenden Sie dieselbe Proben-ID, denselben Domänennamen und denselben Servernamen wie für die vorherige Probeninstallation.

Ausführen von Probe Manager und Probe Gateway auf separaten Computern

Während der Installation können Sie festlegen, die Prozesse für Probe Manager und Probe Gateway zu trennen, damit sie auf verschiedenen Computern ausgeführt werden. Dazu müssen Sie:

17 Die Probe mit der unter "Installieren der Data Flow Probe" auf Seite 138 beschriebenen Prozedur auf beiden Computern installieren.

18 In Schritt 11 auf Seite 146 die Option **Ja** auswählen.

19 Die unter "Konfigurieren der Probe Manager- und Probe Gateway-Komponenten" auf Seite 150 beschriebene Konfiguration durchführen.

Hinweis:

- Sie müssen mindestens eine Probe Gateway-Komponente installieren. Gateway ist mit UCMDB Server verbunden, erhält Aufgaben vom Server und kommuniziert mit den Collectors (Probe Manager).
- Sie können mehrere Probe Manager installieren. Manager führen Jobs aus und erfassen Informationen aus Netzwerken.
- Das Probe Gateway muss eine Liste der verbundenen Manager enthalten.
- Die Probe Manager müssen wissen, mit welchem Gateway sie verbunden sind.

Konfigurieren der Probe Manager- und Probe Gateway-Komponenten

In diesem Abschnitt wird beschrieben, wie Sie die Data Flow Probe einrichten, wenn Probe Manager und Probe Gateway als separate Prozesse auf zwei Computern ausgeführt werden.

Dieser Abschnitt umfasst die folgenden Themen:

1 Einrichten des Probe Gateway-Computers

a Öffnen Sie folgende Datei:

C:\hp\UCMDB\DataFlowProbe\conf\probeMgrList.xml.

b Suchen Sie die Zeile, die mit **<probeMgr ip=** beginnt, und fügen Sie den Namen oder die IP-Adresse des Manager-Computers hinzu. Beispiel:

```
<probeMgr ip="OLYMPICS08">
```

c Öffnen Sie folgende Datei:

C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties

d Suchen Sie die Zeilen, die mit **appilog.collectors.local.ip =** und **appilog.collectors.probe.ip =** beginnen, und geben Sie den Namen oder die IP-Adresse des Gateway-Computers ein. Beispiel:

```
appilog.collectors.local.ip = STARS01
appilog.collectors.probe.ip = STARS01
```

2 Einrichten des Probe Manager-Computers

a Suchen Sie in der Datei **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties** die Zeile, die mit **appilog.collectors.local.ip =** beginnt, und geben Sie den Namen oder die IP-Adresse des Manager-Computers ein. Beispiel:

```
appilog.collectors.local.ip = OLYMPICS08
```

b Suchen Sie die Zeile, die mit **appilog.collectors.probe.ip =** beginnt, und geben Sie den Namen des Gateway-Computers in Großbuchstaben ein. Beispiel:

```
appilog.collectors.probe.ip = STARS01
```

3 Starten der Services

a Starten Sie auf dem Probe Manager-Computer den Manager-Service: **Start** > **Alle Programme** > **UCMDB** > **Data Flow Probe starten**.

b Starten Sie auf dem Probe Gateway-Computer den Gateway-Service: **Start** > **Alle Programme** > **HP UCMDB** > **Data Flow Probe starten (console)**.

Verbinden einer Data Flow Probe mit einem Nicht-Standardkunden

Sie können eine Data Flow Probe mit einem anderen Kunden als dem Standardkunden verbinden. Die Standardkunden-ID lautet **1**.

1. Öffnen Sie die folgende Datei in einem Texteditor:

   C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties.

2. Suchen Sie den Eintrag **Kunden-ID**.
3. Ändern Sie den Wert der Kunden-ID, z. B. in **Kunden-ID = 2**.
4. Starten Sie die Probe erneut, damit die Änderungen angewendet werden.

Referenz

Data Flow Probe – Installationsanforderungen

Dieser Abschnitt umfasst die folgenden Themen:

Hardwareanforderungen

Computer/Prozessor	**Windows:** Mindestens Pentium IV-Prozessor mit 2,4 GHz
Speicher	**Windows:** Mindestens 1 GB RAM (Empfohlen: 2 GB RAM)
Virtueller Speicher (für Windows-Bereitstellung)	Mindestens 2 GB **Hinweis:** Der virtuelle Speicher sollte immer mindestens doppelt so groß wie der physische Speicher sein.
Freier Festplattenplatz	**Windows:** Mindestens 4 GB (mindestens 4 GB für Datenbanksoftware und Datendateien) (Empfohlen: Festplatte mit 20 GB)
Anzeige	**Windows:** Farbpalette mit mindestens 256 Farben (32.000 Farben empfohlen)

Softwareanforderungen

Hardware-plattform	Betriebs-systemtyp	Betriebssystemversion und -edition	Unterstützt	Empfohlen
x86	Windows 2008	SP2, Standard/Enterprise Edition, 32-Bit	Ja	
x86-64	Windows 2008	SP2, Standard/Enterprise Edition, 64-Bit	Ja	Ja
x86-64	Windows 2008	R2, Standard/Enterprise Edition, 64-Bit	Ja	

Hardware-plattform	Betriebs-systemtyp	Betriebssystemversion und -edition	Unterstützt	Empfohlen
x86	Windows 2003	SP2 und R2 SP2, Standard/Enterprise Edition, 32-Bit	Ja	
x86-64	Windows 2003	SP2 und R2 SP2, Standard/Enterprise Edition, 64-Bit	Ja	
	Windows 7	Professional/Enterprise	Nein	
	Windows 2000		Nein	

Anforderungen an die virtuelle Umgebung

Plattform	Betriebssystemversion und -edition	Unterstützt	Empfohlen
VMware ESX 3.x	➤ Windows 2003 Standard/Enterprise Edition SP2 und R2 SP2, 32-/64-Bit ➤ Windows 2008 Standard/ Enterprise SP2, 32-/64-Bit und R2, 64-Bit	Ja	
VMware ESX 4.0	➤ Windows 2003 Standard/Enterprise Edition SP2 und R2 SP2, 32-/64-Bit ➤ Windows 2008 Standard/ Enterprise SP2, 32-/64-Bit und R2, 64-Bit	Ja	Ja
Vor ESX 3.5 (z. B. 3.0.x-Versionen)	➤ Möglicherweise unzureichende Leistung ➤ Keine Unterstützung für Windows 2008 oder Windows 7	Nein	
ESXi VMware	Alle Plattformen	Nein	
MS Hyper-V	Server 2008 v1 und R2	Nein	
Xen Hypervisor 3.x	Alle Plattformen	Nein	

Fehlerbehebung und Einschränkungen

Die MySQL-Datenbank von Data Flow Probe wird möglicherweise so beschädigt, dass keine Wiederherstellung mehr möglich ist, z. B. weil der Computer ohne Beenden des MySQL-Services heruntergefahren wurde.

So beheben Sie die Beschädigung:

1. Halten Sie die Probe an.
2. Führen Sie das Tool **repair_mysql.bat** aus dem folgenden Ordner aus: **C:\hp\UCMDB\DataFlowProbe\tools**.
3. Starten Sie die Probe.

   Kann die Beschädigung durch diese Prozedur nicht behoben werden, wenden Sie sich an HP Software Support.

12

Installieren der Data Flow Probe auf der Linux-Plattform

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Referenz

Aufgaben

Installieren der Data Flow Probe

Wichtig:

- Diese Probe ist nur für Integrationszwecke bestimmt und kann nicht für Discovery verwendet werden. Daher wird diese Probe nicht im Fenster **Data Flow Probe einrichten** angezeigt.
- Auf dem Computer, auf dem Sie die Data Flow Probe installieren, darf keine Instanz einer Microsoft MySQL-Datenbank ausgeführt werden. Ist eine solche Instanz vorhanden, müssen Sie sie deaktivieren.
- Zum Installieren der Data Flow Probe benötigen Sie Root-Berechtigungen für den Linux-Computer.

In der folgenden Prozedur wird beschrieben, wie Sie die Data Flow Probe auf einer Linux-Plattform installieren.

Die Probe kann vor oder nach der Installation von HP Universal CMDB Server installiert werden. Sie müssen jedoch während der Installation der Probe den Servernamen angeben, sodass es sich empfiehlt, den Server vor der Probe zu installieren.

Stellen Sie sicher, dass genug Festplattenplatz verfügbar ist, bevor Sie mit der Installation beginnen. Weitere Informationen finden Sie unter "Data Flow Probe – Unterstützungsanforderungen" auf Seite 170.

Hinweis: Weitere Informationen zur Lizenzierung finden Sie unter "Lizenzierungsmodell für HP Universal CMDB" auf Seite 47.

So installieren Sie die UCMDB Data Flow Probe:

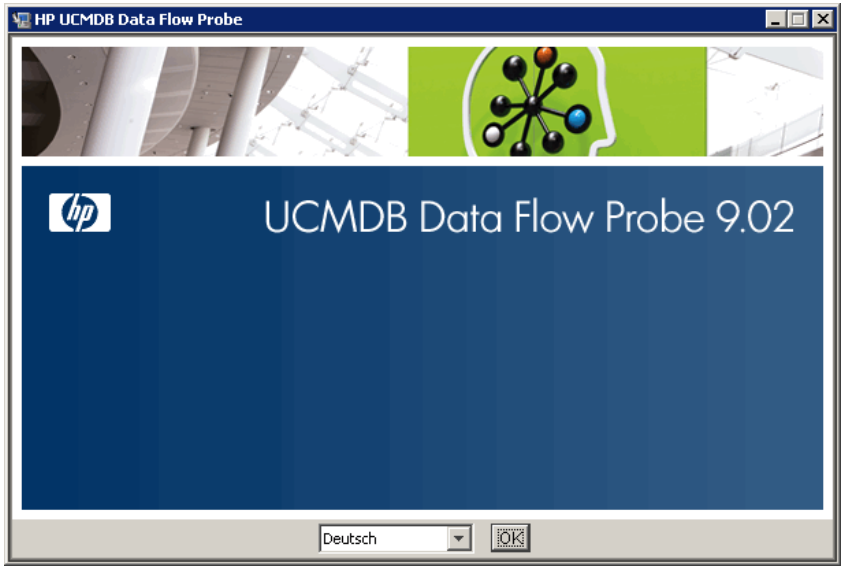
1 Führen Sie den folgenden Befehl aus, um den Installationsassistenten zu starten:

sh <Pfad zum Installationsprogramm>/HPUCMDB_DataFlowProbe_902Linux.bin

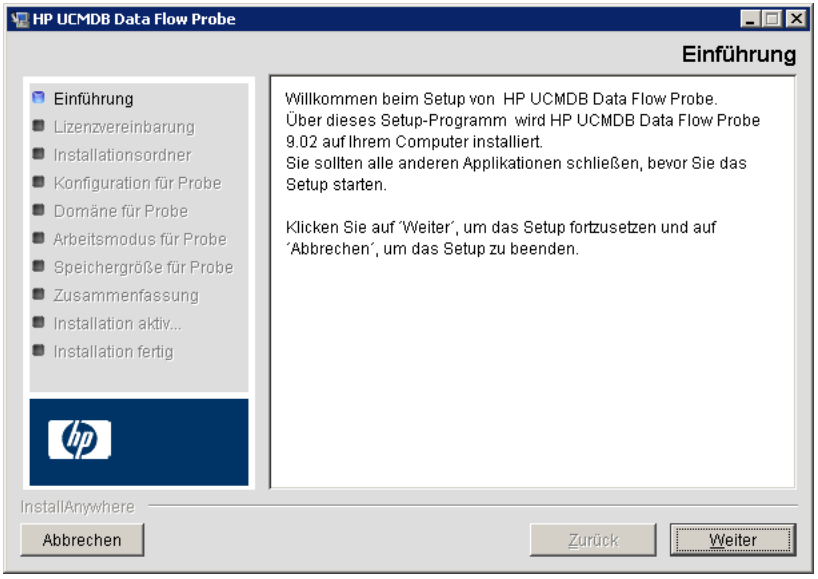
Die folgenden Befehle werden ausgeführt:

```
Vorbereiten der Installation
Extrahieren der JRE aus dem Archiv des Installationsprogramms
Entpacken der JRE
Extrahieren der Installationsressourcen aus dem Archiv des Installationsprogramms
Konfigurieren des Installationsprogramms für die Systemumgebung
Starten des Installationsprogramms
```

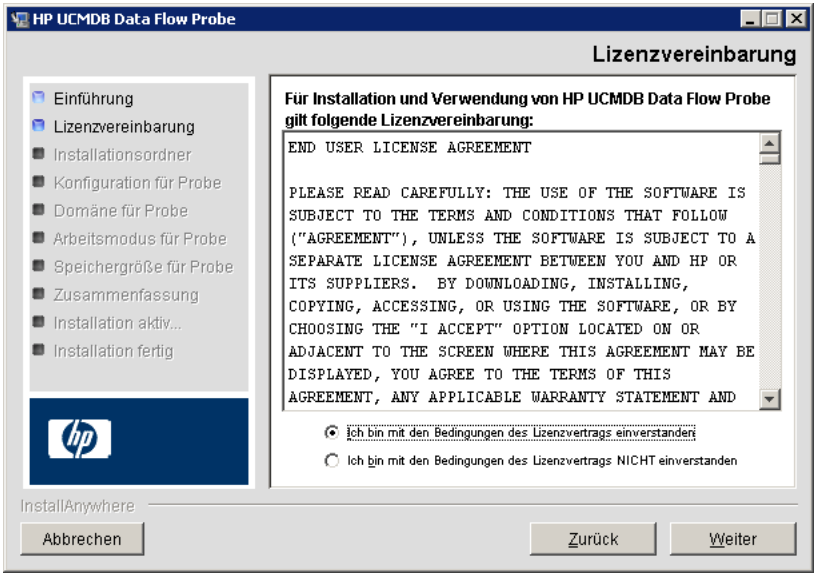
Nachdem der Initialisierungsprozess abgeschlossen ist, wird der Startbildschirm angezeigt.



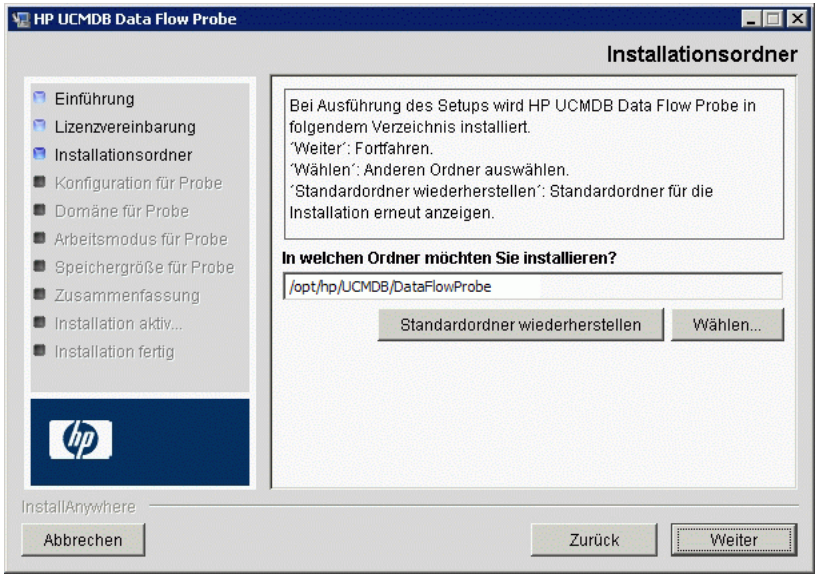
2 Wählen Sie die Gebietssprache aus und klicken Sie auf **OK**, um das Dialogfeld **Einführung** zu öffnen.



3 Klicken Sie auf **Weiter**, um mit der Lizenzvereinbarung fortzufahren.



4 Akzeptieren Sie die Bedingungen der Vereinbarung und klicken Sie auf **Weiter**, um das Dialogfeld **Installationsordner** zu öffnen.



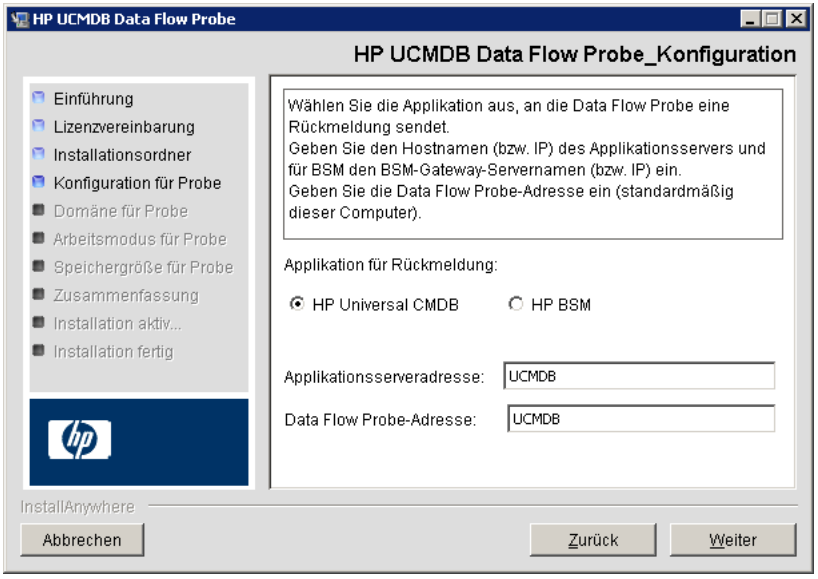
5 Übernehmen Sie die Standardeinstellung oder klicken Sie auf **Wählen**, um ein Standarddialogfeld zum Durchsuchen anzuzeigen. Zum Installieren in einem anderen Verzeichnis suchen Sie den entsprechenden Installationsorder und wählen ihn aus.

Hinweis:

- Sie können den Speicherort der Installation ändern, aber das Verzeichnis muss sich unter **/opt/** befinden.
- Zum Wiederherstellen des Standardinstallationsverzeichnisses, nachdem Sie im Dialogfeld **Durchsuchen** ein Verzeichnis ausgewählt haben, klicken Sie auf **Standardordner wiederherstellen**.

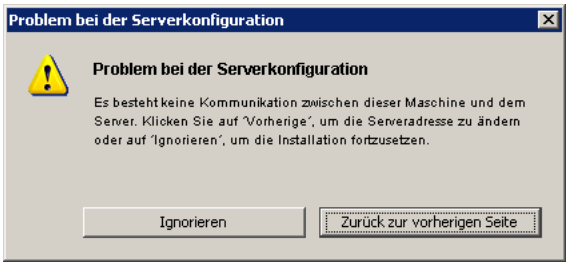
---

6 Klicken Sie auf **Weiter**, um das Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe zu öffnen.

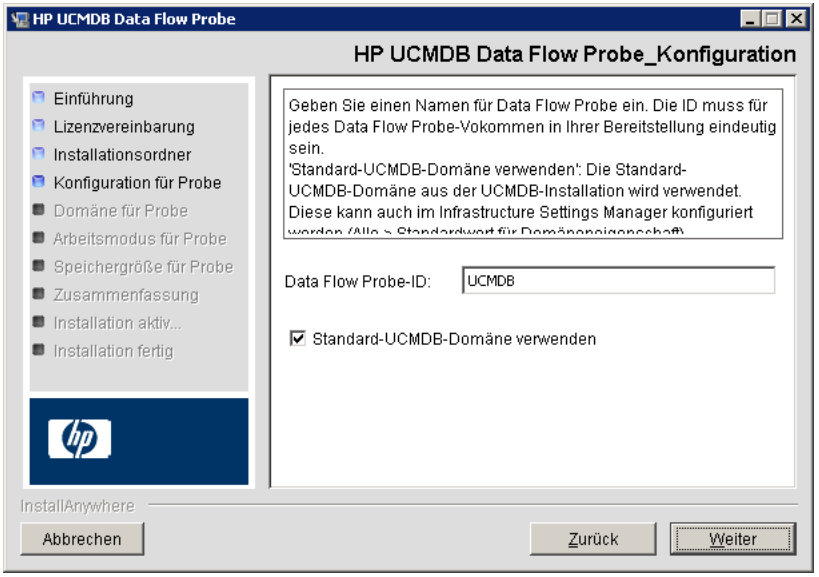


- **Applikation für Rückmeldung.** Wählen Sie den Applikationsserver aus, mit dem Sie arbeiten. Sie können die Probe entweder mit HP Universal CMDB oder mit Business Service Management verwenden.
  - Wenn Sie **HP Universal CMDB** auswählen, geben Sie im Feld **Applikationsserveradresse** den Namen oder die IP-Adresse des HP Universal CMDB-Servers ein, mit dem die Probe verbunden werden soll.
  - Wenn Sie **HP BSM** auswählen, geben Sie im Feld **Applikationsserveradresse** die IP oder den DNS-Namen des Gateway-Servers ein.
- Geben Sie im Feld **Data Flow Probe-Adresse** die IP-Adresse oder den DNS-Namen des Computers ein, auf dem Sie gerade die Probe installieren, oder übernehmen Sie die Standardeinstellung.

7 Wenn Sie die Adresse des Applikationsservers nicht eingeben, wird eine Meldung angezeigt. Sie können auswählen, ob Sie die Installation der Probe ohne Adresseingabe fortsetzen möchten oder ob Sie zur vorherigen Seite zurückkehren und die Adresse hinzufügen möchten.



8 Klicken Sie auf **Weiter**, um das Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe zu öffnen.



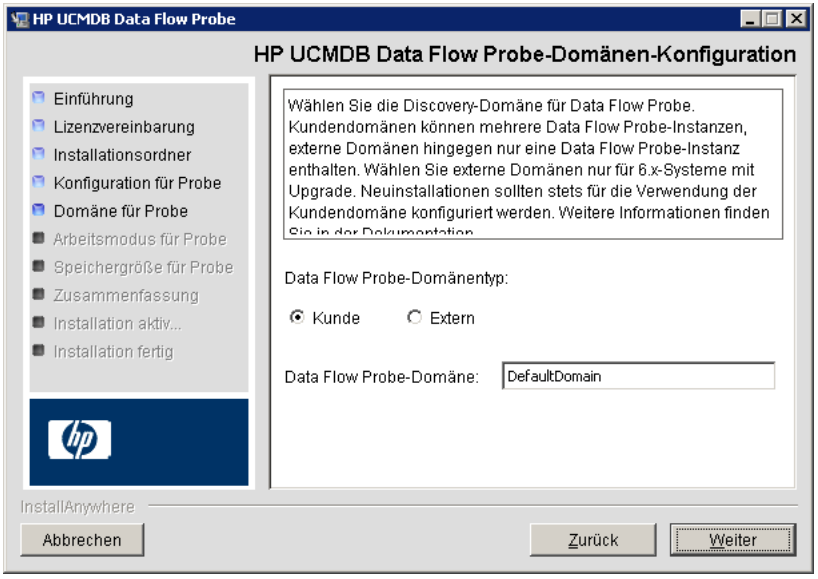
➤ Geben Sie im Feld **Data Flow Probe-ID** einen Namen ein, mit dem die Probe in Ihrer Umgebung erkannt wird. Dieser Name wird im Dialogfeld **Integrationspunkt** angezeigt. Weitere Informationen finden Sie im Abschnitt "Dialogfeld "Neuer Integrationspunkt"/"Integrationspunkt bearbeiten"" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

Wichtig: Jede UCMDB-Probe in Ihrer Bereitstellung muss eine eindeutige ID erhalten.

➤ Wählen Sie **Standard-UCMDB-Domäne verwenden** aus, um die Standard-UCMDB-IP-Adresse oder den Standard-UCMDB-Computernamen zu verwenden, wie in der UCMDB Server-Installation definiert.

Die Standard-UCMDB-Domäne kann auch über die Infrastruktureinstellungen konfiguriert werden, die nach der HP Universal CMDB-Installation verfügbar sind (**Verwaltung** > **Infrastructure Settings Manager** > **Klassenmodell-Einstellungen** > **Standardwert für Domäneneigenschaft**).

9 Klicken Sie auf **Weiter**. Wenn Sie das Kontrollkästchen **Standard-UCMDB-Domäne verwenden** im Dialogfeld für die Konfiguration der HP UCMDB Data Flow Probe deaktiviert haben, wird das Dialogfeld für die Domänenkonfiguration der HP UCMDB Data Flow Probe angezeigt.



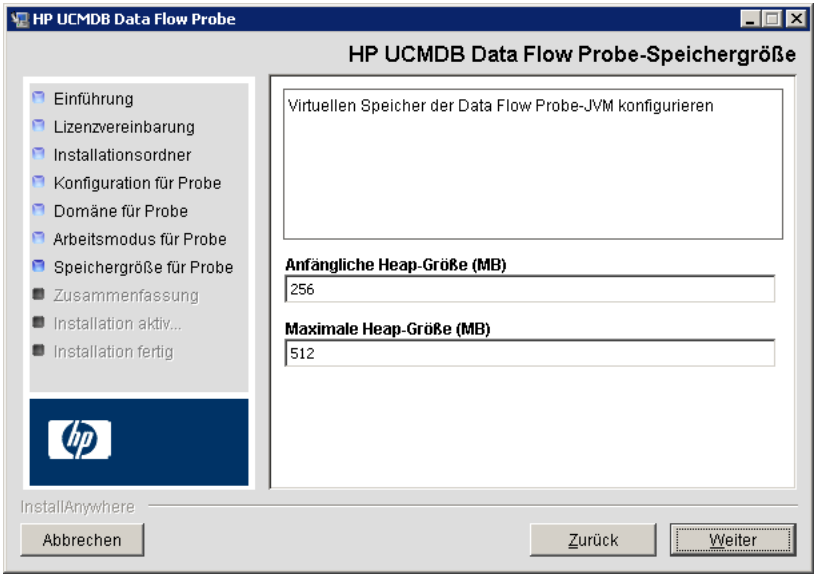
- **Data Flow Probe-Domänentyp**. Wählen Sie **Kunde** oder **Extern** aus, abhängig vom Typ der Domäne, unter der die Probe ausgeführt werden soll:
  - **Kunde.** Wählen Sie diese Option aus, wenn Sie eine oder mehrere Proben in Ihrer Bereitstellung installieren.
  - **Extern.** Wählen Sie diese Option aus, wenn Sie ein Upgrade von Systemen mit Version 6.x durchführen.

  Wichtig: Wählen Sie bei neuen Installationen immer **Kunde** aus.
- **Data Flow Probe-Domäne**. Wenn Sie nicht die in UCMDB definierte Standarddomäne verwenden, geben Sie hier den Domänennamen ein.

Hinweis: Das Dialogfeld für den Arbeitsmodus der HP UCMDB Data Flow Probe wird von der Installationsprozedur übersprungen. Dies liegt daran, dass Probe Gateway und Probe Manager als ein einziger Java-Prozess ausgeführt werden müssen.

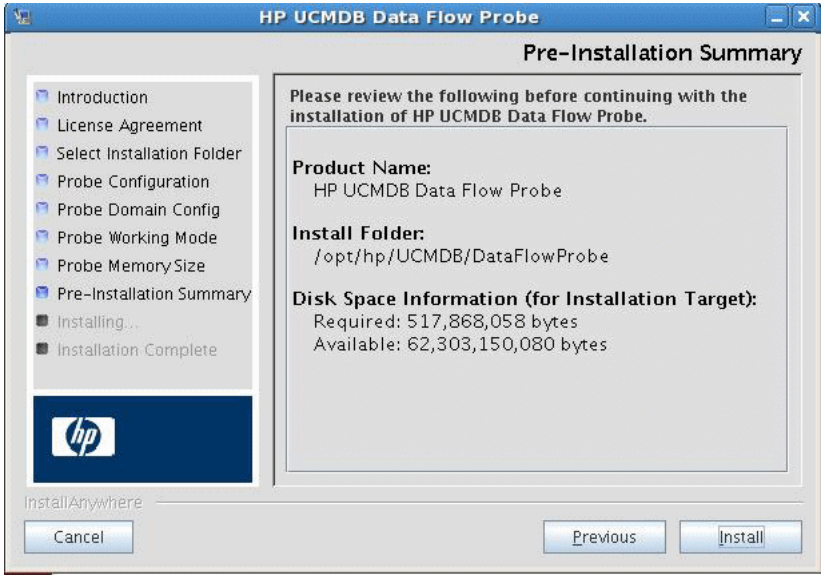
---

10 Klicken Sie auf **Weiter**, um das Dialogfeld für die Speichergröße der HP UCMDB Data Flow Probe zu öffnen.



Definieren Sie den minimalen und maximalen Speicherplatz, der der Probe zugewiesen wird. Die Werte werden in Megabyte angegeben.

11 Klicken Sie auf **Weiter**, um das Dialogfeld **Zusammenfassung** zu öffnen und die ausgewählten Optionen zu überprüfen.



12 Klicken Sie auf **Installieren**, um die Installation der Probe abzuschließen. Nach beendeter Installation wird die Seite **Installation abgeschlossen** angezeigt.

Alle Fehler, die möglicherweise während der Installation auftreten, werden in der folgenden Datei erfasst: **/opt/hp/UCMDB/DataFlowProbe/HP_UCMDB_Data_Flow_Probe_InstallLog.log**. Wenn Sie die Probe in einem anderen Verzeichnis unter **/opt/** installiert haben, befindet sich die Protokolldatei dort.

13 Klicken Sie auf **Fertig**.

14 Aktiveren Sie die Probe mit dem folgenden Befehl: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh start**

Zum Aktivieren der Probe in einer Konsole führen Sie den folgenden Befehl aus: **/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh console**

Die installierte Probe wird im Dialogfeld für neue Integrationspunkte in der Liste der Proben angezeigt. Weitere Informationen finden Sie im Abschnitt "Dialogfeld "Neuer Integrationspunkt"/"Integrationspunkt bearbeiten"" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

Hinweis: Der Benutzer, der den Probe-Service ausführt, muss zur Administratorgruppe gehören.

Anhalten des Probe-Servers

Führen Sie den folgenden Befehl aus, um den Probe-Server anzuhalten:

/opt/hp/UCMDB/DataFlowProbe/bin/ProbeGateway.sh stop

Upgrade der Data Flow Probe

In dieser Aufgabe wird beschrieben, wie Sie ein Upgrade der Data Flow Probe durchführen.

1 Deinstallieren der alten Probe

Deinstallieren Sie alle vorhandenen Proben. Wenn eine Probe gerade ausgeführt wird, halten Sie sie vor dem Deinstallieren an.

Erste Möglichkeit:

➤ Führen Sie in einer Shell-Eingabe Folgendes aus:

```
sh /opt/hp/UCMDB/DataFlowProbe/UninstallerData/Uninstall_Discovery_Probe
```

Zweite Möglichkeit:

➤ Doppelklicken Sie im Dateisystem auf die Datei Uninstall_Discovery_Probe.

2 Installieren der neuen Probe

Sie sollten die neue Probe mit derselben Konfiguration installieren, d. h., verwenden Sie dieselbe Proben-ID, denselben Domänennamen und denselben Servernamen wie für die vorherige Probeninstallation.

Verbinden einer Data Flow Probe mit einem Nicht-Standardkunden

Sie können eine Data Flow Probe mit einem anderen Kunden als dem Standardkunden verbinden. Die Standardkunden-ID lautet **1**.

1 Öffnen Sie die folgende Datei in einem Texteditor:

../DataFlowProbe/conf/DiscoveryProbe.properties.

2 Suchen Sie den Eintrag **customerID**.

3 Ändern Sie den Wert der Kunden-ID, z. B. in **customerId = 2**.

4 Starten Sie die Probe erneut, damit die Änderungen angewendet werden.

Referenz

Data Flow Probe – Unterstützungsanforderungen

Weitere Informationen zu den Mindestanforderungen finden Sie unter "HP Universal CMDB – Unterstützungsmatrix" auf Seite 35.

Fehlerbehebung und Einschränkungen

Die MySQL-Datenbank von Data Flow Probe wird möglicherweise so beschädigt, dass keine Wiederherstellung mehr möglich ist, z. B. weil der Computer ohne Beenden des MySQL-Services heruntergefahren wurde.

So beheben Sie die Beschädigung:

1. Halten Sie die Probe an.
2. Führen Sie das Tool **repair_mysql.sh** aus dem folgenden Ordner aus: **/opt/hp/UCMDB/DataFlowProbe/tools**.
3. Starten Sie die Probe.

   Kann die Beschädigung durch diese Prozedur nicht behoben werden, wenden Sie sich an HP Software Support.

Teil IV

Upgrade von HP Universal CMDB Version 8.0x auf Version 9.0x

13

Upgrade für HP Universal CMDB von Version 8.0x auf Version 9.0x

Wichtig:

- Wenn Sie eine Service-Pack-Version installieren (z. B. 9.02), finden Sie die aktuellen Anweisungen in den Versionshinweisen.
- Es wird dringend empfohlen, gründlich dieses Kapitel zu lesen, bevor Sie mit der Upgrade-Prozedur beginnen.

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

Upgrade – Übersicht

In diesem Kapitel wird erklärt, wie Sie ein Upgrade für HP Universal CMDB (UCMDB) von Version 8.0x auf Version 9.02 durchführen.

Der Upgrade-Prozess wird offline ausgeführt. Dabei werden alle Ressourcen und Daten vom 8.0x-Klassenmodell in das BDM (BTO Data Model) umgewandelt. Weitere Informationen zum Datenmodell finden Sie unter "Einführung in das UCMDB-Datenmodell" im *HP Universal CMDB – Modellierungshandbuch* (PDF).

Sie können das Upgrade nur für Ressourcen durchführen oder ein vollständiges Upgrade vornehmen:

- **Nur Ressourcen**. Einstellungen, Ressourcen und das Klassenmodell werden aktualisiert. Alle CIs werden gelöscht, ebenso die Historienereignisse, sodass die Daten neu erkannt werden müssen.
- **Vollständiges Upgrade**. Die Daten und die Historie sowie alle Ressourcen werden aktualisiert.

Aufgaben

Upgrade für HP Universal CMDB – Zusammenfassung

In diesem Abschnitt sind die erforderlichen Schritte für den Upgrade-Prozess aufgelistet.

Hinweis: Wenn Sie den UCMDB Server auf einer gehärteten Plattform (einschließlich Verwendung des HTTPS-Protokolls) ausführen möchten, lesen Sie die Härtungsprozeduren in Teil VI, "Härten von HP Universal CMDB".

Diese Aufgabe umfasst folgende Schritte:

- "Voraussetzungen" auf Seite 176
- "Überprüfen der Hardware- und Betriebssystemanforderungen" auf Seite 176
- "Vorbereiten der Datenbanken" auf Seite 176
- "Speichern geänderter Integrations- bzw. Föderationsadapter" auf Seite 177
- "Deinstallieren vorheriger UCMDB-Versionen" auf Seite 177
- "Deinstallieren vorheriger Proben" auf Seite 178
- "Installieren von UCMDB Version 9.02" auf Seite 178
- "Ausführen des Upgrade-Tools" auf Seite 179
- "Durchführen der Prozeduren nach dem Upgrade" auf Seite 179
- "Installieren der Data Flow Probe für Version 9.02" auf Seite 180

1 Voraussetzungen

- Wenn Sie eine frühere Version von HP Universal CMDB als 8.04 besitzen, führen Sie ein Upgrade auf Version 8.04 oder höher durch. HP Software empfiehlt ein Upgrade auf die neueste 8.0x-Version.
- Wenn Sie DDM-Content Pack 6.00 oder früher besitzen, müssen Sie DDM-Content Pack 7.00 installieren. Dieser Schritt muss nach dem Upgrade auf Version 8.04 oder höher durchgeführt werden.

2 Überprüfen der Hardware- und Betriebssystemanforderungen

Weitere Informationen finden Sie unter "HP Universal CMDB – Unterstützungsmatrix" auf Seite 35.

3 Vorbereiten der Datenbanken

- Das Upgrade erfordert ungefähr 250 % des Speicherplatzes, der normalerweise für das CMDB-Schema benötigt wird. Stellen Sie sicher, dass dieser Platz bereitgestellt ist.
- Sichern Sie die CMDB-, History- und Foundations-Datenbanken der Version 8.0x. In UCMDB 9.02 sind die Foundations- und CMDB-Schemas kombiniert. Sichern Sie alle drei Schemas einzeln, um die ordnungsgemäße Bindung während des Upgrades auf Version 9.02 zu gewährleisten.

  Wichtig: Führen Sie als zusätzliche Vorsichtsmaßnahme Ihre aktuelle UCMDB-Version mit den gesicherten Schemas aus, um zu überprüfen, dass die Sicherungen nicht beschädigt sind.

- Führen Sie das Datenbankkonsistenz-Tool in der Version 8.0x-Installation aus, um die folgenden beschädigten Daten aus dem CMDB-Schema zu löschen:
  - Links, bei denen die Endobjekte fehlen
  - CIs, bei denen Informationen in einigen Tabellen der Datenmodellhierarchie fehlen

Weitere Informationen zum Arbeiten mit der CMDB finden Sie im *HP Universal CMDB – Datenbankhandbuch* (PDF).

4 Speichern geänderter Integrations- bzw. Föderationsadapter

Für alle Standardadapter: Wenn Sie eine Adapterkonfiguration in Version 8.0x geändert haben, wird dringend empfohlen, dass Sie alle Adapterdateien aus dieser Version speichern und dieselben Änderungen für die Adapterdateien von Version 9.02 vornehmen.

Für alle Nicht-Standardadapter: Sie müssen die Adapter in Version 9.02 erneut bereitstellen. Weitere Informationen finden Sie unter "Package Manager" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Wichtig: Alle Adapter müssen mit dem neuen BDM-Modell kompatibel sein. Wenn Sie Änderungen an vorhandenen Standardadaptern vorgenommen haben, müssen Sie dieselben Änderungen für die Adapterdateien in der Version 9.00 durchführen. Kopieren Sie nicht die Dateien aus Version 8.0x, um die Dateien in Version 9.00 zu überschreiben.

5 Deinstallieren vorheriger UCMDB-Versionen

Die folgende Prozedur gilt **nur, wenn Sie den UCMDB Server Version 9.02 auf demselben Computer installieren möchten, auf dem zuvor die Version 8.0x ausgeführt wurde**. Wenn Sie zwei oder mehr Server verwenden, müssen Sie 8.0x vor dem Upgrade auf 9.02 nicht deinstallieren und können direkt mit dem nächsten Schritt fortfahren ("Deinstallieren vorheriger Proben" auf Seite 178). Allerdings müssen Sie die 8.0x-Instanz anhalten, bevor Sie Version 9.02 installieren.

Hinweis: Wenn Version 7.x installiert ist, führen Sie ein Upgrade von dieser Version auf die neueste 8.0x-Version durch und fahren Sie dann mit der Prozedur in diesem Kapitel fort. Weitere Informationen zum Upgrade auf 8.0x finden Sie in der Dokumentation zu Version 8.0x.

So entfernen Sie den UCMDB Server 8.0x:

a Halten Sie den UCMDB Server an: **Start** > **Alle Programme** > **HP UCMDB** > **HP Universal CMDB Server anhalten**.

b Deinstallieren Sie den Server: **Start** > **Alle Programme** > **HP UCMDB** > **HP Universal CMDB Server deinstallieren**. Weitere Informationen finden Sie unter "Deinstallieren von HP Universal CMDB" auf Seite 86.

c Entfernen Sie den gesamten Ordner **C:\hp\UCMDB** vom UCMDB Server-Computer.

d Starten Sie den UCMDB Server-Computer neu.

6 Deinstallieren vorheriger Proben

Die Mindestanforderung für das Upgrade auf UCMDB 9.02 ist UCMDB Version 8.04 oder höher mit installiertem DDM-Content Pack 7.00.

Halten Sie die DDM-Proben (oder Data Flow Probes) an und deinstallieren Sie sie. Weitere Informationen finden Sie unter "Upgrade der Probe" auf Seite 149 (Windows) oder "Upgrade der Data Flow Probe" auf Seite 169 (Linux).

7 Installieren von UCMDB Version 9.02

Weitere Informationen finden Sie unter "Installieren von HP Universal CMDB auf einer Windows-Plattform" auf Seite 73 oder "Installieren von HP Universal CMDB auf einer Linux-Plattform" auf Seite 89 im *HP Universal CMDB – Bereitstellungshandbuch* (PDF) für Version 9.02.

Wichtig: Richten Sie **nicht** die Datenbank oder das Schema ein. Fahren Sie nach Abschluss der Installation nicht mit dem UCMDB Server-Konfigurationsassistenten fort (um die Datenbank oder das Schema einzurichten). Klicken Sie in Schritt 12 auf Seite 85 auf **Nein**. Fahren Sie stattdessen mit dem nächsten Schritt dieser Prozedur fort.

8 Ausführen des Upgrade-Tools

Sie können ein vollständiges Upgrade vornehmen oder das Upgrade nur für Ressourcen durchführen: Weitere Informationen finden Sie unter "Upgrade – Übersicht" auf Seite 174.

Weitere Informationen zum Ausführen des Upgrades finden Sie unter "Upgrade auf UCMDB 9.02" auf Seite 181.

Informationen zu Fehlerauswirkungen und Protokollmeldungen finden Sie unter "Upgrade-Prozess: Technische Beschreibungen" auf Seite 191.

9 Durchführen der Prozeduren nach dem Upgrade

Nach dem Upgrade sind möglicherweise die folgenden Schritte erforderlich.

- **Reverse-Proxy**. Wenn das aktualisierte System nicht in derselben Umgebung wie das System der Version 8.0x ausgeführt wird, müssen Sie den Reverse-Proxy nach dem Upgrade neu konfigurieren. Weitere Informationen zum Konfigurieren finden Sie unter "Verwenden eines Reverse-Proxy" auf Seite 321.
- **SSL**. Richten Sie die SSL-Konfigurationen wieder ein. Weitere Informationen finden Sie unter "Aktivieren der SSL-Kommunikation" auf Seite 305.
- **LW-SSO**. Richten Sie LW-SSO wieder ein. Weitere Informationen finden Sie unter "Lightweight Single Sign-On-Authentifizierung (LW-SSO) – Allgemeine Referenz" auf Seite 385 und "Aktivieren der Anmeldung in HP Universal CMDB mit LW-SSO" auf Seite 404.
- **LDAP**. Richten Sie die LDAP-Konfiguration und -Zuordnung zwischen LDAP-Benutzern und -Gruppen wieder ein. Weiter Informationen finden Sie unter "Synchronisieren von HP Universal CMDB-Benutzerrollen mit LDAP-Gruppen" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).
- **JMX-Konsole**. Standardbenutzername und -kennwort des Administrators lauten **sysadmin**. Informationen zum Härten der JMX-Konsole finden Sie unter "Ändern des Systembenutzernamens oder Kennworts für die JMX-Konsole" auf Seite 300.

- **Foundations-Schema löschen**. Das Foundations-Schema wird nach dem Upgrade nicht mehr verwendet und kann gelöscht werden.
- **Änderungen für Integrations- bzw. Föderationsadapter erneut vornehmen**. Alle Adapter müssen mit dem neuen BDM-Modell kompatibel sein. Wenn Sie Änderungen an vorhandenen Standardadaptern vorgenommen haben, müssen Sie dieselben Änderungen für die Adapterdateien in der Version 9.02 durchführen. Kopieren Sie nicht die Dateien aus Version 8.0x, um die Dateien in Version 9.02 zu überschreiben. Alle Nicht-Standardadapter müssen neu bereitgestellt werden. Weiter Informationen finden Sie unter "Package Manager" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).
- **Alterung aktivieren**. Nach dem Upgrade ist die Alterung deaktiviert. Dies verhindert, dass CIs gelöscht werden aufgrund der Zeitspanne, in der die Probe keine Daten erfasst (vom Ausführen des Upgrade-Prozesses bis zur Meldung aller CIs durch Discovery).

  Daher wird empfohlen, dass Sie bis zur Stabilisierung des Systems warten, bevor Sie die Alterung wieder aktivieren. Um dies zu prüfen, führen Sie Discovery aus und überwachen Sie alle CIs, die zum Löschen markiert sind.

  Weitere Informationen zur Alterung finden Sie unter "CI-Lebenszyklus und der Alterungsmechanismus" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

  Weitere Informationen zum Ausführen von Discovery finden Sie unter "Discovery-Systemsteuerung – Workflow im erweiterten Modus" im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF).

10 Installieren der Data Flow Probe für Version 9.02

Installieren Sie die Data Flow Probe für Version 9.02. Informationen zum Speicherort der Datei **HPUCMDB_DataFlowProbe_902.exe** finden Sie unter "Installieren der Data Flow Probe auf der Windows-Plattform" auf Seite 137 oder "Installieren der Data Flow Probe auf der Linux-Plattform" auf Seite 157.

Upgrade auf UCMDB 9.02

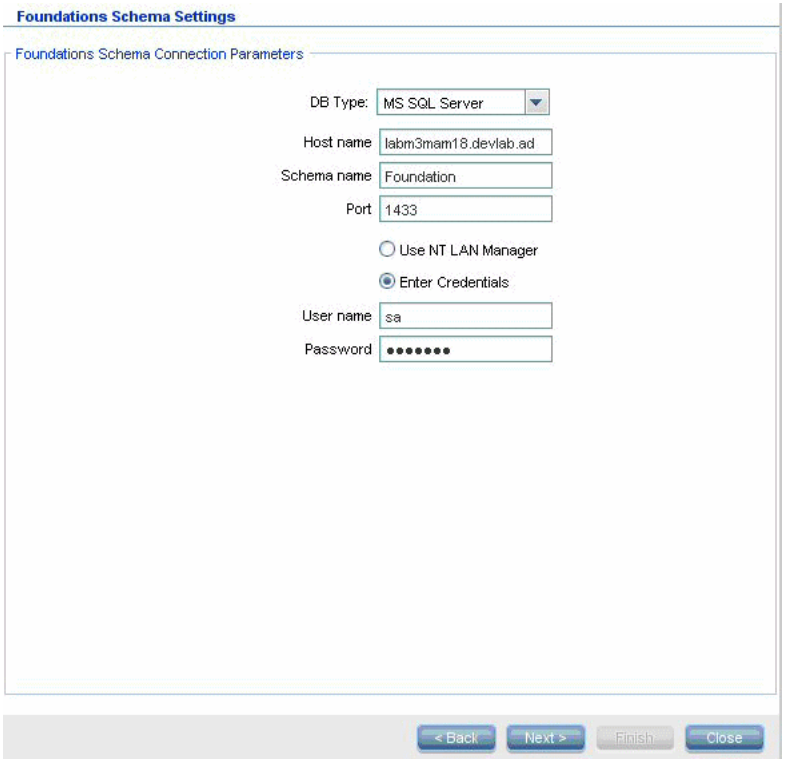
In diesem Abschnitt wird erklärt, wie Sie ein Upgrade für Daten von UCMDB Version 8.04 oder höher auf Version 9.02 vornehmen.

Wichtig: Sie dürfen diese Upgrade-Prozedur nur durchführen, wenn Sie UCMDB Version 8.04 oder höher mit DDM-Content Pack 7.00 installiert haben.

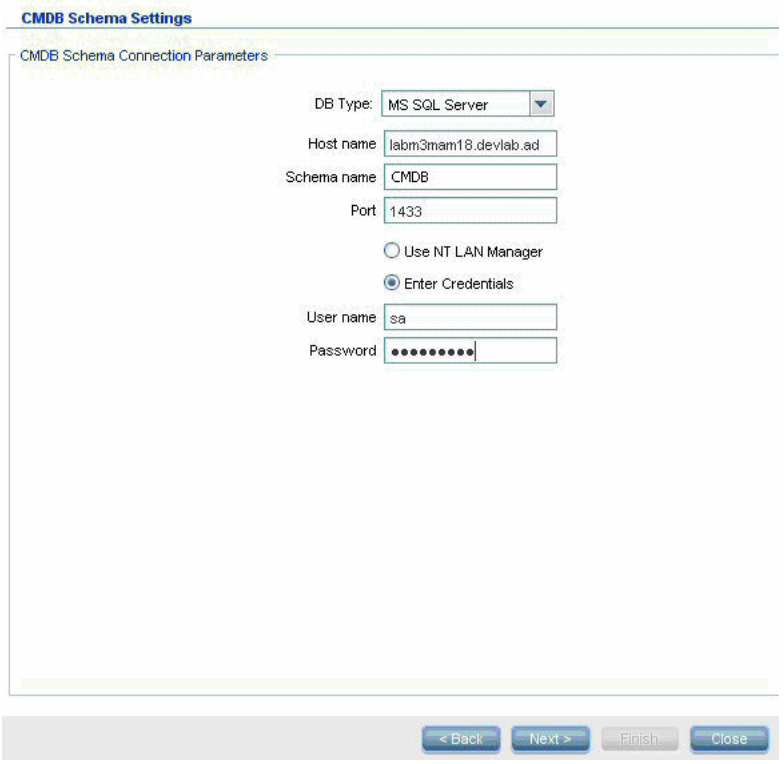
---

1. Suchen Sie die Upgrade-Datei und führen Sie sie aus: **C:\hp\UCMDB\UCMDBServer\tools\upgrade.bat** (Windows) oder **upgrade.sh** (Linux).
2. Der Assistent **Das Upgrade wird vorbereitet** wird geöffnet. Klicken Sie auf **Weiter**, um das Fenster für das UCMDB Server-Upgrade zu öffnen.
3. Wählen Sie eine Datenbank vom Typ **Oracle** oder **MS SQL Server** aus und richten Sie die Verbindungsparameter für das **Foundations-Schema** ein.

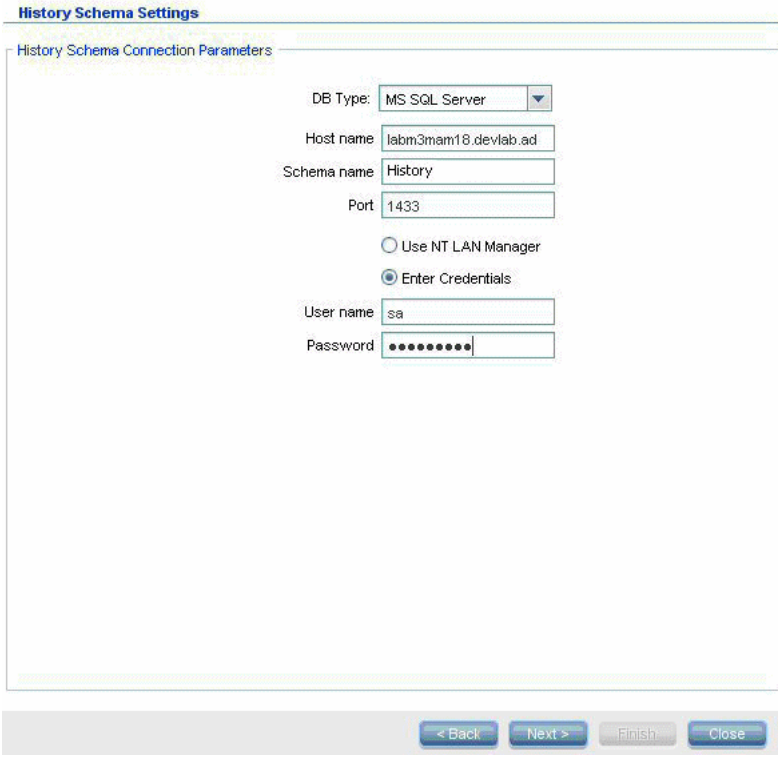
Der **Schemaname** sollte mit dem Namen des zuvor replizierten Foundations-Schemas aus UCMDB 8.0x übereinstimmen. Weitere Informationen zu den Verbindungsparametern finden Sie unter "Erforderliche Informationen zum Festlegen von Datenbankparametern" auf Seite 107.



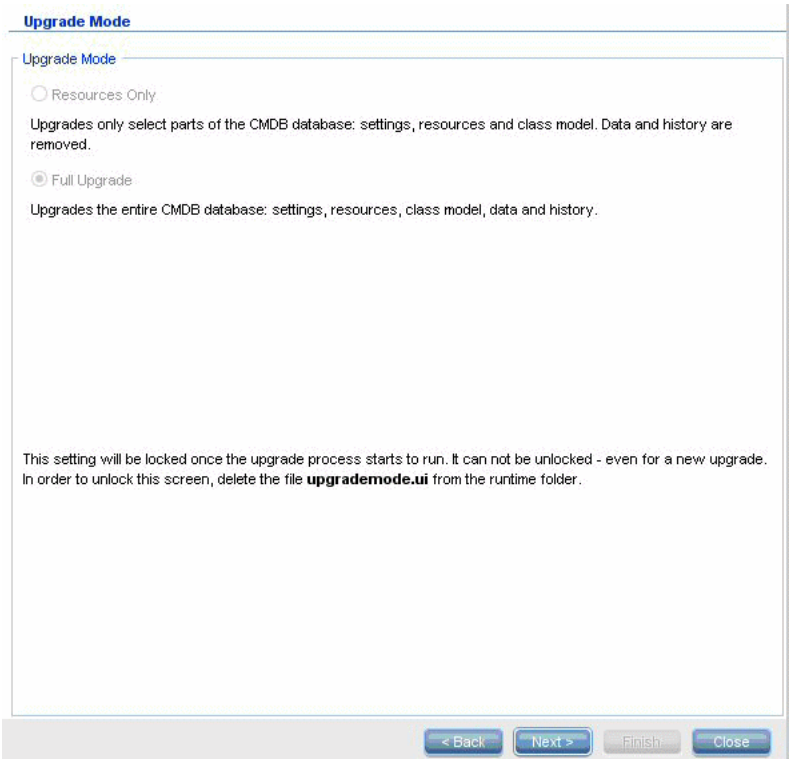
4 Klicken Sie auf **Weiter** und richten Sie die Verbindungsparameter für das **CMDB-Schema** ein. Der **Schemaname** sollte mit dem Namen des zuvor replizierten CMDB-Schemas aus UCMDB 8.0x übereinstimmen.



5 Klicken Sie auf **Weiter** und richten Sie die Verbindungsparameter für das **Historienschema** ein. Der **Schemaname** sollte mit dem Namen des zuvor replizierten Historienschemas aus UCMDB 8.0x übereinstimmen.

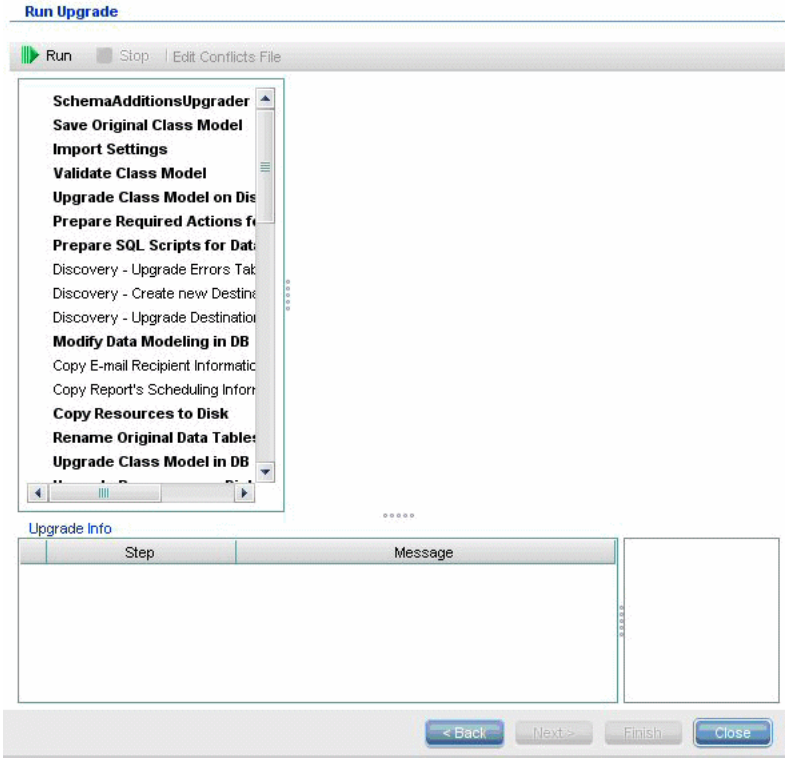


6 Klicken Sie auf **Weiter** und wählen Sie den Upgrade-Modus aus:

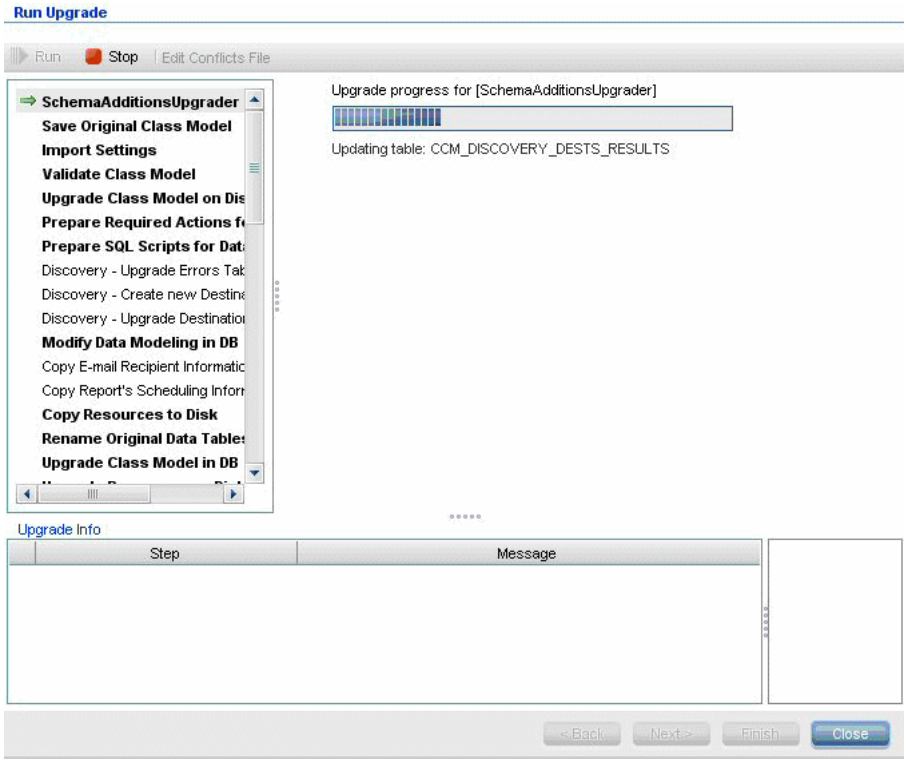


- **Nur Ressourcen.** Nur ausgewählte Bereiche der CMDB, die keine Daten oder Historie beinhalten, werden aktualisiert.
- **Vollständiges Upgrade.** Die gesamte CMDB wird aktualisiert, einschließlich Daten und Historie.

7 Klicken Sie auf **Weiter**. Im Fenster **Upgrade ausführen** werden die Upgrade-Schritte aufgeführt. Klicken Sie auf **Ausführen**, um das Upgrade zu starten.



8 Im Fenster **Upgrade ausführen** wird der Fortschritt jedes Schrittes angezeigt.



Informationen zu Fehlerauswirkungen und Protokollmeldungen in den einzelnen Schritten finden Sie unter "Upgrade-Schritte" auf Seite 194.

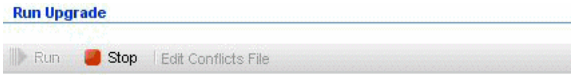
Informationen zum Prüfen von Datenmodellkonflikten finden Sie unter "Prüfen von Datenmodellkonflikten" auf Seite 189.

9 Um einen bestimmten Schritt erneut auszuführen, klicken Sie im Ausschnitt **Schritt** mit der rechten Maustaste auf den Schritt und wählen **Ausgewählte Elemente ausführen** aus.

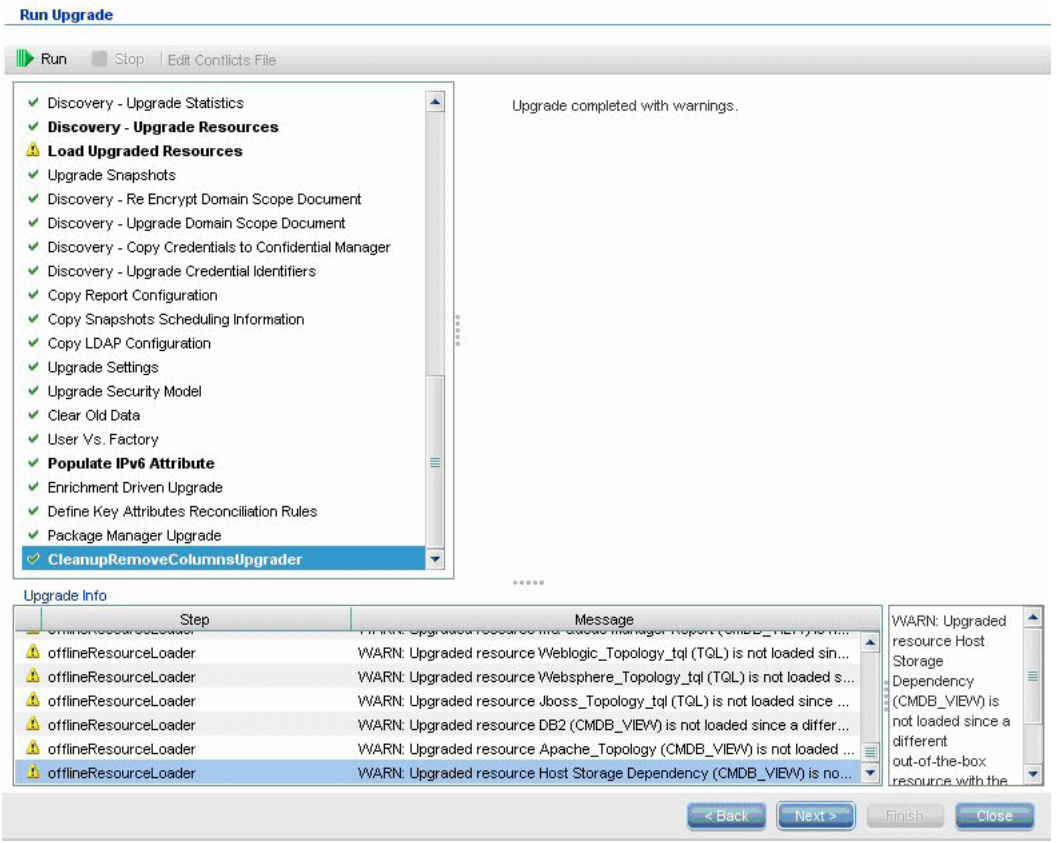
Wichtig: Erfolgreiche Upgrade-Schritte sollten nur zu Fehlerbehebungszwecken erneut ausgeführt werden.

Beenden der Upgrade-Prozedur

Das Upgrade ist möglicherweise erst nach längerer Zeit abgeschlossen. Um das Upgrade zu einem beliebigen Zeitpunkt zu beenden, klicken Sie auf die rote Schaltfläche **Stopp**:



Schritte, die mit einer Warnung abgeschlossen werden oder deren Ausführung fehlschlägt, werden im Ausschnitt **Upgrade-Info** protokolliert. Markieren Sie zum Anzeigen dieser Informationen die Zeile mit dem Upgrade-Schritt. Die relevanten Informationen werden rechts angezeigt.



Referenz

Fehlerbehebung und Einschränkungen

In diesem Abschnitt werden die Fehlerbehebung und Einschränkungen für das Upgrade von UCMDB 8.04 oder höher auf UCMDB 9.02 beschrieben.

Prüfen von Datenmodellkonflikten

Beim Upgrade-Schritt "Validate Data Model" werden das vorherige Klassenmodell, die vordefinierten Transformationen und das Standarddatenmodell als Eingabe verwendet, um ein geändertes Datenmodell zu erzeugen (nach dem Hinzufügen fehlender Datenmodellentitäten). Dieses befindet sich auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\old-class-model.xml**.

Wird ein Konflikt erkannt, z. B. weil ein Benutzer einer neuen Standardklasse bzw. einem neuen Standardattribut einen neuen Klassen- oder Attributnamen zuweist, wird eine neue zusätzliche Transformationsdatei auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\added-class-model-changes.xml** erzeugt und der Upgrade-Prozess schlägt fehl.

In der neuen Transformationsdatei wird eine zusätzliche Transformation definiert, um die Konflikte durch das Umbenennen von Klassen und Attributen zu lösen. Durch die erneute Ausführung des Upgrades werden diese neuen Transformationen einbezogen und das Upgrade kann fortgesetzt werden.

Wichtig: Wenn eine zusätzliche Transformationsdatei erzeugt wird, müssen Sie den Upgrade-Assistenten schließen und neu starten.

Ressourcen werden nicht in die aktualisierte UCMDB geladen

Ressourcen, die während des Upgrades entfernte Klassen verwenden, können nicht aktualisiert und in die aktualisierte UCMDB geladen werden. Ebenfalls entfernt werden Abfragen, die während des Upgrades entfernte Attribute als Eigenschaftsbedingung verwenden. Neben den Datenmodelltransformationen für diese Ressourcen werden die folgenden Änderungen vorgenommen:

- Ansichten werden neu definiert, um der neuen Ansichtsdefinition zu entsprechen.
- Topologie-Reports werden als Ansichten neu definiert. In UCMDB 9.02 werden Reports und Ansichten als verschiedene Visualisierungsformen derselben Daten betrachtet.
- Abfragen werden in einem benutzerfreundlichen XML-Format gespeichert.

14

Upgrade-Prozess: Technische Beschreibungen

Dieses Kapitel umfasst die folgenden Themen:

Referenz

Referenz

Eingabeparameter für den Upgrade-Prozess

Je nach ausgeführtem Upgrade-Typ (**Vollständig** oder **Nur Ressourcen**) werden im Upgrade-Prozess die folgenden Komponenten verwendet:

- Ihr Datenbankschema.
- Dateien mit Beschreibungen für die Klassenmodelltransformation während des Upgrades. Diese Dateien enden mit **_changes.xml** und befinden sich im Verzeichnis **C:\hp\UCMDB\UCMDBServer\conf\upgrade**.
- Das Standardklassenmodell von Version 8.04 und DDM-Content Pack 6.00. Diese Version ermöglicht, dass fehlende Klassenmodellentitäten im Upgrade-Prozess vor dem eigentlichen Upgrade hinzugefügt werden.
- Das Standarddatenmodell von Version 9.00 und DDM-Content Pack 6.00. Diese Version ermöglicht, dass fehlende Klassenmodellentitäten im Upgrade-Prozess nach dem eigentlichen Upgrade hinzugefügt werden und stellt sicher, dass das aktualisierte Klassenmodell mit HP Universal CMDB und Business Service Management kompatibel ist.

Protokolldateien für den Upgrade-Prozess

Während des Upgrades werden die folgenden Protokolldateien verwendet:

- **upgrade.detailed.log**. Dies ist die wichtigste Protokolldatei für die Upgrade-Prozedur. Alle Upgrade-Aktionen werden in diesem Protokoll erfasst (außer wenn für einen bestimmten Upgrade-Schritt etwas anderes angegeben wird). Diese Datei ist in der Regel zwischen 30 MB und 70 MB groß.
- **upgrade.short.log**. Eine Zusammenfassung des detaillierten Protokolls. Alle Zeilen dieser Datei sind auch in **upgrade.detailed.log** enthalten. Diese Datei sollte als Inhaltsverzeichnis für die detaillierte Datei oder als allgemeine Übersicht verwendet werden. Diese Datei ist in der Regel kleiner als 5 MB.
- **upgrade.detailed.attribute_cleanup.log**. Diese Protokolldatei zeigt den Fortschritt einer vollständigen Bereinigung des Datenmodells, damit Attribute nur ein Mal in einer Klassenhierarchie definiert sind. Für alle anderen Definitionen sollte **Attribut-Überschreibung** gelten und alle ungültigen Attribut-Überschreibungen werden entfernt. Dieser Prozess wird während des gesamten Upgrades mehrmals ausgeführt, nämlich bei der Bearbeitung des Klassenmodells (Prüfung anhand des vorherigen Klassenmodells, Upgrade des Klassenmodells und Prüfung anhand des Zielklassenmodells). Alle diese Protokolldateien zusammen (**.log**-Datei und alle Roll-over-Dateien) können mehrere hundert MB groß sein.
- **error.log**. Diese Datei, die sich nicht speziell auf das Upgrade bezieht, enthält alle von anderen Protokollen gesendeten Fehler und Warnungen (außer bei expliziter Sperrung). Sie kann zur Darstellung und als allgemeine Übersicht des Upgrade-Erfolgs verwendet werden.
- **mam.packaging.log**. Dieses Protokoll ist nur für den Schritt "Redeploy Basic Packages" relevant und enthält alle Informationen zu diesem Schritt. Weitere Informationen finden Sie unter "Redeploy Basic Packages" auf Seite 250.

Upgrade-Schritte

In diesem Abschnitt werden alle Schritte im gesamten Upgrade-Prozess beschrieben. Zu jedem Schritt der Upgrade-Prozedur finden Sie folgende Informationen:

- Eine Beschreibung des Schrittes.
- Ob der Schritt kritisch ist. Ein Schritt wird in den folgenden Fällen als kritisch erachtet:
  - Wird der Schritt ausgelassen, kann der UCMDB Server nach dem Upgrade nicht gestartet werden.
  - Wird der Schritt ausgelassen, gehen kritische Konfigurationen oder Daten verloren, die sich nach dem Upgrade nicht wiederherstellen lassen.
  - Wird der Schritt ausgelassen, funktioniert eine kritische Komponente nach dem Upgrade nicht ordnungsgemäß.
- Ob der Schritt erneut ausgeführt werden kann. Falls das Upgrade fehlschlägt, kann dieser Schritt für dieselben Schemas möglicherweise erneut ausgeführt werden.
- Fehlerauswirkungen. Wie wirkt sich das Fehlschlagen dieses Upgrade-Schrittes auf die UCMDB aus? Falls der Schritt erneut ausgeführt werden kann, wie lassen sich die Probleme beheben?
- Protokolldateien. Wichtige typische Meldungen aus der Protokolldatei für diesen Upgrade-Schritt und die Bedeutung jeder Meldung. Falls nicht anders angegeben, werden alle Meldungen in den folgenden Protokolldateien angezeigt:
  - **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.detailed.log**
  - **C:\hp\UCMDB\UCMDBServer\runtime\log\upgrade.short.log** (Protokollmeldungen in dieser Datei sind möglicherweise auch in der Datei **upgrade.detailed.log** vorhanden.)

    Weitere Informationen zu Protokollen finden Sie unter "Protokolldateien für den Upgrade-Prozess" auf Seite 193.

Wichtig: Schritte mit Bedeutung für den Upgrade-Typ **Nur Ressourcen** sind entsprechend gekennzeichnet.

Dieser Abschnitt umfasst folgende Schritte:

SchemaAdditionsUpgrader

Fügt die neuen erforderlichen Tabellen und Spalten zur CMDB hinzu.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

- Berechtigungsprobleme (keine ausreichenden Berechtigungen)
- Datenbankverbindungsprobleme (Datenbank kann nicht angebunden werden)
- Sperrung (Tabellen können nicht geändert werden)

Protokolldateien

- Updating table: … Aktualisieren einer bestimmten Tabelle in der Datenbank.
- Initializing default customer registration. Aktualisieren der allgemeinen Kundeninformationen.

Save Original Class Model

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Speichert das gesamte Klassenmodell vor dem Upgrade auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml**.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

- Das vorhandene Benutzerklassenmodell kann nicht aus der CMDB gelesen werden. Vermutliche Ursache: eine beschädigte Klassenmodelldefinition. Lösung: Bearbeiten Sie die Klassenmodelldefinition in der Datenbank manuell, bevor Sie versuchen, den Schritt erneut auszuführen.
- Die CMDB hat keine Schreibberechtigungen für den Ordner **C:\hp\UCMDB\UCMDBServer\runtime**. Ordnerberechtigungen zum **Lesen/Schreiben/Erstellen** werden für den gesamten Installationsordner benötigt (obwohl die meisten Schreibbefehle nur im Ordner **C:\hp\UCMDB\UCMDBServer \runtime** ausgeführt werden).

Protokolldateien

Fehler in den Dateien **cmdb.classmodel.log** oder **error.log** zeigen möglicherweise an, welche Entität im Klassenmodell nicht geladen werden konnte.

Import Settings

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die relevanten Einstellungen aus der Foundations-Datenbank in die Verwaltungstabelle der CMDB.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Einstellungen wurden nicht ordnungsgemäß migriert und stattdessen werden werkseitige CMDB-Standardwerte verwendet. Wenn der Alterungsmechanismus aktiviert ist, werden möglicherweise große Teile des CMDB-Datenmodells beim ersten Starten der CMDB entfernt.

Foundations-Datenbank falsch konfiguriert (oder nicht vorhanden).
Lösung: Konfigurieren Sie die Foundations-Datenbank mit dem Upgrade-Assistenten. Wenn die Datenbank beschädigt wurde oder eine neue Datenbank verwendet werden soll, erstellen Sie mit dem Datenbankassistenten von UCMDB 8.0x eine leere Foundations-Datenbank.

Protokolldateien

- Fetch old settings. Abrufen der Einstellungen aus der 8.0x-Foundations-Datenbank.
- Set new settings. Schreiben der Einstellungen in die neue Verwaltungsdatenbank.
- Aging mechanism has been disabled. Informationen zur Alterung finden Sie unter "CI-Lebenszyklus und der Alterungsmechanismus" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Validate Class Model

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Stellt sicher, dass Ihr altes Klassenmodell, das aus der Datei **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml** gelesen wird, mit dem erwarteten Standardklassenmodell abgestimmt ist. Dies ist erforderlich, damit bei den Klassenmodelltransformationen im Rahmen des Upgrade-Prozesses auf das alte Klassenmodell zugegriffen werden kann. In diesem Schritt werden das vorherige Klassenmodell, die vordefinierten Transformationen und die Standardklassenmodelle als Eingabe verwendet, um ein geändertes Klassenmodell zu erzeugen, nachdem die fehlenden Klassenmodellentitäten zur Datei **C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml** hinzugefügt wurden.

Wichtig:

Die Dateien für Klassenmodelländerungen dürfen nach Abschluss dieses Schrittes nicht mehr geändert werden. Dies gilt für die Standarddateien, die automatische Konfliktlösungsdatei und alle Dateien, die manuell unter **C:\hp\UCMDB\UCMDBServer\conf\upgrade** abgelegt werden.

Wenn die Dateien für Klassenmodelländerungen geändert werden, müssen der Upgrade-Assistent und die automatische Konfliktlösungsdatei vollständig geschlossen und neu geöffnet werden, damit die Änderungen korrekt angewendet werden.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Hinweis: Wenn die Datei **original-class-model.xml** zu Beginn dieses Schrittes noch nicht vorhanden ist, wird sie erneut aus der Datenbank gelesen.

Fehlerauswirkungen

Falls dieser Schritt fehlschlägt, prüfen Sie Folgendes:

- **Fehlende Attribut-Übereinstimmung**. Der **Attributtyp** unterscheidet sich von den Attributtypen des Standardklassenmodells. Die Typkonvertierung wird nicht unterstützt.
- **Klassen- oder Attributkonflikt**. Der neue Klassen- oder Attributname, den der Benutzer definiert hat, wird einer neuen Standardklasse bzw. einem neuen Standardattribut zugeordnet. In diesem Fall wird automatisch eine neue Transformationsdatei erzeugt und auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\added-class-model-changes.xml** gespeichert; der Upgrade-Prozess schlägt fehl. In der neuen

Transformationsdatei wird eine zusätzliche Transformation definiert, um die Konflikte durch das Umbenennen von Klassen und Attributen zu lösen. Führen Sie das Upgrade erneut aus, damit diese neuen Transformationen einbezogen werden und das Upgrade fortgesetzt wird. Vor der erneuten Ausführung des Upgrades können Sie diese Aktionen auch manuell ändern, z. B. indem Sie neue Namen auswählen.

Hinweis: Wenn eine Konfliktlösungsdatei erstellt wurde oder wenn Sie diese Datei über die Benutzeroberfläche ändern, müssen Sie den Upgrade-Assistenten vollständig schließen und neu öffnen, damit diese Änderungen korrekt geladen werden.

Protokolldateien

- Bei einer fehlenden Entität oder einer nicht unterstützten zusätzlichen Entität im Benutzerklassenmodell wird eine Warnung in die Protokolldatei geschrieben. Die Warnung enthält den Typ der Entität, ihren Namen, den Ort in der Klassenmodellhierarchie und die Aktion zum Verarbeiten der Entität (falls vorhanden).
  - Attribute type change is not allowed. Attribute <Name> in Class <Name> change type from <alter Typ> in <neuer Typ>. Bei Änderungen des Attributtyps enthält der Fehler den Namen des Attributs und seine Klasse.
  - Class hierarchy change may cause upgrade problems in Class <Name>. Der Ort des Klassennamens in der Klassenmodellhierarchie wurde geändert. Bestimmte Arten von Hierarchieänderungen können beim Upgrade verarbeitet werden, doch zu diesem Zeitpunkt des Upgrades liegen noch nicht genug Informationen vor, um über die Änderung zu entscheiden.
  - Class removal is not allowed in Class <Name>. Class was added. Eine Werk-Klasse fehlt im Benutzerklassenmodell, sodass die Klasse im Modell wieder erzwungen wird. Dies kann passieren, wenn ein Benutzer eine Klasse entfernt oder wenn bei der Bereitstellung von Content Pack 6.00 ein Fehler auftritt.

- Class Qualifier addition of type <Name> is not allowed. The qualifier was removed in Class <Name>. Bestimmte Typen von Klassenqualifizierern dürfen nicht vom Benutzer hinzugefügt werden. Wenn ein Benutzer einen dieser Qualifizierer hinzugefügt hat, wird diese Meldung angezeigt und der Klassenqualifizierer wird aus der Klasse entfernt.
- Class Qualifier removal of type <Name> is not allowed in Class <Name>. The qualifier was added. Wenn ein Qualifizierer in einer Werk-Klasse fehlt, wird er zur Klasse hinzugefügt.
- Attribute removal <Name> is not allowed. Attribute <Name> in Class <Name>. The Attribute was added. Ein Werk-Attribut fehlt im Benutzerklassenmodell in einer Werk-Klasse, sodass das Attribut zur Klasse hinzugefügt wird. Dies kann passieren, wenn ein Benutzer ein Attribut entfernt oder wenn bei der Bereitstellung von Content Pack 6.00 ein Fehler auftritt.
- Attribute Qualifier addition of type <Name> in new attribute <Name> is not allowed. The qualifier was removed in Class <Name>. Neue Attribute sind Attribute, die ein Benutzer zu einer Werk-Klasse hinzufügt. Bestimmte Typen von Attributqualifizierern dürfen jedoch nicht zu neuen Attributen hinzugefügt werden, sodass der Attributqualifizierer aus dem Attribut im Benutzerklassenmodell entfernt wird.
- Attribute Qualifier addition of type <Name> in existing attribute <Name> is not allowed. The qualifier was removed in Class <Name>. Bestimmte Typen von Attributqualifizierern dürfen Benutzer nicht zu Werk-Attributen hinzufügen. Daher wird der Attributqualifizierer aus dem Attribut im Benutzerklassenmodell entfernt.
- Attribute Qualifier addition of type <Name> in new attribute <Name> is not allowed. The qualifier was removed from the attribute override in Class <Name>. Neue Attribute sind Attribute, die ein Benutzer für eine Werk-Klasse erstellt. Außerdem hat der Benutzer eine Überschreibung für das neue Attribut in einer Unterklasse hinzugefügt. Bestimmte Typen von Attributqualifizierern dürfen jedoch nicht zu neuen Attributen oder deren Überschreibungen hinzugefügt werden. Daher wird der Attributqualifizierer aus der Attribut-Überschreibung im Benutzerklassenmodell entfernt.

- Attribute Qualifier addition of type <Name> in existing attribute <Name> is not allowed. The qualifier was removed from the attribute override in Class <Name>. Bestimmte Typen von Attributqualifizierern dürfen nicht zu Werk-Attributen oder deren Überschreibungen hinzugefügt werden. Daher wird der Attributqualifizierer aus der Attribut-Überschreibung im Benutzerklassenmodell entfernt.
- Attribute Qualifier removal <Name> is not allowed. Attribute <Name> in Class <Name>. Ein Benutzer hat einen Attributqualifizierer entfernt, der mit dem Standardklassenmodell bereitgestellt wurde. Bestimmte Typen von Attributqualifizierern dürfen nicht aus Werk-Attributen entfernt werden.
- Attribute Qualifier removal <Name> in override is not allowed. Attribute <Name> in Class <Name>. Ein Benutzer hat einen Attributqualifizierer in einer Attribut-Überschreibung entfernt, die mit dem Standardklassenmodell bereitgestellt wurde. Bestimmte Typen von Attributqualifizierern dürfen nicht aus Werk-Attribut-Überschreibungen entfernt werden.
- Valid Link <Name> removal is not allowed. Ein gültiger Link wurde von einem Benutzer entfernt oder konnte nicht aus Content Pack 6.00 bereitgestellt werden. Der gültige Link wird im Benutzerklassenmodell wiederhergestellt.
- Calculated Link <Name> removal is not allowed. Class <Name>. Ein berechneter Link wurde vom Benutzer entfernt oder konnte nicht aus Content Pack 6.00 bereitgestellt werden. Der berechnete Link wird im Benutzerklassenmodell wiederhergestellt.
- TypeDef <Name> removal is not allowed. Wenn eine Werk-Typdefinition (Aufzählung oder Liste) im Benutzerklassenmodell fehlt, wird sie im Modell wiederhergestellt. Die Definition kann fehlen, weil sie vom Benutzer entfernt wurde oder weil bei der Content Pack 6.00-Bereitstellung ein Fehler aufgetreten ist.

- Enum entry removal is not allowed. Enum <Name> with Enum entry key <Schlüssel> and Enum entry value <Wert>. Wenn ein Aufzählungseintrag in einer Aufzählungstypdefinition fehlt, wird der Eintrag in der Aufzählungsdefinition wiederhergestellt. Der Aufzählungseintrag kann fehlen, weil er vom Benutzer entfernt wurde oder weil bei der Content Pack 6.00-Bereitstellung ein Fehler aufgetreten ist.
- List entry removal is not allowed. List <Name> with List entry value <Wert>. Wenn ein Listeneintrag in einer Listentypdefinition fehlt, wird der Eintrag in der Liste wiederhergestellt. Der Listeneintrag kann fehlen, weil er vom Benutzer entfernt wurde oder weil bei der Content Pack 6.00-Bereitstellung ein Fehler aufgetreten ist.
- Enum entry addition can cause conflicts. Enum <Name> with Enum entry key <Schlüssel> and Enum entry value <Wert>. Ein Benutzer hat einen Eintrag zu einer Aufzählungstypdefinition hinzugefügt. Zu diesem Zeitpunkt des Upgrades liegen nicht genug Informationen vor, um zu entscheiden, ob das Upgrade aufgrund des hinzugefügten Eintrags fehlschlägt.
- List entry addition can cause conflicts. List <Name> with List entry value <Wert>. Ein Benutzer hat einen Eintrag zu einer Listentypdefinition hinzugefügt. Zu diesem Zeitpunkt des Upgrades liegen nicht genug Informationen vor, um zu entscheiden, ob das Upgrade aufgrund des hinzugefügten Eintrags fehlschlägt.

- Bei Änderungen des Attributtyps wird ein Fehler mit dem Namen des Attributs und seiner Klasse ausgegeben.
- Änderungen der Hierarchie führen zu einer Warnung mit dem Namen der Klasse, deren übergeordnete Klasse sich geändert hat.
- Bei Problemen mit dem Benutzerklassenmodell wird die folgende Fehlermeldung ausgegeben: User class model is not valid for upgrade.
- Bei Problemen mit Klassenmodelltransformationen wird die folgende Fehlermeldung ausgegeben: Upgrade configuration files are not valid.

Upgrade Class Model on Disk

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Verwendet das Klassenmodell, das im Schritt "Validate Class Model" erzeugt wurde (**C:\hp\UCMDB\UCMDBServer\runtime\original-fixed-class-model.xml**), sowie die vordefinierten Transformationsdateien, um das aktualisierte Klassenmodell zu erzeugen. Dieses aktualisierte Modell wird auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml** gespeichert. Weitere Informationen finden Sie unter "Validate Class Model" auf Seite 199.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Das Klassenmodell kann derzeit nicht ordnungsgemäß aktualisiert werden.

- **Lösung 1**: Bearbeiten Sie die problematischen Klassen in der UCMDB 8.0x-Instanz und führen Sie das Upgrade erneut aus.
- **Lösung 2**: Bearbeiten Sie die Änderungsdateien für das Klassenmodell. Weitere Informationen finden Sie unter "Validate Class Model" auf Seite 199. Wenn Sie diese Dateien bearbeiten, müssen Sie den Schritt "Validate Class Model" erneut ausführen, bevor Sie das Upgrade fortsetzen.

Protokolldateien

- **Allgemeine Meldungen (alle Klassenmodellentitäten der höchsten Ebene)**:
  - Adding non-modified <Typ der Entität> <Name der Entität>. Die Entität wurde zwischen Benutzer- und Zielklassenmodell nicht geändert. Diese Meldung kann auch Adding un-upgraded… lauten.
  - Adding <Typ der Entität> <Name>. Eine aktualisierte Entität wird zum Zielklassenmodell hinzugefügt.

- Skipping <Typ der Entität> <Name> - Dropped in upgrade. Die Entität muss explizit aus dem Upgrade entfernt werden. Diese Meldung kann auch Not adding… lauten.
- Skipping <Typ der Entität> <Name> - exists in new basic CM. Die Entität ist im Basisklassenmodell vorhanden und die dortige Definition wird verwendet.
- Adding new <Typ der Entität> <Name>. Eine neue Entität, die für das Hinzufügen während des Upgrades markiert ist, wird zum Zielklassenmodell hinzugefügt.
- Skipping adding new <Typ der Entität> <Name> - exists in new basic CM. Eine neue Entität, die für das Hinzufügen während des Upgrades markiert ist, wird nicht zum Zielklassenmodell hinzugefügt, da sie bereits im Basisklassenmodell festgelegt ist.

- **Meldungen für berechnete Links**:
  - Skipping calculated link <Name> - exists in new basic CM, adding only triplets. Der berechnete Link ist im Basisklassenmodell vorhanden, aber Dreiergruppen aus dem Benutzerklassenmodell werden hinzugefügt, um (TQL-) Abfrageergebnisse beizubehalten.
- **Meldungen für Klassen**:
  - About to upgrade class <Name>. Diese Meldung wird vor dem Upgrade einer Klasse erstellt. Tritt ein Fehler auf, kann anhand dieser Meldung verfolgt werden, welche Klasse den Fehler verursacht hat.
  - Skipping class <Name> - already added as a calculated link. Die Klasse wurde bereits als Teil eines berechneten Links hinzugefügt. Aus den vorherigen Protokollmeldungen geht hervor, was genau mit dieser Klasse geschehen ist.
  - skipping adding new class <Name> extends <Name der übergeordneten Klasse> which does not exist. Die Klasse wird nicht zum Klassenmodell hinzugefügt, weil die übergeordnete Klasse im Zielklassenmodell nicht gefunden wurde.
- **Meldungen für gültige Links**:

- Skipping adding new valid link <Name> - <Ende> class <Klassenname> does not exist. Der gültige Link kann nicht hinzugefügt werden, weil eine Klasse (**Ende 1**, **Ende 2** oder **Link**) im Zielklassenmodell nicht gefunden wurde.

- Duplicate CITs found: <Namen>. Aufgrund eines Fehlers wurden CITs doppelt zum Zielklassenmodell hinzugefügt. Dieser Fehler kann nur behoben werden, indem die Änderungsdateien für das Upgrade des Klassenmodells bearbeitet werden und die Schritte zur Prüfung des Klassenmodells und zum Upgrade des Klassenmodells erneut ausgeführt werden. Weitere Informationen finden Sie unter "Validate Class Model" auf Seite 199 und "Upgrade Class Model on Disk" auf Seite 205.

- Adding <alter Name> > <neuer Name> to rename map. Die Umbenennungskarte wird verwendet, um alte Klassennamen zu bestimmen und sie den neuen Klassennamen zuzuordnen.

- Mismatch between incremental rename map and changes util! Using incremental rename map. Incremental: <alter Name> > <neuer Name>. Util: <alter Name 2> > <neuer Name 2>. Die Umbenennungskarte und die Upgrade-Definition stimmen nicht überein. Diese Meldung sollte zur Überprüfung vermerkt werden, da sie auf ein Problem beim Upgrade des Klassenmodells hinweisen kann. Der Upgrade-Prozess wird durch diese Meldung jedoch nicht angehalten.

- **Prüfung gültiger Links**:

  - Start removing invalid links. Gültige Links müssen überprüft werden und ungültige Links (d. h. keine Klasse vom Typ **Ende 1**, **Ende 2** oder **Link**) werden entfernt.

  - Link <Entität> <Name> does not exist in target class model - Removing valid link <Name>. Die Entität des gültigen Links (Klasse **Ende 1**, **Ende 2** oder **Link**) ist im Zielklassenmodell nicht vorhanden, sodass der gültige Link entfernt werden muss, damit das gesamte Klassenmodell gültig ist. Dies kann später dazu führen, dass Fehler beim Upgrade von Ressourcen (z. B. TQLs und Ansichten) auftreten.

  - Start removing invalid links. Diese Meldung wird angezeigt, wenn dieser Unterschritt abgeschlossen ist.

➤ Bei Benutzerklassen, deren Schlüsselattribute von den übergeordneten Klassen abweichen, werden alle Schlüsselattribute wiederhergestellt. Für jedes Schlüsselattribut, das aus dem Standardvorgänger entfernt und zur neuen Benutzerklasse hinzugefügt wurde, wird im Protokoll die folgende Informationsmeldung erstellt: Added ID qualifier to attribute <Attributname> in class <Klassenname>.

Prepare Required Actions for Data Upgrade

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Verwendet die Datei **C:\hp\UCMDB\UCMDBServer\runtime\original-class-model.xml**, die Datei **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml** und die Klassenmodelltransformationen, um die erforderlichen Aktionen für die Datentransformation abzuleiten.

Speichert das Analyseergebnis auf der Festplatte in der folgenden Datei: **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-actions.xml**. Bei diesem Schritt werden CITs übersprungen, durch die das Daten-Upgrade die Daten auslässt, die nicht aktualisiert werden können. Die CITs sind in der Datei **C:\hp\UCMDB\UCMDBServer\upgrade\DataModelUpgradeConfig.xml** (**app-infra.jar**) aufgelistet.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Das Upgrade kann nicht die erforderlichen Aktionen ableiten, um das Datenmodell vom Klassenmodell der vorherigen Version in das Zielklassenmodell umzuwandeln. Das Konfigurations- und Daten-Upgrade kann erst fortgesetzt werden, wenn dieser Schritt abgeschlossen ist.

Protokolldateien – Erste Analyse

Hinweis: In diesem Abschnitt steht **DE** für Datenelemente: CIs oder Links.

Allgemeine Informationen

- Bei diesem Schritt wird die Daten-Upgrade-Konfiguration als eine Reihe von Kopierregeln mit möglichen Transformationen und Bedingungen betrachtet.
- Für ein Attribut sind folgende Quellen möglich:
  - Eine Eigenschaft des Quell-DE.
  - Ein konstanter Wert für alle DEs einer bestimmten konkreten Klasse.
- Die Protokolle für diesen Schritt sind verschachtelt (mit Einrückungen). Einer eingerückten Protokollmeldung geht in der Regel eine Kopfzeile voraus, die den Analysekontext angibt.
- Typen von Klassenregeln:
  - Geändert, Verschoben, Zusammengeführt. Wenn DEs zu Regeln gehören, die als einer dieser Typen markiert sind, sollen die DEs in das neue Datenmodell kopiert werden (mit möglichen Transformationen).
  - Hinzugefügt, Veraltet. Diese CITs sind neu. Daher können sie keine DEs aufweisen.
  - Entfernt. Diese CITs werden während des Upgrades explizit entfernt. Ihre DEs werden nicht in das Zielklassenmodell kopiert (außer wenn eine andere Regel etwas anderes vorschreibt).
- Typen von Attributregeln:
  - Hinzugefügt. Die Regel definiert ein Attribut, das entweder neu ist oder seinen Namen behält.
  - Veraltet, Geändert. Die Regel definiert eine Transformation eines vorhandenen Attributs, das umbenannt wird.
  - Entfernt. Die Regel definiert, dass dieses Attribut im Ziel-DE nicht vorhanden sein soll.

- Standardregel oder Standardaktion. Für einen bestimmten CIT definiert. Dies bedeutet, dass die Namen von Ziel-CIT und Quell-CIT identisch sind. Attribute von DEs, die auf der Ziel-CIT-Ebene definiert sind, werden aus Attributen mit demselben Namen auf der Quell-CIT-Ebene kopiert. Für Attribute im übergeordneten CIT werden die Regeln des übergeordneten CIT verwendet.

Allgemeine Klassen- oder Regelanalyse

- Rule type for class <Name> is <Typ>. Die Analyse für die angegebene Klasse wird nun gestartet.
- Class <Name> added to added CITs. Der CIT ist neu, sodass keine DEs dafür vorhanden sind. Der CIT wird in einer Referenzliste mit den hinzugefügten CITs in der XML-Datei erfasst.
- Class <Name> added to removed CITs. Der CIT ist zusammen mit allen seinen DEs zum Entfernen markiert.
- Change has empty class name. Eine Warnung, dass die angeforderte Transformation ungültig ist und keine Aktion durchgeführt wird. Grund: ungültige Transformationsdefinition.
- Target CIT name is <Name>, Source CIT name is <Name> (from <Quelle>). DEs aus dem Quell-CIT werden in den Ziel-CIT kopiert.
- Target CIT <Name> does not exist in target class model, skipping rule! Eine Warnung, dass der Ziel-CIT nicht ordnungsgemäß erstellt wurde. Die gesamte Regel wird übersprungen, weil sie nicht abgeschlossen werden kann. Grund: ungültige Transformationsdefinition oder Fehler beim Upgrade des Klassenmodells.
- Source CIT <Name> does not exist in source class model, skipping rule! Eine Warnung, dass der Quell-CIT nicht im Benutzerklassenmodell gefunden wurde. Die gesamte Regel wird übersprungen, weil sie nicht abgeschlossen werden kann. Grund: ungültige Transformationsdefinition, Fehler beim Upgrade des Klassenmodells oder das Benutzerklassenmodell (nach Problembehebungen) entspricht nicht dem 8.0x-Klassenmodell.

- Source CIT <Name> does not exist in source class model, skipping rule, adding to added CITs! Eine Warnung, dass die Regeln nicht dem tatsächlichen Klassenmodell entsprechen. Der Quell-CIT wurde nicht gefunden, sodass der Ziel-CIT wie ein neuer CIT behandelt werden muss (d. h., es gibt kein Daten-Upgrade). Grund: ungültige Transformationsdefinition, Fehler beim Upgrade des Klassenmodells oder das Benutzerklassenmodell (nach Problembehebungen) entspricht nicht dem 8.0x-Klassenmodell.
- Source CIT is empty, Target CIT is empty. Eine Warnung, dass die Transformationsregel ungültig ist. Die Regel wird übersprungen. Grund: ungültige Transformationsdefinition.

Analyse der Kopierbedingungen

- Could not create copy condition for source CIT <Name> - CIT does not exist in old class model. Die Klasse weist eine Bedingung für das Kopieren von DEs auf, aber dieser Quell-CIT ist im Benutzerklassenmodell nicht vorhanden. Eine Warnung, dass die Bedingung ignoriert wird. Grund: ungültige Transformationsdefinition oder das Benutzerklassenmodell (nach Problembehebungen) entspricht nicht dem 8.0x-Klassenmodell.
- Could not create copy condition for source CIT <Name> and attribute <Attributname> - CIT exists but does not have the attribute. Die Klasse weist eine Bedingung für das Kopieren von DEs auf, aber dieses Attribut im Quell-CIT ist im Benutzerklassenmodell nicht vorhanden. Eine Warnung, dass die Kopieranweisung ignoriert wird. Grund: ungültige Transformationsdefinition oder das Benutzerklassenmodell (nach Problembehebungen) entspricht nicht dem 8.0x-Klassenmodell.
- Copy condition attribute: <Name>, Type: <Typ>, Operator: <Operator>, Copy condition value: <Wert>. Damit ein DE kopiert (und nicht verworfen) wird, muss der Wert des Attributs die angegebene Bedingung beibehalten (z. B. **IP-Port ungleich 3**).
- Attribute condition.attribute name is empty. Der Attributname ist leer. Eine Warnung, dass die Kopierbedingung ungültig ist und nicht verwendet wird (alle DEs werden kopiert). Grund: ungültige Transformationsdefinition.

- Copy condition value is empty. Der Wert der Kopierbedingung ist leer. Eine Warnung, dass die Kopierbedingung ungültig ist und nicht verwendet wird (alle DEs werden kopiert). Grund: ungültige Transformationsdefinition.

Allgemeine Attributanalyse

- Entering copy attribute analysis. Die Attributanalyse wird nun gestartet.
- Rule type for attribute <alter Name> > <neuer Name> is <Regeltyp>. Die Analyse für diese Regel wird nun gestartet. Hinweis: Die Typen ZUSAMMENGEFÜHRT und VERSCHOBEN gibt es bei Attributregeln nicht.
- Rule type changed from <ursprünglicher Typ> to ADDED - no old name or oldName == Name. Obwohl die Regel als geändert definiert ist, muss dieses Attribut bei der Datenaktion als hinzugefügt behandelt werden, da entweder der Attributname nicht geändert wurde oder kein solches altes Attribut vorhanden ist (Unterschied zwischen dem Benutzerklassenmodell und dem erwarteten 8.0x-Klassenmodell).
- No target class <Name> in new class model. Eine Warnung, dass die Zielklasse im Zielklassenmodell nicht gefunden wurde und diese Attributregel übersprungen wird. Grund: Fehler beim Upgrade des Klassenmodells.
- No target attribute <Name> in target class <Klassenname> in new class model. Eine Warnung, dass das Zielattribut in der Zielklasse im Zielklassenmodell nicht gefunden wurde und diese Attributregel übersprungen wird. Grund: Fehler beim Upgrade des Klassenmodells.
- Attribute <Name> in class <Klassenname> in new class model is declared STATIC_ATTRIBUTE. Skipping rule. Statische Attribute sind mit dem CIT und nicht mit dem eigentlichen DE verbunden. Daher sollen sie während des Daten-Upgrades nicht kopiert werden.
- Attribute <Name> in class <Klassenname> in new class model is of simple list type. Skipping rule. Wertelisten (mehrere Werte) werden in einem anderen Upgrade-Schritt verarbeitet und an dieser Stelle übersprungen.

- Attribute <Name> is a root class attribute that is not duplicated to concrete classes. Skipping rule. Diese Regel wird übersprungen, weil das Attribut nicht in die konkreten Klassentabellen in der Datenbank kopiert werden soll.

Analyse zum Kopieren von Attributen aus Klassen

- Copy attribute from class. Dieser Attributwert wird von der konkreten Klasse des DE bestimmt.
- Attribute constant value: <Wert>. Bei dieser konkreten Klasse weist das Attribut den in der Meldung angegebenen Wert auf.

Analyse zum Kopieren von Attributen aus Attributen

- Copy attribute from attribute. Dieser Attributwert wird von einem anderen Attribut bestimmt.
- Old attribute name: <Name>. Gilt für ein hinzugefügtes Attribut: Das Quellattribut weist den in der Meldung angegebenen Namen auf.
- Source attribute name (from enum): <Name>, Source attribute name (from OldName): <Name>. Gilt für ein geändertes Attribut: Die Quelle für diese Regel ist entweder konstant (from enum) oder ein anderes Attribut (from OldName).
- **Zugeordnete Transformation im Kopierattribut**:
  - Entering map transformation analysis. Die Quelle soll durch eine Quelle-Ziel-Zuordnung (Dictionary) umgewandelt werden.
  - Adding transformation: <alter Wert> > <neuer Wert>. Der alte Wert soll durch den neuen Wert ersetzt werden.
  - From value is empty. To value is empty. Der Von- bzw. Zu-Wert ist leer und die Transformation wird nicht durchgeführt. Grund: ungültige Transformationsdefinition.

Analyse für hinzugefügte Attribute (neu oder nicht umbenannt)

- Copy attribute from default value: <Name>. Das Attribut hat keine Attributquelle, sodass sein Wert durch den neuen Standardwert bestimmt wird.

- Attribute name is empty, Attribute default value is empty. Die Attributregel ist ungültig und wird nicht verwendet. Grund: ungültige Transformationsdefinition.

Analyse für geänderte Attribute (umbenannt)

- Copy attribute from default value: <Name>. Der Attributwert wird von einem anderen Attribut im Quell-DE bestimmt.
  - Attribute name is empty, Attribute default value is empty. Die Attributregel ist ungültig und wird nicht verwendet. Grund: ungültige Transformationsdefinition.

Übliche Attributanalyse

- Completing and adding. Eine Meldung, dass das Upgrade mit der allgemeinen Analyse für diese Attributregel beginnt.
- Attribute was not properly completed. Die allgemeine Analysephase ist fehlgeschlagen und die Attributregel wird nicht verwendet. Dieser Meldung geht eine der folgenden voran:
  - Target CIT empty. Der Ziel-CIT ist leer. Grund: ungültige Regel.
  - Target CIT does not exist in new class model. Der Ziel-CIT ist leer. Grund: ungültige Regel oder Fehler beim Upgrade des Klassenmodells.
  - Target attribute name is empty. Der Name des Zielattributs ist leer. Grund: ungültige Regel.
  - Target attribute <Name> does not exist in target CIT in new class model! Das Attribut wurde im Zielklassenmodell nicht gefunden. Grund: ungültige Regel oder Fehler beim Upgrade des Klassenmodells.
  - Cannot determine target type <Name>. Der Typ des Zielattributs ist ungültig. Grund: Fehler beim Upgrade des Klassenmodells.
  - Source CIT name is empty. Der Quell-CIT ist leer. Grund: ungültige Regel, Fehler beim Upgrade des Klassenmodells oder vorheriger Fehler bei der Datenaktionsanalyse.
  - Source attribute name is empty, Source attribute is null. Der Quell-CIT ist leer. Grund: ungültige Regel, Fehler beim Upgrade des Klassenmodells oder vorheriger Fehler bei der Datenaktionsanalyse.

- Typen:
  - Setting new type <Typ>, Setting old type <Typ>. Für das Attribut wurde der angegebene Typ festgelegt. Diese Angabe wird später verwendet, um die richtige SQL-Typkonvertierung zu erstellen.
  - Target attribute is <Name>, Source attribute is <Name>. Das Attribut weist den in der Meldung angegebenen Namen auf.
  - Constant value requires new type declaration. New type and old type are <Typ>. Das Attribut soll durch einen konstanten Wert mit dem angegebenen Typ gefüllt werden.
- Standardwerte:
  - Target default value is <Wert>. Das Zielattribut hat einen Standardwert. Dieser Wert wird verwendet, wenn die ursprüngliche DE-Eigenschaft leer ist.
  - Source default value is <Wert>. Wenn die ursprüngliche DE-Eigenschaft dem alten Standardwert entspricht, wird sie in den neuen Standardwert umgewandelt.
- Größenbeschränkungen:
  - New size set <Größe> set from default, Constant value new size is <Größe>. Das Zielattribut hat den Typ Zeichenkette. Daher muss es eine Größenbeschränkung aufweisen. Da kein Wert angegeben wurde, wird die Standard-Größenbeschränkung verwendet (50 Zeichen).
  - Old size is <Größe>, setting truncate flag. Die Ziel-Größenbeschränkung ist kleiner als die Quell-Größenbeschränkung. Werte können verkürzt werden.
  - New size is <Größe>. Es wurde eine neue Größenbeschränkung festgelegt.

- Attribute did not pass validation. Die abschließende Prüfung wurde nicht bestanden, sodass die Attributregel nicht verwendet wird. Die Ursachen müssen den Meldungen für die eigentliche Aktionserstellung entnommen werden. Dieser Meldung muss eine der folgenden vorangehen:
  - No target attribute. Aus einem beliebigen Grund bleibt der Name des Zielattributs leer.
  - Target attribute does not exist in target class model. Das Zielattribut ist im Zielklassenmodell nicht vorhanden.
  - No source. Die Attributquelle (Quellattribut oder konstanter Wert) kann nicht bestimmt werden.
  - Source attribute does not exist in source class model
  - Source attribute size limit > Target attribute size limit but truncate needed flag is false.
  - Target attribute target type is missing.
  - Target attribute source type is missing.
  - Target attribute source and target types are not the same, but attribute source is of type CONSTANT_VALUE.
  - Instruction for target attribute already exists. Werte für das Zielattribut in diesem bestimmten CIT werden bereits durch eine andere Regel erzeugt.
  - Value transformation source is empty, Value transformation target is empty. Die Transformation der Wertekarte ist ungültig.

Protokolldateien – Nach der Analyse

Rules Flattening. Die in den Klassenmodelländerungen definierten Regeln wurden in Aktionen umgesetzt. In dieser Phase werden Regeln aus übergeordneten Klassen in untergeordnete Klassen kopiert, um einen vollständigen, nicht-trivialen Regelsatz zu erstellen, der nicht an die Klassenhierarchie gebunden ist.

- Flatten rules stage. Die Phase beginnt.
- Building class to direct children map. Das Erstellen eines vollständigen Dictionary für die Zuordnung von übergeordneten Klassen zu untergeordneten Klassen wird gestartet.
  - Class <Name der untergeordneten Klasse> is a child of <Name der übergeordneten Klasse>.
  - Class appeared twice. Warnung, dass eine Klasse zweimal gefunden wurde. Höchstwahrscheinlich ist das Klassenmodell nicht gültig.
- Building by target and by source rules map. Das Erstellen von zwei Dictionarys für die Zuordnung von Klassen zu Regeln wird gestartet: Eines davon ist Quellklasse-zu-Regel und das andere Zielklasse-zu-Regel.
  - Found rule from <Quelle> to <Ziel>.
  - Adding this rule will corrupt the by target map, By source map already contains this CIT. Eine Warnung, dass die Regel nicht zur Karte hinzugefügt werden kann, weil bereits eine andere Instanz davon unter einer anderen Quell- oder Zielklasse vorhanden ist. Die Regel wird für untergeordnete Klassen ignoriert.
- Entering DFS over target class model. Die Phase zur Abflachung der Struktur wird gestartet, indem das Klassenmodell von oben nach unten durchlaufen wird.
  - Visiting <Klasse> (added <untergeordnete Klassen> children). Die Verarbeitung der angegebenen Klasse wird gestartet. Dabei wurde festgestellt, dass diese Klasse die angegebenen untergeordneten Klassen aufweist, die später verarbeitet werden.
  - No rule for <Name>, it exists in old class model and it was not explicitly added or removed - adding default rule. Eine Standardregel wird verwendet, um die DEs dieses CIT zu kopieren.

- Visiting rule from <Name der Quellklasse>. Die Suche nach Attributregeln vom angegebenen Quell-CIT aus wird gestartet. In dieser Phase wird die Quellstruktur von unten (vom angegebenen CIT) nach oben (Stamm) überprüft, um den richtigen Regelsatz zu erfassen. Die unterste Regel, die einen Wert für ein Zielattribut erzeugt, wird verwendet.
  - Visiting source class <Name>. Die angegebene Quellklasse wird überprüft.
  - Found rule from source class <Quelle> to <Ziel>. Das Überprüfen der angegebenen Attribut-Kopierregel wird gestartet.
  - Rule matches for flattening. Die Regel kann für die Zielklasse angewendet werden (die Zielklasse der Regel ist die **aktuelle** Zielklasse oder eine übergeordnete Klasse davon).
  - Going over source rules with targets: <Ziele>. Das Untersuchen der Regel mit den angegebenen Zielattributen wird gestartet.

    Rule to <Ziel> is not mapped - attribute exists in concrete source class and concrete target class. Die Regel wird nicht verwendet, weil das Attribut in der konkreten Quellklasse und in der konkreten Zielklasse vorhanden ist (es soll im derzeitigen Zustand kopiert werden).

    Rule to <Ziel> is not mapped. Für das angegebene Zielattribut besteht immer noch keine Regel für die Werterzeugung.

    Rule is not in ignore list - adding to target attribute rules. Die angegebene Regel wird verwendet, um Werte für das Zielattribut zu erzeugen.

    Attribute did not pass validation. Die Prüfung der Attributregel wurde nicht bestanden. Informationen zu möglichen Meldungen und Ursachen bei der Prüfung finden Sie im vorherigen Abschnitt.

    Rule is in ignore list - not added. Das Attribut kann nicht kopiert werden (und ist entsprechend markiert), sodass es nicht verwendet werden kann.

- Going over ignore list: <Attribute>. Entfernte Attribute werden in dieser Liste angezeigt. Attribute aus dieser Liste sollen nicht in das Zielattribut kopiert werden. Da die Untersuchung von unten nach oben erfolgt, wird diese Liste auf jeder CIT-Ebene erstellt und ergänzt.

  Adding ignored attribute <Name>. Ein Attribut wurde in der Liste der nicht zu kopierenden Attribute gefunden. Es wird zur aktuellen Liste der zu ignorierenden Attribute hinzugefügt, damit es nicht kopiert wird, falls es im übergeordneten CIT erscheint.

- Going over copy conditions. Kopiert die Kopierbedingungen (ob das DE überhaupt kopiert werden soll). Dies wird auch aus der übergeordneten Klasse kopiert (die unterste Regel erhält Vorrang).

  Copy condition is for attribute name <Name>. Es wurde eine Kopierbedingung gefunden, die vom angegebenen Attribut abhängt.

  Adding copy condition for attribute name <Name> with values <Werte>. Das Attribut wurde noch nicht durch eine andere Kopierbedingung eingeschränkt. Nun wird es durch die "aktuelle" Kopierbedingung eingeschränkt.

Phase zur Eliminierung abstrakter Klassen. Abstrakte CITs haben keine DEs (oder Tabellen unter dem neuen Datenmodell). Für diese CITs erstellte Regeln (Abflachungsprozess, Fehler und fehlende Übereinstimmung zwischen 8.0x-Benutzerklassenmodell und dem erwarteten Klassenmodellergebnis) werden nun gelöscht.

- Remove abstract classes stage. Die Phase wird gestartet.
- Removing rule from <Quellname> to <Zielname> - <Quelle/Ziel> is abstract in new class model. Diese Kopierregel wird entfernt, weil entweder der Quell-CIT oder der Ziel-CIT als abstrakt markiert ist.

Phase für triviale Regeln. Wenn ein Attribut mit demselben Namen im Quell-CIT vorhanden ist und der Attributname nicht zu den Attributen gehört, die nicht kopiert werden sollen, wird eine Standardregel dafür hinzugefügt.

- Found rule from <Quellklasse> to <Zielklasse>. Die angegebene Regel wird verarbeitet.
- Adding CMDB_ID rule. Alle CITs sollen eine Regel für das Kopieren der Spalte mit der CMDB-ID aufweisen.
- Target class <Klassenname> is a link. Adding <Ende 1> and <Ende 2> rules. Alle Link-Klassen sollen zwei Regeln für das Kopieren der Spalte für Ende 1 und der Spalte für Ende 2 aufweisen.
- Checking attribute <Name>. Das angegebene Attribut wird verarbeitet.
- Attribute <Name> has qualifier STATIC_ATTRIBUTE, skipping. Das Attribut ist statisch und soll daher nicht kopiert werden.
- Attribute <Name> is CmdbSimpleList, skipping. Attribute mit mehreren Werten werden in einem anderen Upgrade-Schritt verarbeitet, sodass keine Regel benötigt wird.
- Attribute <Name> appears in root, skipping. Das Attribut erscheint in der Stammklasse und wird nicht in den untergeordneten Tabellen dupliziert, sodass keine Regel benötigt wird.
- Attribute is not mapped, nor in 'do not copy' list. Das Attribut soll mit einer Standardregel kopiert werden.
- Found source attribute with the same name - creating default copy rule. Ein Attribut mit demselben Namen wurde im Quellklassenmodell gefunden, sodass es zur Quelle für die Standardregel wird.
- No source attribute, checking default value, Found non empty default value - creating default constant copy rule. Standardeinstellung: <Wert>. Es gibt kein Quellattribut mit demselben Namen, sodass der Standardwert (falls vorhanden) als Quelle für die Standardregel verwendet wird. Falls die zweite Meldung nicht erscheint, wird keine Regel verwendet und der Attributwert bleibt leer.
- Completing and adding. Attribute was not properly completed. Attribute did not pass validation. Diese Meldungen haben dieselbe Bedeutung wie in der ersten Phase.

Prepare SQL Scripts for Data Upgrade

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Analysiert die Datei **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-actions.xml**, erzeugt die SQL-Anweisungen, die für das Daten-Upgrade in der Datenbank ausgeführt werden müssen, und speichert sie auf der Festplatte unter **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql**.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Fehler in diesem Upgrade-Schritt führen dazu, dass die Aktionen (aus der XML-Datei) nicht in die SQL-Anweisungen umgesetzt werden können, durch die das Datenmodell aus dem Klassenmodell der vorherigen Version in das Zielklassenmodell umgewandelt wird. Das Konfigurations- und Daten-Upgrade kann erst fortgesetzt werden, wenn dieser Schritt abgeschlossen ist.

Möglichkeiten zur Fehlerbehebung: Entfernen Sie die problematische Aktion (die gesamte Klasse oder nur das Attribut) aus der XML-Datei für die Daten-Upgrade-Aktionen. Dies führt möglicherweise zu einem Datenverlust (diese Klasse bzw. dieses Attribut wird nicht kopiert), doch das Upgrade kann fortgesetzt werden.

Protokolldateien

- Could not create cast for <Quellklasse> > <Zielklasse>, on <Quelle> > <Zielattribut>. Der SQL-Generator konnte nicht die richtige Methode ermitteln, um den Typ der Quelle (Attribut oder Konstante) in den Typ des Zielattributs umzuwandeln. Mögliche Ursachen sind nicht unterstützte Typkonvertierungen (es werden nicht alle möglichen Typumwandlungen unterstützt) oder eine mangelhafte Analyse (Fehler/falsche Definitionen/unerwartete Änderungen des Benutzerklassenmodells). Als Folge davon werden diese Attributwerte nicht konvertiert. Dies kann während des SQL-Aufrufs dazu führen, dass die Anweisung fehlschlägt. Durch diesen Fehler wird der Upgrade-Prozess nicht angehalten.
- Could not create copy condition for <Quellklasse> > <Zielklasse>. Der SQL-Generator hat die Kopierbedingung nicht verstanden. Mögliche Ursachen sind nicht unterstützte Bedingungen (es werden nicht alle möglichen Bedingungen unterstützt) oder eine mangelhafte Analyse (Fehler/falsche Definitionen/unerwartete Änderungen des Benutzerklassenmodells). Als Folge davon wird diese Kopierbedingung nicht angewendet und alle CIs des Quell-CIT werden kopiert. Durch diesen Fehler wird der Upgrade-Prozess nicht angehalten.
- Default value exceeding 4000 characters is ignored. Table: <Tabelle>. Column: <Spalte>. Der Standardwertesatz für diese Spalte ist zu groß und passt nicht in die SQL-Anweisung. Mögliche Ursache ist ein zu großer Standardwert im Benutzerklassenmodell. Als Folge davon wird kein Standardwert für diese Spalte verwendet. Durch diesen Fehler wird der Upgrade-Prozess nicht angehalten.

Discovery – Upgrade Errors Table

Führt ein Upgrade für die Discovery-Fehlerdaten durch (die in der Tabelle **CCM_DISCOVERY_ERRORS** in der CMDB gespeichert sind). In der Tabelle werden Fehlermeldungen durch Fehlercodes mit Parametern (Discovery-Laufzeitdaten) ersetzt.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Informationen zu Discovery-Fehlern gehen verloren. Wird dieser Schritt ausgelassen, müssen Sie die Tabelle **CCM_DISCOVERY_ ERRORS** in der CMDB kürzen und alle Discovery-Jobs erneut aktivieren, nachdem der Server wieder ausgeführt wird.

Protokolldateien

- Starting upgrade 'CCM_DISCOVERY_ERRORS' table
- Upgrade 'CCM_DISCOVERY_ERRORS' table was successfully finished!
- Failed to upgrade 'CCM_DISCOVERY_ERRORS' table

Discovery – Create New Destination IPs Table

Erstellt in der CMDB eine neue Tabelle mit dem Namen **CCM_DISCOVERY_DEST_IPS**. Die neue Tabelle enthält die IPs der einzelnen Ziele. Die Daten werden aus der Tabelle **CCM_DISCOVERY_DESTS** extrahiert (Discovery-Laufzeitdaten).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Informationen zu Discovery-Zielen gehen verloren. Wird dieser Schritt ausgelassen, müssen Sie die Tabelle **CCM_DISCOVERY_DEST_IPS** in der CMDB kürzen und alle Discovery-Jobs erneut aktivieren, nachdem der Server wieder ausgeführt wird.

Protokolldateien

- Starting upgrade 'CCM_DISCOVERY_DEST_IPS' table
- Upgrade 'CCM_DISCOVERY_DEST_IPS' table was successfully finished!
- Failed to upgrade 'CCM_DISCOVERY_DEST_IPS' table

Discovery – Upgrade Destinations Table

Benennt die CI-Typen in der Tabelle **CCM_DISCOVERY_DESTS** in der CMDB um (Discovery-Laufzeitdaten).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Informationen zu Discovery-Zielen gehen verloren. Wird dieser Schritt ausgelassen, müssen Sie die Tabelle **CCM_DISCOVERY_DESTS** in der CMDB kürzen und alle Discovery-Jobs erneut aktivieren, nachdem der Server wieder ausgeführt wird.

Protokolldateien

- Starting upgrade 'CCM_DISCOVERY_DESTS' table
- Upgrade 'CCM_DISCOVERY_DESTS' table was successfully finished!
- Failed to upgrade 'CCM_DISCOVERY_DESTS' table
- Ci type [alter CI-Typ] has been upgraded to [neuer CI-Typ]. Weist darauf hin, dass die Klasse [alter CI-Typ] umbenannt wurde in [neuer CI-Typ].
- Failed to update [alter CI-Typ], skipped. Zeigt an, dass ein CI-Typ nicht im Einklang mit dem neuen Schema geändert werden konnte, möglicherweise aufgrund einer Dateninkonsistenz in der CMDB oder weil der Benutzer einen falschen CI-Typ definiert hat. Dies beeinträchtigt nicht die Discovery-Funktionalität, kann sich aber auf die Zielanzeige in der Benutzeroberfläche auswirken.

Modify Data Modeling in DB

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Ändert die CMDB-Struktur in die neue 9.00-Struktur.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Fehler führen dazu, dass die Datenbankschemas nicht das richtige Format für die neue UCMDB aufweisen. Der Upgrade-Prozess kann ohne diesen Schritt nicht fortgesetzt werden. Um die erneute Ausführung dieses Schrittes zu versuchen, müssen Sie die CMDB-Schemas aus der Sicherung wiederherstellen, den Ordner **C:\hp\UCMDB\UCMDBServer\runtime** löschen und das Upgrade-Tool von Beginn an ausführen.

Protokolldateien

Keine

Copy E-mail Recipient Information

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die Informationen zu E-Mail-Empfängern aus der Datentabelle **EmailRecipient** in die Verwaltungstabelle **EN_UI_RECIPIENTS** in der CMDB. (In UCMDB 8.x wurden die Empfängerdaten als CI modelliert). **EmailRecipient** wird später als Teil des Daten-Upgrades entfernt.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	Ja, falls das Upgrade des Klassenmodells noch nicht ausgeführt wurde

Fehlerauswirkungen

Geplante Reports werden nicht gesendet. Benutzer müssen Empfänger über den Recipients Manager oder über die aktualisierten geplanten Jobs selbst hinzufügen.

Protokolldateien

- Number of EmailRecipients in the CMDB is x. Die Anzahl der vorhandenen Empfänger.
- Failed to handle Recipient. Das Upgrade ist fehlgeschlagen.
- RecipientUpgrader is complete. Das Upgrade war erfolgreich.

Copy Report's Scheduling Information

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die Konfiguration für geplante Reports aus der Foundations-Datenbank in die neue Verwaltungstabelle der CMDB.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Die geplanten Reports werden nicht aktualisiert, sodass Sie sie erneut planen müssen.

Protokolldateien

- Upgrade of scheduled report finished successfully.
- Failed to upgrade scheduled reports. Allgemeiner Fehler.
- Failed to upgrade scheduled report of job name <Jobname>. Fehler bei einem bestimmten Job.

Copy Resources to Disk

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Extrahiert Abfragen, Ansichten, Reports, Enrichments und Korrelationen aus der Datenbank und speichert sie auf der Festplatte. Die Ressourcen werden im Unterordner **C:\hp\UCMDB\UCMDBServer\runtime\1\<Ressourcentyp>\<Unterordner name>** gespeichert. Der Ressourcentyp kann folgendermaßen lauten:

- **bacviews**. Alter Ressourcentyp, den es in 9.0 nicht gibt.
- **bundles**. Wird zum Definieren einer Ressourcengruppe verwendet. Ermöglicht Viele-zu-Viele-Beziehungen.
- **cmdbview**. Neue Ansichtsdefinition, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **Correlations**. Korrelationsregeln, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **Enrichments**. Enrichment-Regeln, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **goldmaster**. Goldmaster-Report-Definition, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **Patterns**. Abfragen (TQLs), für die ein Upgrade der Struktur und des Klassenmodells ausgeführt wird.
- **reports**. Topologie-Reports, die zunächst durch ein Struktur-Upgrade zu "cmdbview" werden, bevor das Klassenmodell-Upgrade ausgeführt wird.
- **singlepatternref**. Perspektive-basierte Abfrage, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **viewrefs**. Perspektive-basierte Ansicht, für die nur ein Klassenmodell-Upgrade ausgeführt wird.
- **views**. Alte Ansichtsdefinitionen, die durch ein Struktur-Upgrade zu "cmdbview" werden.

Der Unterordner kann folgendermaßen lauten:

- **db**. Ursprüngliche Ressourcen.
- **structure**. Ressourcen nach dem Struktur-Upgrade.
- **classmodel**. Ressourcen nach dem Klassenmodell-Upgrade.

Ressourcen werden in zwei Phasen aktualisiert:

- **Struktur-Upgrade**. Aktualisiert die Ressourcen vom alten in das neue Format. Dieser Schritt wird für Pattern, Ansichten und Topologie-Reports durchgeführt. Aktualisierte Ressourcen werden im Ordner **structure** gespeichert, mit Ausnahme von Ansichten und Reports, die beide im Ordner **cmdbview\structure** aktualisiert werden. Ressourcen mit einem Struktur-Upgrade werden vom Unterordner **db** in den Unterordner **structure** kopiert.
- **Klassenmodell-Upgrade.** Aktualisiert die Ressourcen gemäß den Klassenmodelltransformationen. Dies betrifft alle Ressourcen. Aktualisierte Ressourcen werden im Ordner **classmodel** gespeichert.

Neben den Ressouren werden einige zusätzliche Daten kopiert: **bundles** (Ressourcengruppierung) und **bacviews** (Ansichtsverarbeitung). Diese werden während des Upgrades nicht geändert.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Ressourcen können nicht aktualisiert werden, weil auf der Festplatte keine Ressourcen für das Upgrade vorhanden sind. Versuchen Sie nicht fortzufahren, ohne diesen Schritt abzuschließen.

Protokolldateien

- Meldungen zum Abrufen von Ressourcen aus der Datenbank:
  - Got <Anzahl> <Ressourcentyp> from database. Gibt an, wie viele Ressourcen für jeden Ressourcentyp aus der Datenbank abgerufen wurden. Dieser Meldung folgt eine Liste mit den Ressourcennamen.
  - Did not succeed to read <Ressourcentyp> from database . In der Ausnahme, die mit der Meldung angezeigt wird, finden Sie die Problembeschreibung.
  - Did not succeed to write <Ressourcentyp> to disk! Suchen Sie in der zugehörigen Ausnahme nach der Ursache. Stellen Sie sicher, dass Schreibberechtigungen und ausreichend Festplattenplatz vorhanden sind.

- Could not write resource <Name>. Suchen Sie in der zugehörigen Ausnahme nach der Ursache. Stellen Sie sicher, dass Schreibberechtigungen und ausreichend Festplattenplatz vorhanden sind.
- Did not succed to write resource bundles to disk! Suchen Sie in der zugehörigen Ausnahme nach der Ursache. Stellen Sie sicher, dass Schreibberechtigungen und ausreichend Festplattenplatz vorhanden sind.

- Meldungen zum Entfernen von Ressourcen aus der Datenbank:
  - Did not succeed to remove all <Ressourcentyp> from database. In der Ausnahme, die mit der Meldung angezeigt wird, finden Sie die Problembeschreibung.
  - Did not succeed to remove from database all <Ressourcentyp> additional data for <Ressourcentyp>. In der Ausnahme, die mit der Meldung angezeigt wird, finden Sie die Problembeschreibung.

Truncate Data Tables

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Entfernt alle irrelevanten Daten aus den CMDB- und History-Schemas. Alle Nicht-Konfigurationsdaten, die nicht für das Upgrade vom Typ "Nur Ressourcen" erforderlich sind, werden in diesem Schritt gelöscht.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Nicht aktualisierte Daten verbleiben in den CMDB- und History-Schemas. Da ein Teil der Daten in den nächsten Schritten nicht aktualisiert wird, ist das Systemverhalten nach beendetem Upgrade nicht vorhersehbar.

Protokolldateien

- Truncating table <Name>. Alle Daten werden aus der angegebenen Tabelle entfernt.
- Table <Name> will not be truncated (data is needed for resources upgrade). Die Tabelle enthält Konfigurationsdaten, die nicht gelöscht werden.
- Query to delete unrelevant data from root table: <SQL-Anweisung>. Durch diese Anweisung werden alle irrelevanten Daten aus der Stammtabelle entfernt.

Rename Original Data Tables

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Benennt die alten Datentabellen um und fügt dabei das Präfix **TEMP_** zu den Namen aller CDM-Tabellen hinzu.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Der Upgrade-Prozess muss von Beginn an erneut ausgeführt werden, nachdem das Problem behoben wurde. Stellen Sie die Datenbankschemas wieder her, löschen Sie den Ordner **C:\hp\UCMDB\UCMDBServer\runtime** und starten Sie das Upgrade von ganz vorne.

Protokolldateien

Keine

Upgrade Class Model in DB

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kürzt die Klassenmodelltabellen in der CMDB und entfernt alte Klassenmodelldefinitionen, verwendet die Datei **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-class-model.xml**, um die Klassenmodelltabellen mit den aktualisierten Klassenmodelldaten aufzufüllen, und erstellt die neuen Datentabellen (CDM-Tabellen) mit aktualisierter Struktur.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Fehler führen dazu, dass das neue Klassenmodell nicht in die Datenbank geladen wird. Das Upgrade kann ohne das neue Klassenmodell nicht fortgesetzt werden.

Protokolldateien

Keine

Upgrade Resources on Disk

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Liest die ursprünglichen Abfragen, Ansichten, Reports, Enrichments und Korrelationen von der Festplatte, aktualisiert sie und speichert die aktualisierte Version auf der Festplatte. Wichtig: Ressourcen, die während des Upgrades entfernte Klassen verwenden, können nicht aktualisiert und in die aktualisierte UCMDB geladen werden. Ebenfalls entfernt werden Abfragen, die während des Upgrades entfernte Attribute als Eigenschaftsbedingung verwenden. Neben den Klassenmodelltransformationen für diese Ressourcen werden die folgenden Änderungen vorgenommen:

- Ansichten werden neu definiert, um der neuen Ansichtsdefinition zu entsprechen.
- Topologie-Reports werden als Ansichten neu definiert. In UCMDB 9.02 werden Reports und Ansichten als verschiedene Visualisierungsformen derselben Daten betrachtet.
- Abfragen werden in einem neuen, benutzerfreundlichen XML-Format gespeichert.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Fehler im gesamten Schritt führen dazu, dass das gesamte Upgrade fehlschlägt. In diesem Fall kann das Upgrade nach Behebung der Probleme ab diesem Schritt erneut ausgeführt werden.

Fehler beim Upgrade einzelner Ressourcen können behoben werden, indem dieser Schritt erneut ausgeführt wird oder nachdem das Upgrade beendet ist. Die fehlerhaften Ressourcen sollten manuell aktualisiert werden, um das Problem zu beheben, das den Upgrade-Fehler verursacht hat.

Protokolldateien

- Allgemeine Protokollmeldungen:

- Removing all the following resources: [<Liste der Ressourcennamen>] of type <Name> due to filter_resources.xml configuration file. Die Konfigurationsdatei **filter_resources.xml** enthält alle Namen und Typen der alten Ressourcen aus UCMDB 8.0x, die es in UCMDB 9.0x nicht gibt. Alle diese Ressourcen werden im Upgrade-Prozess entfernt. In dieser Protokollmeldung sind alle diese Ressourcen angegeben.

- Pattern-Upgrade:
  - About to upgrade pattern structure for the following patterns (<Pattern-Anzahl>) <Liste der Pattern-Namen>. Listet die Pattern-Namen auf, die aktualisiert werden.
  - About to check if pattern <Name> should be removed. Benachrichtigung vor der Überprüfung, ob das Pattern aktualisiert werden muss oder nicht. Wird das Pattern entfernt, werden Sie in der nächsten Meldung über diese Aktion informiert.
  - Pattern <Name> should be removed - has template instance group id. Alle Pattern in der Instanz der Gruppenvorlage werden durch das Upgrade entfernt.
  - About to remove unneeded pattern <Name>. Nicht aktualisierte Pattern wie das Pattern <Name> befinden sich im Pfad **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\patterns\unupgradeable\<Pattern-Name>.xml**. Das Pattern wurde nicht aktualisiert und befindet sich daher nach dem Upgrade nicht unter den Ressourcen.
  - About to check if pattern <Name> should be upgraded. Benachrichtigung vor der Überprüfung, ob dieses Pattern aktualisiert werden muss. In den folgenden Meldungen sind die Gründe für das Aktualisieren eines Pattern angegeben.
  - Pattern <Name> _should_ be upgraded, about to upgrade. Das Pattern wird aktualisiert. In den folgenden Meldungen sind die Teile des Pattern angegeben, die aktualisiert werden.
  - About to write patterns to disk after structure upgrade (<Pattern-Anzahl>):{<Liste der Pattern-Namen>}. Diese Pattern befinden sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\patterns\structure**.

- About to upgrade pattern <Name>. Das Klassenmodell-Upgrade im Pattern wird gestartet.
- Pattern <Name> was upgraded. Das Pattern wurde aktualisiert und befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\patterns\classmodel**.
- Pattern <Name> did not need upgrade. Alle Klassenmodellentitäten im Pattern sind bereits mit 9.0 kompatibel. Das Pattern befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\patterns\classmodel**.
- Pattern <Name> is not valid after upgrade. Das Pattern wurde entfernt und nicht aktualisiert. Dies liegt wahrscheinlich daran, dass mindestens eine Klassenmodellentität nicht mehr im Klassenmodell vorkommt.
- Could not upgrade pattern <Name>. Suchen Sie in der folgenden Ausnahme nach der Problembeschreibung.

- Einzel-Pattern-Referenz:
  - About to upgrade single pattern reference <Name>. Die resultierenden Ressourcen befinden sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\singlepatternref\classmodel**.
- Enrichment-Upgrade:
  - About to upgrade enrichment <Name>. Das Enrichment erfordert kein Struktur-Upgrade, sodass direkt mit dem Upgrade des Klassenmodells begonnen wird.
  - Couldn't obtain pattern <Name> for enrichment definition <Name>. Das Pattern für das aktuelle Enrichment ist nicht vorhanden.
  - Enrichment <Name> was upgraded. Das Enrichment wurde aktualisiert und befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\enrichments\classmodel**.

- Enrichment <Name> did not need upgrade. Alle Klassenmodellentitäten im Enrichment sind bereits mit 9.0 kompatibel. Das Enrichment befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\enrichments\classmodel**.
- Enrichment <Name> is not valid after upgrade. Das Enrichment wurde entfernt und nicht aktualisiert. Dies liegt wahrscheinlich daran, dass mindestens eine Klassenmodellentität nicht mehr im Klassenmodell vorkommt.

- Korrelations-Upgrade:
  - About to upgrade correlation <Name>. Die Korrelation erfordert kein Struktur-Upgrade, sodass direkt mit dem Upgrade des Klassenmodells begonnen wird.
  - Correlation <Name> was upgraded. Die Korrelation wurde aktualisiert und befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\correlations\classmodel**.
- Gold Master-Report-Upgrade:
  - About to upgrade gold master definitions for class model changes. Gold Master erfordert kein Struktur-Upgrade, sodass direkt mit dem Upgrade des Klassenmodells begonnen wird.
  - Got <Anzahl> gold master definitions. Anzahl der Gold Master im System.
  - Gold master report <Name> was upgraded for class model changes. Der Report wurde aktualisiert und befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\goldmaster\classmodel**.
  - Gold master report <Name> was not changed. Alle Klassenmodellentitäten im Report sind bereits mit 9.0 kompatibel. Der Report befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\goldmaster\classmodel**.

- Ansichts-Upgrade:
  - About to upgrade view <Name> structure.
  - Could not upgrade template view [bac view name: [<Name>], mam name: [<Name>]] - <Grund>. Ein häufiger Grund lautet Pattern by name [<Name>] not found. Dies kann passieren, nachdem das Pattern während des Pattern-Upgrades entfernt wurde. Die Liste der entfernten Pattern finden Sie in der Protokollmeldung Removing all the following resources: [<Liste der Ressourcennamen>] of type <Name> due to filter_resources.xml configuration file.
  - View <Name> structure was upgraded by a previous depending view. Die Ansicht wurde zuvor aktualisiert. Es ist kein erneutes Upgrade erforderlich.
  - View <Name> structure was upgraded. Die Ansicht befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\cmdbview\classmodel** oder **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\bacviews\classmodel**, je nach Ansichtstyp.
  - Could not upgrade view <Name>. In der zugehörigen Ausnahme finden Sie die Ursache für den Fehler. Die Ansicht wird nicht aktualisiert und befindet sich in einem der folgenden Ordner: **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\cmdbview\unupgradeable** oder **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\bacviews\unupgradeable**, je nach Ansichtstyp.
  - About to upgrade view <Name>. Das Upgrade der Klassenmodellentitäten in der Ansicht wird gestartet.
  - Class model transformation for view <Name> finished. Die Ansicht befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\cmdbview\classmodel**.
  - Could not upgrade view <Name>. Die Ansichten befinden sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\cmdbview\unupgradeable**.

- About to copy unchanged BacViews. Die Ansichten befinden sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\bacviews\classmodel**.

- Report-Upgrade:
  - About to upgrade report <Name> structure.
  - Upgrading report <Name> with tql name <Name>.
  - Report pattern <Name> for report <Name> was not found. Das aktualisierte Pattern für den aktuellen Report wurde auf der Festplatte nicht gefunden. Wird das Pattern nicht in Version 9.0x verschoben (nach dem Upgrade oder im derzeitigen Zustand), befindet es sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\patterns\unupgradeable** und diese Meldung wird ausgegeben. Der Report befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\reports\structure**.
  - Report <Name> was upgraded to view <Name>. Das Upgrade für den Report wurde beendet. Der Report befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\cmdbview\structure**. Das Klassenmodell-Upgrade erfolgt durch das Ansichts-Upgrade.
  - Could not upgrade report structure <Name>. Suchen Sie in der Ausnahme nach der Ursache für den Fehler. Der Report befindet sich unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\<Kunden-ID>\reports\unupgradeable**.

Upgrade Data

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Führt SQL-Anweisungen aus der Datei **C:\hp\UCMDB\UCMDBServer\runtime\data-upgrade-script.sql** aus, liest Daten aus den alten Datentabellen und den **TEMP**-Tabellen, führt die erforderliche Transformation durch und füllt die neuen Datentabellen (CDM-Tabellen) mit den aktualisierten Daten auf.

Hinweis: In diesem Schritt verdoppelt sich der Platzbedarf der CMDB. Nach beendetem Upgrade wird dieser Platz wieder freigegeben.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Daten in der Datenbank werden nicht aktualisiert.

Protokolldateien

Keine.

Create Temporary Removed CIs Table

Erstellt in der CDMB-Datenbank eine neue temporäre Tabelle mit dem Namen **UPGRADE_REMOVED_ELEMENTS**. Diese enthält die IDs und Typen aller Objekte, die während des Upgrades entfernt wurden (d. h. nicht aus den alten in die neuen Datentabellen kopiert wurden), für die Verwendung in späteren Schritten.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Fehler führen dazu, dass die Schritte zum Upgrade der Tabelle mit Listenattributen und zum Verarbeiten inkonsistenter Daten nicht ausgeführt werden können.

Protokolldateien

Keine.

Populate Root Table

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die aktualisierten relevanten Attributwerte aus untergeordneten Datentabellen in die Stammtabelle (CDM ROOT).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Die Stammtabelle wird nicht aufgefüllt und in der UCMDB sind keine CIs vorhanden. Fehler führen zum selben Ergebnis wie das Löschen aller Daten aus der UCMBD. Zur Wiederherstellung müssen Sie die Upgrade-Prozedur von Beginn an neu starten.

Protokolldateien

Keine.

Upgrade List Attribute Table

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Aktualisiert die Attribute vom Typ "Liste", die in einer separaten Tabelle gespeichert sind.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Alle Attribute vom Typ **Liste** weisen falsche Werte auf.

Protokolldateien

Keine.

Delete Legacy Configuration Tables

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Entfernt Tabellen, die in der CMDB nicht mehr benötigt werden.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Die Tabellen, die gelöscht werden sollen, verbleiben im CMDB-Schema, beeinträchtigen jedoch nicht das normale Verhalten der UCMDB. Diese Tabellen können manuell entfernt werden.

Protokolldateien

Keine.

Upgrade History DB

Aktualisiert die History-Datenbank. Die History-Datenbank kann große Datenmengen enthalten. In diesem Schritt werden immer die zuletzt aktualisierten Daten vermerkt, damit das Upgrade nach Fehlern an dem Punkt fortgesetzt werden kann, an dem es angehalten wurde.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Dieser Schritt kann mehrmals erneut ausgeführt werden, wobei zur Fehlerbehebung bestimmte Wiederherstellungsdateien herangezogen werden, die sich im Ordner **C:\hp\UCMDB\UCMDBServer\runtime\upgrade** befinden. Jede Datei enthält den Status eines Unterschrittes. Alle Dateien zusammen enthalten den Status des gesamten History-Upgrades. Die Dateinamen lauten:

- **recovery_for_history_cleanup.txt**
- **recovery_for_history_class_remove_upgrader.txt**
- **recovery_for_history_attribute_remove_upgrader.txt**
- **recovery_for_history_attribute_rename_upgrader.txt**
- **recovery_for_history_class_rename_upgrader.txt**
- **recovery_for_history_snapshot_upgrader.txt**

Wird dieser Schritt ausgelassen, gehen Historiendaten verloren und über den Konfigurationsassistenten muss ein neues Historienschema erstellt werden.

Protokolldateien

- Allgemeine Protokollmeldungen:
  - History DB upgrader failed, but is not failing upgrade process… Es ist ein Fehler aufgetreten.
  - INFO - <Schrittname> is upgrading chunk <aktuelle Chunk-Nummer> out of <Gesamtzahl der Chunks>. Meldung mit Fortschrittsbericht.
  - No upgrade is needed. Upgrade was finished in the previous upgrade. Die History-Datenbank wurde nicht zum ersten Mal ausgeführt. Beim vorherigen Mal wurde das Upgrade erfolgreich abgeschlossen.
  - <Schrittname> is upgrading chunk <Nummer> out of <Anzahl>. Gibt den Fortschritt für jeden Upgrade-Schritt an.
  - Executing SQL statement on attributes between event id <Nummer> and <Nummer>. Statement: <SQL-Anweisung>. Attribute eines bestimmten Typs werden aktualisiert oder entfernt (wie in der SQL-Anweisung angegeben).

- old Class <Name> has history attributes of types <Liste der Namen>. Für jede Klasse, die entfernt oder aktualisiert werden muss, werden alle zu verarbeitenden Attributtypen aufgelistet.

- Create auxiliary tables for History DB upgrade. In diesem Schritt vor dem Upgrade werden relevante Daten zusammengestellt:
  - The history DB has <Anzahl> events. Informationsmeldung mit der Anzahl an Historienereignissen, die sich derzeit in der History-Datenbank befinden.
  - The Chunk between rows <Nummer> and <Nummer>, translate to events IDs between <Nummer> and <Nummer>. Jeder Chunk bezieht sich auf eine Reihe von Zeilen in der History-Datenbank; dies wird in eine SQL-Anweisung für eine Reihe von Historienereignis-IDs umgesetzt.
- Collect non-history data from the history DB. Für die History-Datenbank werden Bereinigungsvorgänge durchgeführt, um nicht vorhandene oder nicht historienbezogene Klassenmodellelemente zu entfernen. In diesem Schritt werden die relevanten Daten für die spätere Verarbeitung zusammengestellt.
  - Recover cleanup data from file <Name>. Das Upgrade wurde bereits zuvor ausgeführt. Die relevanten Daten für die Bereinigung des Schemas wurden zuvor erfasst und sind in der Datei verfügbar.
  - Collect data from table for type <Name>. Bereinigungsdaten werden für jeden Attributtyp separat zusammengestellt.
  - Class <Name>, attribute <Name> is monitored in history DB. Listet alle Attribute für jede Klasse im Klassenmodell auf, die einen Eintrag in der History-Datenbank aufweist.
  - Summary of all collect data from History DB. In den folgenden Protokollmeldungen sind die erfassten Daten nach Klassenname gruppiert.
  - Class <Name>, attributes [<Liste der Namen>] are monitored in history DB. Listet erneut alle Attribute für alle Klassen auf, die Einträge in der History-Datenbank aufweisen, gruppiert nach Klassenname.

- Cleanup problems found in the history DB. In den folgenden Protokollmeldungen sind alle Daten angegeben, die aus der History-Datenbank entfernt werden müssen, weil sie nicht mit dem Klassenmodell konsistent sind.
  - Class <Name> exists in history DB but not in class model. Die Klasse wird aus der History-Datenbank entfernt.
  - Link Class <Name> is not marked as monitored for change. Die Klasse wird aus der History-Datenbank entfernt. (Bei Link-Klassen muss der Qualifizierer TRACK_LINK_CHANGES überwacht werden.)
  - Attribute <Name> in Class <Name> exists in history DB but not in class model. Das Attribut wird aus der History-Datenbank entfernt.
  - Attribute <Name> in Class <Name> exists in history DB but not marked as monitored for change. Das Attribut wird aus der History-Datenbank entfernt.
  - Class <Name> has no attributes marked as monitored for change. Die Klasse wird aus der History-Datenbank entfernt.
- Get colliding rules. Falls im Rahmen der Änderungen im Klassenmodell eine Zusammenführung von Attributen erforderlich ist, müssen diese Attribute bestimmt und verarbeitet werden.
  - Skipped - Attribute name: <Name> Class name: <Name> was not found in old ClassModel. Protokollmeldung ohne Bedeutung.
  - Classes <Liste der Namen> have history qualifiers. Diese Klassen verfügen über Attribute, die sich potenziell zusammenführen lassen. Dies wird in der nächsten Phase überprüft.
  - Classes <Liste der Name> has renamed attributes with CopyAttributeFromAttribute. Diese Klassen weisen Attribute auf, die als Datenquelle für die zusammengeführten Attribute dienten.
  - Add remove data to configuration for merge rules:

    Attribute <Name> in Class <Name> has colliding renaming rules. Diesem Attribut wurden mindestens zwei Attribute im alten Klassenmodell zugeordnet.

    Attribute <Name> in Class <Name> will receive its value from <alter Attributname>. Die Datenquelle des Attributs wird bestimmt.

Attribute <Name> in Class <Name> has more than one rename (including alias) without copyAttributeFromAttribute rule. Alle zusammengeführten Attribute sind nicht als Datenquelle für das neue Attribut definiert. Ein beliebiges altes Attribut wird als Datenquelle ausgewählt.

In class <Name> the following attributes will be removed because of merging: <Liste der alten Attributnamen>. Zusammenfassung aller Attribute pro Klasse, die durch das Zusammenführen entfernt werden.

- Removes history events that contain removed class model classes. In diesem Schritt werden alle Klassen ermittelt, die aus der History-Datenbank entfernt werden müssen.
  - Class remove rule: oldClassName (object) = <Name>
  - Class remove rule: oldClassName (link) = <Name>
  - Class remove rule: oldClassName (cleanup) = <Name>. Die Regel wurde in der Bereinigungsphase erstellt.
  - Executing SQL statement for remove class between event id <Nummer> and <Nummer>. Statement: <SQL-Anweisung>. Das Entfernen der Klassen im aktuellen Chunk wird durchgeführt.
- Removes history events that contain removed class model attributes. In diesem Schritt werden alle Attribute ermittelt, die aus der History-Datenbank entfernt werden müssen.
  - Attribute remove rule: oldClassName = <Name>, oldAttributeName <Name>, attribute type = <Name>
  - Attribute remove rule (cleanup): oldClassName = <Name>, oldAttributeName <Name>, attribute type = <Name> Die Regel wurde in der Bereinigungsphase erstellt.
- Upgrades records that contain renamed class model attributes. In diesem Schritt werden alle Attribute ermittelt, die in der History-Datenbank umbenannt werden müssen.
  - Attribute rename rule: oldClassName = <Name>, oldAttributeName <Name>, new attribute name = <Name>, attribute type = <Name>

- Upgrades records that contain renamed class model attributes. In diesem Schritt werden alle Klassen ermittelt, die in der History-Datenbank umbenannt werden müssen.
  - Class rename rule: oldClassName (object) = <Name> new class name = <Name>
  - Class rename rule: oldClassName (object) = <Name> new class name = <Name>
  - Executing SQL statement for rename class between event id <Nummer> and <Nummer>. Statement: <SQL-Anweisung>
- Upgrades records that contain snapshot result. In diesem Schritt werden alle Baselines ermittelt, die in der History-Datenbank aktualisiert werden müssen.
  - Executing SQL statement on snapshots between event id <Nummer>
  - ExecuteBatch for snapshot is done in seconds

Handle Non-Consistent Data

Führt Folgendes aus:

- Entfernt Links, bei denen während des Upgrades ein Endobjekt entfernt wurde.
- Führt bei Bedarf ein rekursives Löschen durch.
- Berechnet für alle Objekte und Links den Wert der Attribute neu, die als berechnete Attribute definiert wurden.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Die Daten sind inkonsistent; dies kann sich auf die Werte von berechneten Attributen auswirken. Durch das Ausführen des Datenbankkonsistenz-Tools nach beendetem Upgrade werden Links nur entfernt, wenn eines ihrer Endobjekte fehlt.

Protokolldateien

Die folgenden Protokollmeldungen werden im kurzen Upgrade-Protokoll angezeigt:

- Found x objects/links that were removed during upgrade. Die Anzahl an Objekten und Links, die während des Upgrades entfernt wurden.
- Found x dangling links. Die Anzahl an Links ohne Endobjekt, die entfernt werden.
- Found x recursive-delete objects. Die Anzahl an Objekten, die aufgrund von rekursivem Löschen entfernt werden.
- Updating calculated attributes for type CLASS_NAME (x instances, y bulks). Für jede Zeile der einzelnen Objekt-/Linktypen wird die Attribut-Neuberechnung ausgeführt.

Recalculate Non-Random Generated IDs

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Berechnet die IDs aller Objekte neu, deren IDs nicht zufällig zugewiesen, sondern abhängig vom Objekttyp und von den Schlüsseleigenschaften berechnet werden.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Protokolldateien

Keine

Populate Global ID

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Im eigenständigen Modus funktioniert UCMDB als CMS und erfordert für jedes CI eine globale ID. In diesem Schritt wird die Spalte mit der globalen ID in der Stammdatentabelle aufgefüllt.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Möglicherweise erhalten die CIs keine globale ID. Dies kann bei Integrationen oder komplexen Bereitstellungen von UCMDB sehr problematisch werden.

Problemumgehung. Mit den Services für mehrere CMDB-Instanzen kann dieses Problem nach dem Upgrade behoben werden:

- Wird ein Server als Generator für globale IDs benötigt, müssen Sie ihn zunächst zu einem Generator für nicht globale IDs machen und anschließend zu einem Generator für globale IDs.
- Wird ein Server als Generator für nicht globale IDs benötigt, müssen Sie ihn zunächst zu einem Generator für globale IDs machen und anschließend zu einem Generator für nicht globale IDs.

Protokolldateien

Keine.

Discovery – Upgrade Configuration

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Berechnet die IDs der DFM-Konfigurations-CIs neu.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	N

Fehlerauswirkungen

Discovery funktioniert möglicherweise nicht. Wenn Sie diesen Schritt auslassen, müssen Sie Folgendes durchführen:

1. Deaktivieren Sie die drei Upgrade-Programme.
2. Exportieren Sie die Benutzer-Packages aus der vorherigen CMDB.
3. Aktualisieren Sie alle Packages manuell durch das Migrations-Tool für Packages. Weitere Informationen finden Sie unter "Upgrade für Packages von Version 8.04 auf 9.02" auf Seite 267.
4. Entfernen Sie vor dem Upgrade-Prozess die folgenden Instanzen von Discovery-Konfigurations-CIs aus der CMDB:
   - domain
   - discoveryjob
   - discoverymodule
   - cmdbclass
   - discoverypattern
   - discoverywizard
   - discoveryprobegateway
   - discoveryprobemanager
   - discoveryresource
   - discoverytql
   - triggers
   - management
5. Importieren Sie nach dem Upgrade-Prozess die aktualisierten Packages.

Protokolldateien

- Starting upgrade Discovery Configuration CIs.
- Upgrade Discovery Configuration CIs was successfully finished!
- Failed to upgrade some Discovery Configuration CIs.
- About to get discovery configuration CIs and links from server.
- Finish getting discovery configuration CIs and links from server. Instanzen von Discovery-Konfigurations-CIs werden aus der CMDB geladen.
- About to remove old Discovery Configuration CIs.
- Finish removing old Discovery Configuration CIs. Alte CIs werden aus der CMDB entfernt. CIs sind nun ausschließlich im Cache vorhanden. Fehler in diesem Schritt können zu einem Datenverlust führen.
- About to update discovery configuration CIs.
- Finish updating [Anzahl an CIs] discovery configuration CIs. Die CIs werden aktualisiert und in der CMDB gespeichert.
- Failed to add CI [neue CI-ID, CI-Typ], (old CI [alte CI-ID]) skipped. Ein bestimmtes CI im Schema konnte nicht aktualisiert werden. Weitere Informationen finden Sie im Fehlerprotokoll.
- About to update links related to discovery configuration CIs.
- Finish updating links related to discovery configuration CIs. Die Links zwischen CIs werden wiederhergestellt. Fehler in diesem Schritt können zu Dateninkonsistenz führen.

Federation – Remove old Configuration

Entfernt die alten Konfigurationsdaten der Föderation (die neue Konfiguration wird bereitgestellt).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Möglicherweise funktioniert die Föderation oder Replizierung nicht.

Problemumgehung. Verwenden Sie den JMX-Vorgang **deleteByClassType** (in den Modellservices), um alle Instanzen des CIT **fcmdb_configuration** zu entfernen. Informationen zum Arbeiten mit der JMX-Konsole finden Sie unter .

Protokolldateien

Protokollmeldungen finden Sie in den Protokolldateien **cmdb.model.audit.short.log** und **cmdb.model.audit.detailed.appender**.

Redeploy Basic Packages

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Stellt die CMDB-Werk-Packages bereit. Klassenmodellaktualisierungen sind in diesem Schritt auf Hinzufügungen beschränkt, damit die Werk-Packages keine vom Benutzer hinzugefügten Attribute entfernen.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Nach Fehlern können diese Packages aus der UCMDB selbst erneut bereitgestellt werden. Alle Hinzufügungen des Benutzers zu diesen Klassen können jedoch bei der erneuten Bereitstellung verloren gehen.

Protokolldateien

Protokollmeldungen finden Sie in der Protokolldatei **mam.packaging.log**.

Validate Upgraded Class Model

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Prüft die BDM- und CMS-Kompatibilität des aktualisierten Klassenmodells, indem es mit einem 9.02-Klassenmodell verglichen wird. Fehlende Klassenmodellentitäten werden hinzugefügt.

Das Klassenmodell, das vor diesem Schritt in der Datenbank vorhanden ist (Upgrade + Packages), wird in der Datei **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-after-packages-class-model.xml** gespeichert. Das aktualisierte Klassenmodell wird unter **C:\hp\UCMDB\UCMDBServer\runtime\upgraded-fixed-after-packages-class-model.xml** gespeichert.

Wird das Klassenmodell in diesem Schritt geändert, wird es wieder in der Datenbank aktualisiert.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Durch Fehler in dieser Phase schlägt nicht der gesamte Upgrade-Prozess fehl. Die Fehler müssen jedoch ernst genommen werden, da sie bedeuten, dass das Benutzerklassenmodell unvollständig und nicht CMS- und Business Service Management-kompatibel ist.

Protokolldateien

Weitere Informationen finden Sie unter "Validate Class Model" auf Seite 199.

Discovery – Upgrade Statistics

Benennt die CI-Typen in der Tabelle **CCM_DISCOVERY_STATS** in der CMDB um (Discovery-Historiendaten).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Statistikdaten aus vorherigen Discovery-Ausführungen gehen verloren. Wird dieser Schritt ausgelassen, muss der Benutzer die Tabelle **CCM_DISCOVERY_STATS** in der CMDB kürzen.

Protokolldateien

- Starting upgrade CCM_DISCOVERY_STATS table.
- Upgrade 'CCM_DISCOVERY_STATS' table was successfully finished!
- Failed to upgrade 'CCM_DISCOVERY_STATS' table.
- Ci type [alter CI-Typ] has been upgraded to [neuer CI-Typ]. Gibt an, dass ein alter CI-Typ in einen neuen CI-Typ umbenannt wurde.
- Failed to update [alter CI-Typ], skipped. Zeigt an, dass ein CI-Typ nicht im Einklang mit dem neuen Schema geändert werden konnte. Ursache kann eine Dateninkonsistenz in der CMDB sein oder der Benutzer hat einen falschen CI-Typ definiert. Dies wirkt sich nicht auf die Discovery aus, doch die Zeile für dieses CI wird im Statistik-Panel rot angezeigt.

Discovery – Upgrade Resources

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Aktualisiert die Discovery-Ressourcen: Pattern, Jobs und Module (Discovery-Konfigurationsdaten).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Dieselben wie beim Schritt "Discovery – Upgrade Configuration" auf Seite 247.

Protokolldateien

- Starting upgrade discovery resources.
- Upgrade discovery resources have been successfully finished!
- Upgrade discovery resources have been finished. Failed to upgrade the following resources: [Ressourcenname 1], [Ressourcenname 2], …

- File containing resources to filter, upgrade/filtered_resources.xml, not found. Die Datei mit der Liste der Ressourcen, die während des Upgrades entfernt werden sollen, wurde nicht gefunden, sodass keine Ressourcen entfernt werden.
- Resource [Ressourcenname] of type [Untersystem] was successfully updated. Gibt an, dass die Ressource erfolgreich aktualisiert wurde.
- Failed to upgrade res [Ressourcenname] of type [Untersystem]/ The resource might be already compatible with new schema. Please check resource manually. Die Ressource wurde nicht aktualisiert. Prüfen Sie die Ressource manuell nach dem Starten der CMDB. In den meisten Fällen gibt es für solche Fehler eine weitere Protokollmeldung mit ausführlicheren Informationen.

Load Upgraded Resources

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Lädt die aktualisierten Ressourcen, die im vorherigen Schritt "Discovery – Upgrade Resources" auf Seite 252 erstellt wurden, von der Festplatte in die Datenbank.

Hinweis: Aktualisierte Ressourcen aus den Werk-Packages haben Vorrang vor Benutzerressourcen. Dies bedeutet, falls dieselbe Ressource (Name und Typ) sowohl in den Werk-Packages als auch im aktualisierten Ressourcenordner vorhanden ist, wird die Version aus den Werk-Packages verwendet.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Die aktualisierten Ressourcen werden nicht in die Datenbank geladen. Die Werk-Ressourcen sind durch den Schritt "Redeploy Basic Packages" auf Seite 250 bereits in der Datenbank. Nur die Benutzerressourcen fehlen in der Datenbank.

Protokolldateien

- Got <Anzahl> <Typ> from disk. Gibt die Anzahl an Ressourcen an, die für jeden Typ von der Festplatte abgerufen wurden. Dieser Meldung folgt eine Liste mit diesen Ressourcen.
- Could not get resources map - all resources will be deployed from disk. Die Werk-Packages, die für die Datenbank bereitgestellt wurden, können nicht abgerufen werden. Die Werk-Ressourcen können keinen Vorrang vor den Benutzerressourcen erhalten, sodass alle Benutzerressourcen in die Datenbank geladen und die Werk-Ressourcen mit demselben Namen und Typ überschrieben werden.
- Did not succeed to add business view enrichment <Name>. Die Problembeschreibung finden Sie in der zugehörigen Ausnahme.
- Did not succeed to add gold master definition <Name>. Die Problembeschreibung finden Sie in der zugehörigen Ausnahme.
- Resource <Name> does not exist in CMDB and should be added. Die Ressource ist eine Benutzerressource und wird in die Datenbank geladen.
- Resource <Name> could not be loaded because of missing dependencies: <Liste der Namen>. Die Ressource kann nicht in die Datenbank geladen werden, weil dafür benötigte andere Ressourcen nicht in der Datenbank vorhanden sind. Nach Abschluss des Upgrades kann dieser Schritt erneut ausgeführt werden, um diese Ressourcen zu laden.
- Upgraded resource <Name> and out-of-the-box resource are the same, not loading upgraded resource. Die Werk-Ressource wurde nicht vom Benutzer geändert.
- Upgraded resource <Name> is not loaded since a different out-of-the-box resource with the same type and name already exists. Der Benutzer hat die Werk-Ressource geändert und verliert die von ihm vorgenommenen Änderungen.

➤ Failed to add <Typ> <Name>. Die Ressource des angegebenen Typs wurde nicht geladen.

Upgrade Snapshots

Speichert die aktualisierten Baseline-Daten in der CMDB.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Protokolldateien

Keine.

Discovery – Re-Encrypt Domain Scope Document

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Sorgt für eine Neuverschlüsselung der Datei **domainScopeDocument** von der DES-Verschlüsselung (die in 8.0x verwendet wird) in die AES-Verschlüsselung.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Discovery funktioniert möglicherweise nicht. Wird dieser Schritt ausgelassen, müssen Sie Folgendes durchführen:

1. Exportieren Sie die Datei **domainScopeDocument** aus der alten CMDB.
2. Importieren Sie nach dem Upgrade-Prozess die Datei **domainScopeDocument**. Weitere Informationen finden Sie unter "Exportieren und Importieren von Anmelde- und Bereichsinformationen im verschlüsselten Format" auf Seite 346.

Protokolldateien

- Upgrade process of DomainScopeDocument re-encryption to AES had been started.
- Upgrade process of DomainScopeDocument re-encryption to AES had been finished successfully.
- Upgrade process of DomainScopeDocument re-encryption to AES had been failed.
- DSD is empty - doing nothing... Zeigt an, dass die Datei **domainScopeDocument** leer ist und dieser Schritt daher redundant ist und nichts bewirkt.
- The DSD already encrypted by AES - doing nothing… Zeigt an, dass die Datei **domainScopeDocument** bereits AES-Verschlüsselung aufweist, sodass der Schritt redundant ist und nichts bewirkt.
- The DSD is encrypted by 3DES... Gibt an, dass die Datei **domainScopeDocument** eine 3DES-Verschlüsselung aufweist und daher eine AES-Neuverschlüsselung durchgeführt wird.
- Failed to decrypt DSD by 3DES. Weist darauf hin, dass der Verschlüsselungsprozess für die Datei **domainScopeDocument** fehlgeschlagen ist (die AES-Neuverschlüsselung der Datei **domainScopeDocument** konnte in diesem Schritt nicht durchgeführt werden). Sie müssen die Datei **domainScopeDocument** nach dem Upgrade-Prozess in das UCMDB-System importieren.
- Failed to encrypt DSD by AES. Der Schritt ist fehlgeschlagen. Sie müssen die Datei **domainScopeDocument** nach dem Upgrade-Prozess in das UCMDB-System importieren.
- Got empty DSD after AES encryption. Der Schritt ist fehlgeschlagen. Sie müssen die Datei **domainScopeDocument** nach dem Upgrade-Prozess in das UCMDB-System importieren.
- Got empty DSD after 3DES decryption. Der Schritt ist fehlgeschlagen. Sie müssen die Datei **domainScopeDocument** nach dem Upgrade-Prozess in das UCMDB-System importieren.
- Failed to decrypt the DSD by AES and 3DES. Der Schritt ist fehlgeschlagen. Sie müssen die Datei **domainScopeDocument** nach dem Upgrade-Prozess in das UCMDB-System importieren.

Discovery – Upgrade Domain Scope Document

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Benennt die CI-Typen und Attribute in der Datei **domainScopeDocument** um.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Siehe "Discovery – Re-Encrypt Domain Scope Document" auf Seite 255.

Protokolldateien

- Upgrade process of DomainScopeDocument data has been started
- DomainScopeDocument data has been successfully upgraded
- Failed to upgrade DomainScopeDocument data

Discovery – Copy Credentials to Confidential Manager

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Extrahiert Anmeldeinformationen aus der Datei **domainScopeDocument** in den Confidential Manager. Anmeldeinformationen in der Datei **domainScopeDocument** werden durch Confidential Manager-IDs ersetzt. Weitere Informationen finden Sie unter "Confidential Manager" auf Seite 407.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Dieselben wie beim Schritt "Discovery – Re-Encrypt Domain Scope Document" auf Seite 255.

Protokolldateien

- Upgrade process of DomainScopeDocument insertion to Confidential Manager had been started
- Upgrade process of DomainScopeDocument insertion to Confidential Manager had been finished successfully
- Upgrade process of DomainScopeDocument insertion to Confidential Manager had been failed

Discovery – Upgrade Credential Identifiers

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Aktualisiert das Attribut **credential_id** für die CIs in der CMDB so, dass sie den Confidential Manager-IDs entsprechen.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Das Attribut der Anmeldeinformationen für vorhandene CIs enthält falsche Daten. Wird dieser Schritt ausgelassen, müssen Sie eine umfassende Discovery ausführen, um die Daten wiederherzustellen.

Protokolldateien

- Upgrade process of credentials_id's update had been started.
- Upgrade process of credentials_id's update had been finished successfully.
- Upgrade process of credentials_id's update had been failed.

➤ Failed to get layout (and update credentials id) for object of type <Typ>. Gibt an, dass der Upgrade-Prozess für den angegebenen Typ fehlgeschlagen ist. Dies bedeutet, dass die CIs des angegebenen Typs möglicherweise veraltete IDs für Anmeldeinformationen enthalten. Nach Abschluss des Upgrade-Prozesses müssen Sie eine umfassende erneute Discovery für das System ausführen.

Copy Report Configuration

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die Report-Konfiguration aus der Foundations-Datenbank in die neue Verwaltungsdatenbank.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Favoritenfilter aus 8.0x werden nicht aktualisiert und ihr Zeitplan ist nicht verfügbar.

Protokolldateien

➤ Failed to upgrade report: <Report-Name>.

Copy Snapshots Scheduling Information

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Kopiert die Zeitplandaten für Baselines aus der Foundations-Datenbank in die neuen Verwaltungstabellen der CMDB. Entfernt außerdem geplante Jobs mit Typen, die nicht mehr relevant sind (TQL ausführen, Ansichten erneut erstellen und Packages bereitstellen).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Geplante Baselines werden nicht aktualisiert und Sie müssen sie erneut definieren.

Protokolldateien

➤ Failed to handle schedulerJob [<schedulerJob.toString()>].

Upgrade Settings

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Benennt die CI-Typen in ausgewählten Einstellungen um.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Wenn Klassen im Settings Manager vorhanden waren, deren Name durch das Klassenmodell-Upgrade geändert wurde, tritt je nach Einstellung möglicherweise ein seltsames Applikationsverhalten auf.

Beispiel: Der Stamm-CIT und seine Beziehung wurden definiert. Eine zusätzliche Einstellung ist der Frontend-URL. Wenn ein Load Balancer definiert ist, müssen Sie möglicherweise den Frontend-URL neu definieren. Die Reverse-Proxy-Einstellungen sind nicht betroffen.

Protokolldateien

➤ SettingsClassModelUpgrader failed oder das Upgrade für eine bestimmte Einstellung mit dem Präfix ist fehlgeschlagen.

Upgrade Security Model

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Aktualisiert die Berechtigungen im Einklang mit dem neuen ACL-Modell.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Manche Berechtigungen sind mit dem neuen ACL-Modell abgestimmt, andere jedoch nicht. Administratoren müssen den Security Manager aufrufen und sicherstellen, dass alle erforderlichen Berechtigungen vorhanden sind bzw. die Berechtigungen bei Bedarf einrichten.

Protokolldateien

➤ Role [<Rollenname>] failed to get permissions due to the following error:…

Clear Old Data

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Entfernt die alten Datentabellen (TEMP-Tabellen).

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Die UCMDB funktioniert ordnungsgemäß, könnte aber durch unnötig in den Tabellen verbliebene Daten gebremst werden. Sie können alle Tabellen mit dem Präfix **TEMP** manuell entfernen.

Protokolldateien

Keine.

User vs. Factory

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Vergleicht das aktualisierte Klassenmodell mit einem Standardklassenmodell, um für jede Klassenmodellentität zu entscheiden, ob es sich um eine Benutzer- oder Werk-Entität handelt.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Alle Klassenmodellentitäten sind als Werk-Entitäten markiert. Bestimmte Vorgänge im Klassenmodell sind für Benutzer-Entitäten, die Vorrang vor Werk-Entitäten haben, nicht möglich.

Protokolldateien

Die folgenden Meldungen weisen auf Probleme im Datenmodell hin. Die in der Meldung angegebene Entität ist eine Werk-Entität, die im Benutzerklassenmodell fehlt. Dies kann auf ein vorheriges Problem bei der Bereitstellung von Content Pack 6.00 oder im Upgrade-Prozess hinweisen.

Einer oder mehrere der folgenden Schritte können betroffen sein:

- "Validate Class Model" auf Seite 199.
- "Upgrade Class Model on Disk" auf Seite 205.

- "Upgrade Class Model in DB" auf Seite 231.
- "Redeploy Basic Packages" auf Seite 250.
- "Validate Upgraded Class Model" auf Seite 250.

- !!! Class <Name> doesn't exist in the upgraded class model.
- !!! Class <Name> is missing qualifiers in the upgraded class model. The qualifiers are: <Liste der Namen>.
- !!! Attribute <Name> in Class <Name> is missing from the upgraded class model.
- !!! Attribute <Name> in Class <Name> is missing qualifiers in the upgraded class model. The qualifiers are: <Liste der Namen>.
- !!! Attribute Override <Name> was removed in Class <Name> and is missing qualifiers in the upgraded class model. The qualifiers are: <Liste der Namen>.
- !!! Attribute Override <Name> in Class <Name> is missing qualifiers in the upgraded class model. The qualifiers are: <Liste der Namen>.
- !!! Class <Name> is missing method <Name> in the upgraded class model.
- !!! Method <Name> in Class <Name> is missing qualifiers in the upgraded class model. The qualifiers are: <Liste der Namen>.
- !!! Valid Link <Name> is missing in the upgraded class model.
- !!! Valid Link <Name> is missing qualifiers in the upgraded class model. The qualifiers are <Liste der Namen>.
- !!! Calculated Link <Name> with Class <Name> is missing in the upgraded class model.
- !!! Calculated Link <Name> with Class <Name> is missing triplet in the upgraded class model. The triplet is <Dreiergruppe>.
- !!! Enum <Name> doesn't exist in the upgraded class model.
- !!! List <Name> doesn't exist in the upgraded class model.
- !!! Enum entry with key <Nummer> and value <Wert> in Enum <Name> doesn't exist in the upgraded class model.
- !!! List entry <Wert> in List <Name> doesn't exist in the upgraded class model.

Populate IPv6 Attribute

Kopiert den IP-Wert aus dem Name-Attribut in das neue IP-Adresswert-Attribut der IP-Adresse-Klasse, das der IPv6-normalisierten Form entspricht.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
J	J

Fehlerauswirkungen

Discovery funktioniert möglicherweise nicht.

Problemumgehung. Sie sollten die IPs und das IP-Subnet in der CMDB aktualisieren. Die Aktualisierung kann manuell über die Benutzeroberfläche vorgenommen werden (eine nach der anderen).

Protokolldateien

Protokollmeldungen finden Sie in der Protokolldatei **cmdb.reconciliation.log**.

Enrichment Driven Upgrade

Ruft vordefinierte Enrichments auf, um Daten im Rahmen des Upgrade-Prozesses zu aktualisieren.

1. Aktualisierung des Name-Attributs für die J2EE-Domäne, um das Suffix zu entfernen (alle Zeichen nach "@").

2. Aktualisierung des Name-Attributs für die Cluster-Ressourcengruppe, um das Suffix aus dem Wert ihres Host-Schlüsselattributs anzugeben (alle Zeichen nach ":").

3. Entfernen alter Report-Archiv-CIs, die nicht aktualisiert werden.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Define Key Attributes Reconciliation Rules

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Fügt eine Abstimmungsregel vom Typ "Schlüsselattribute" zu allen benutzerdefinierten CI-Typen mit Schlüsselattributen hinzu.

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Ein benutzerdefinierter CIT, der in 8.00 durch Schlüsselattribute identifiziert wurde, verwendet die übergeordnete Abstimmungsregel.

Die Regel für die Identifikation durch Schlüsselattribute kann später aus einer Package-/Abstimmungs-JMX hinzugefügt werden.

Protokolldateien

Keine.

Package Manager Upgrade

Hinweis: Upgrade vom Typ "Nur Ressourcen".

Aktualisiert die im UCMDB Server-Modell gespeicherten Package-Informationen.

Die Konfigurationsdatei für das Package Manager-Upgrade ist unter **C:\hp\UCMDB\UCMDBServer\runtime\upgrade\PackageManagerUpgrader\config.xml** (**cmdb.jar**) gespeichert. In der Konfiguration sind die veralteten Untersysteme und die Umbenennungsregeln für Untersysteme aufgelistet.

Das Upgrade-Tool für den Package Manager führt die folgenden Schritte aus:

1. Entfernt die Ressourcen von veralteten Untersystemen aus den Packages
2. Benennt alte Untersystemnamen in die neuen um
3. Aktualisiert den Namen der vom Package Manager verwendeten Klassenmodellressourcen
   - **a** Ändert Klassennamen in Klassendefinitionen
   - **b** Ändert Klassennamen in den Definitionen gültiger Links
   - **c** Ändert Klassennamen in den Dreiergruppen von Definitionen berechneter Links
4. Entfernt nicht vorhandene Ressourcen aus Packages

Ist kritisch (J/N)	Kann erneut ausgeführt werden (J/N)
N	J

Fehlerauswirkungen

Falsche Package-Informationen können zum Erstellen falscher Package-Dateien während des Package-Exports führen. Außerdem können sie Fehler verursachen, wenn versucht wird, die Bereitstellung eines Packages aufzuheben.

Protokolldateien

Keine.

15

Upgrade für Packages von Version 8.04 auf 9.02

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

Dienstprogramm für die Package-Migration – Übersicht

In diesem Kapitel wird erklärt, wie Sie das Dienstprogramm für die Package-Migration verwenden, um benutzerdefinierte Packages in HP Universal CMDB (UCMDB) von Version 8.04 auf Version 9.02 zu migrieren.

Benutzerdefinierte Packages, die vor dem Upgrade des Systems auf Version 9.02 erstellt wurden, enthalten möglicherweise Ressourcen, die in der neuen Version nicht unterstützt werden. Um das Risiko von Problemen in diesen benutzerdefinierten Packages zu senken, sollten Sie die Packages offline mit dem mitgelieferten Dienstprogramm für die Package-Migration migrieren, bevor Sie die Packages im UCMDB-System der Version 9.02 bereitstellen.

Die Offline-Migration benutzerdefinierter Packages mit dem Dienstprogramm für die Package-Migration bietet folgende Vorteile:

- Es ist keine Ausfallzeit erforderlich.
- Die Migration benutzerdefinierter Packages kann vor der Bereitstellung der Packages im System abgeschlossen werden, um Risiken zu senken.
- Sie können Ihre Packages migrieren, sofort bereitstellen und die Daten neu erkennen.
- HP Content Packages können in einem einzigen Prozess migriert werden, um das Risiko beschädigter Daten zu senken.

Mit dem Dienstprogramm für die Package-Migration können Sie benutzerdefinierte Packages offline migrieren, ohne einen Server ausführen zu müssen.

Aufgaben

Migrieren benutzerdefinierter Packages

In der folgenden Prozedur wird erklärt, wie Sie benutzerdefinierte Packages auf HP Universal CMDB Version 9.02 migrieren.

So migrieren Sie benutzerdefinierte Packages:

1. Speichern Sie die benutzerdefinierten Packages, die migriert werden sollen, in einem separaten Verzeichnis zusammen mit den Packages, von denen die aktualisierten Ressourcen abhängen. Beispiel:
   - Wenn ein benutzerdefiniertes Package eine Ansichts- oder Enrichment-Regel enthält, die auf einer TQL-Definition in einem anderen Package beruht, speichern Sie das Package mit der TQL-Definition im selben Verzeichnis wie das benutzerdefinierte Package.
   - Wenn ein benutzerdefiniertes Package einen Verweis auf eine benutzerdefinierte Klasse enthält, die in keinem der Werk-Packages bereitgestellt wird, speichern Sie das Package mit der benutzerdefinierten Klasse im selben Verzeichnis wie das benutzerdefinierte Package.
2. Stellen Sie sicher, dass Sie über die XML-Dateien mit der alten Klassenmodelldefinition verfügen, d. h. mit dem Klassenmodell der UCMDB-Version (z. B. 7.0 oder 7.5), mit dem Ihr Package erstellt wurde.

   Zum Erstellen des Klassenmodells rufen Sie die JMX-Konsole auf, navigieren zu **UCMDB:service=Class Model Services** und führen die Methode **exportClassModelToXML** aus.
3. Führen Sie das Skript aus:
   - Windows: **C:\hp\UCMDB\UCMDBServer\tools\packupgrade.bat**
   - Solaris: **C:/hp/UCMDB/UCMDBServer/2f/packupgrade/bin/packupgrade.sh**

Im Folgenden ist die Syntax für die Skriptausführung dargestellt. (Diese Informationen können Sie auch anzeigen, indem Sie das Skript ohne Argumente ausführen.)

```
packupgrade -cm {CLASS_MODEL_DEF_FILE} [-u {UPGRADE_CONFIG_FILE}] [-
exclude <package(s)>] -out {OUTPUT_DIR} {INPUT_DIR}
```

-i. Anmelden an der JMX-Konsole.

-cm {CLASS_MODEL_DEF_FILE}. Dateiname der alten Klassenmodelldefinition; diese Datei kann über JMX erstellt werden: Navigieren Sie in der JMX-Konsole zu **Class Model Services** und rufen Sie die Methode **exportClassModelToXml** auf.

-u {UPGRADE_CONFIG_FILE}. Die Upgrade-Konfigurationsdatei.

-exclude {package(s)}. Das auszuschließende Package oder die Liste der auszuschließenden Package-Namen, durch Kommas getrennt.

-filterResources {file path of filtered resources list}. Liste mit den auszuschließenden Ressourcen in der betreffenden XML-Datei (die XML-Datei sollte der Datei **schema\filtered_resources.xsd** entsprechen).

-fullCM. Ändert das Klassenmodell-Upgrade in den **vollständigen Modus**. Im vollständigen Modus werden neue Packages erstellt und das Klassenmodell wird als Ganzes verarbeitet, um mehr Prüfungen und Korrekturen zu ermöglichen. Im vollständigen Modus decken die Packages (mindestens) das gesamte Standardklassenmodell ab. Standardmäßig erfolgt das Upgrade im **partiellen Modus**, d. h. unvollständig.

-analyzeDataActions {DATA_ACTIONS_FILE}. Analysiert die Änderungen und erzeugt die Analysedatei für Datenaktionen mit dem angegebenen Dateinamen. Impliziert **-fullCM**.

-outputFullCM {OUTPUT_FULL_CM_FILE}. Gibt das vollständige neue Klassenmodell in eine Datei aus. Impliziert **-fullCM**.

-out {OUTPUT_DIR}. Verzeichnispfad für aktualisierte Packages.

-doNotCreateNewPackages. Durch diese Option erstellt das Upgrade-Programm keine neue Package-Datei.

{INPUT_DIR}. Der Verzeichnispfad der zu aktualisierenden Packages.

Umgebungsvariablen. **ucmdb.home**. Muss auf das Produktverzeichnis verweisen (in der Regel **C:\hp\UCMDB\UCMDBServer** für UCMDB im eigenständigen Modus).

4 Suchen Sie die migrierten Packages im angegebenen Ausgabeverzeichnis. Stellen Sie die migrierten Packages im UCMDB-System der Version 9.02 bereit.

Referenz

Fehlerbehebung und Einschränkungen

- Das Dienstprogramm für die Package-Migration wurde nur für Packages geprüft, die mit UCMDB 8.04 kompatibel sind.
- Packages mit Enrichment-Definitionen, die auf gelöschte oder aktualisierte CI-Typen verweisen, können nicht mit dem Dienstprogramm für die Package-Migration aktualisiert werden.
- Eine partielle Migration wird nicht unterstützt. Das Dienstprogramm für die Package-Migration erstellt kein neues Package, wenn eine oder mehrere Ressourcen nicht erfolgreich migriert werden können.

Teil V

Hochverfügbarkeit und Kapazitätsplanung

16

Installieren im Hochverfügbarkeitsmodus

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

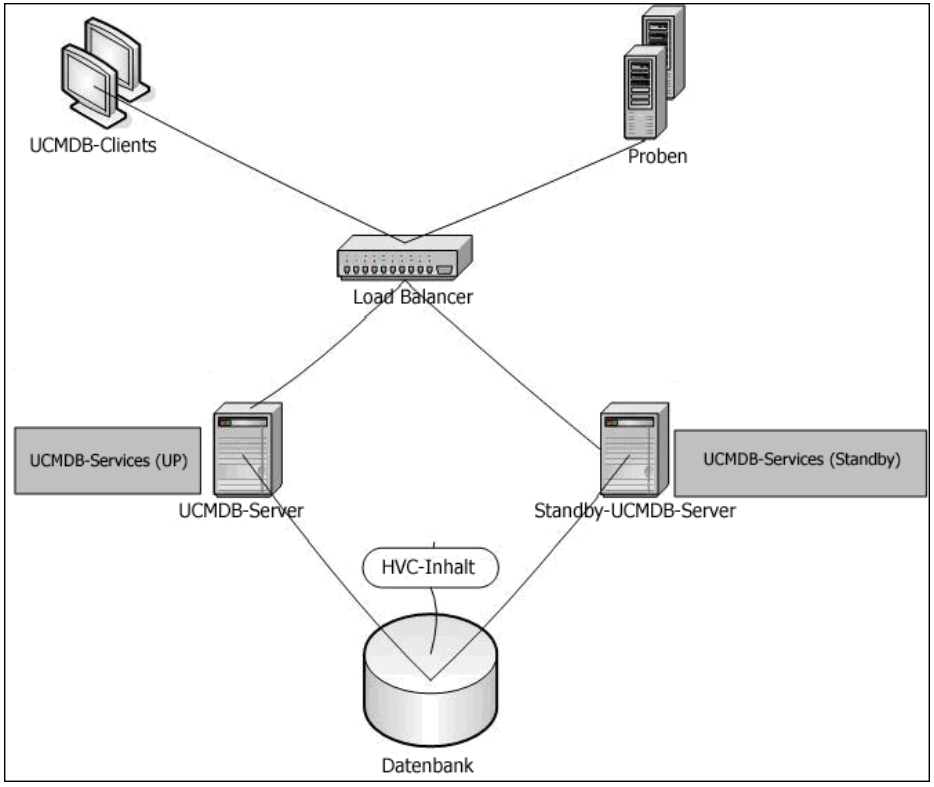
Übergänge zwischen den aktiven und passiven Servern

Konzepte

Best Practices für die HP Universal CMDB-Hochverfügbarkeitslösung

In diesem Abschnitt werden Best Practices für die praktische Umsetzung der HP Universal CMDB-Hochverfügbarkeitslösung beschrieben.

Grafik zur Lösung:



- Alle externen Zugriffe auf die HP Universal CMDB-Applikation erfolgen über den Load Balancer.
- Zwei oder mehr Server sind konfiguriert.

- HP Universal CMDB-Services werden auf allen Servern im Cluster ausgeführt, aber die Kundenkomponenten sind nur auf dem aktiven Server aktiv.
- Load Balancer mit:
  - Keep-Alive-Adresse **http://<UCMDB Server:Port>/ping?clusterId=<Cluster-ID>.**
  - Round-Robin-Richtlinie für die Server.
  - Beibehaltung von Sticky Sessions.
  - Konfiguration einer virtuellen IP pro Cluster.
- Verbindung jedes Servers mit zwei separaten Netzwerken:
  - Frontend (für Load Balancer-Zugriff)
  - Backend (für Datenbank- und Hochverfügbarkeitscontroller-Kommunikation)

Übergänge zwischen den aktiven und passiven Servern

Um die Startzeiten der passiven Computer während eines Übergangs vom aktiven Computer zu verbessern, startet HP Universal CMDB die passiven Computer im partiellen Modus.

In diesem Fall wird die Modelltopologie-Komponente auf den passiven Computern im schreibgeschützten Modus gestartet. Anschließend wird sie von der UCMDB-Datenbank alle paar Sekunden mit den Änderungen synchronisiert, die auf dem aktiven Server erfolgen.

Wenn der passive Computer übernimmt, startet er schnell, da der Großteil des Modells bereits in den Speicher geladen wurde.

Aufgaben

Installieren von HP Universal CMDB im Hochverfügbarkeitsmodus

In diesem Abschnitt werden die Prozeduren beschrieben, die für das Installieren, Starten und Konfigurieren von HP Universal CMDB im Hochverfügbarkeitsmodus gelten.

Hinweis: Der Hochverfügbarkeitsmodus wird in einer Mehrkundenumgebung nicht unterstützt.

Dieser Abschnitt umfasst die folgenden Themen:

1 Installieren der Server

a Installieren Sie den UCMDB Server auf zwei oder mehr Computern, ohne den Konfigurationsassistenten auszuführen (wählen Sie bei der Eingabeaufforderung für den Assistenten **Nein** aus). Die typische Konfiguration besteht aus einem **aktiven** Server und einem **passiven** Server.

Weitere Informationen finden Sie unter "Installieren von HP Universal CMDB auf einer Windows-Plattform" auf Seite 73 oder "Installieren von HP Universal CMDB auf einer Linux-Plattform" auf Seite 89.

Hinweis: Die Computer, die für die aktiven und passiven UCMDB Server verwendet werden, sollten ähnliche Hardware (insbesondere dieselbe Speichermenge) aufweisen und mit demselben Betriebssystem ausgeführt werden.

---

b Führen Sie den Konfigurationsassistenten auf dem Server aus, der zum aktiven Server werden soll. Wählen Sie **Neues Schema erstellen** aus. Weitere Informationen finden Sie unter "UCMDB-Serverkonfiguration" auf Seite 105.

c Führen Sie den Konfigurationsassistenten auf dem passiven Server aus. Wählen Sie **Mit einem vorhandenen Schema verbinden** aus und geben Sie die Details des Schemas ein, das Sie für den aktiven Server erstellt haben.

- Zum Ausführen des Assistenten auf einer Windows-Plattform wählen Sie **Start** > **Alle Programme** > **HP UCMDB** > **Konfigurationsassistenten für HP Universal CMDB Server starten** aus.
- So führen Sie den Assistenten auf einer Linux-Plattform aus:

```
/opt/hp/UCMDB/UCMDBServer/bin/configure.sh
```

2 Abschließen des Serverstarts

a Starten Sie den aktiven Server. Warten Sie, bis der Startvorgang abgeschlossen ist.

b **Für Windows**: Rufen Sie **server_management.bat** (das Serververwaltungs-Tool) im folgenden Ordner auf: **C:\hp\UCMDB\UCMDBServer\tools**.

Für Linux: Führen Sie **server_management.sh** im folgenden Ordner aus: **/opt/hp/UCMDB/UCMDBServer/tools/**.

- Geben Sie auf der Anmeldeseite den Servernamen und die Anmeldeinformationen ein.

Wenn der Standard-SSL-Port verwendet wird (Port **8443**), geben Sie nur den Servernamen ein (z. B. **localhost**).

Wenn der SSL-Port geändert wurde, geben Sie den Servernamen und den neuen Port ein (z. B. **localhost:443**).

➤ Geben Sie den Benutzernamen und das Kennwort des Systembenutzers ein (die Standardeinstellungen lauten **sysadmin** und **sysadmin**).

Hinweis: Die Verbindung vom Tool zum HP Universal CMDB Server wird über HTTPS hergestellt. Tritt ein Problem mit der Verbindung auf, stellen Sie sicher, dass der **SSL**-Modus konfiguriert ist (**HTTPS-Verbindungen aktivieren** muss den Wert **True** aufweisen).

---

c Wählen Sie im linken Menü des Serververwaltungs-Tools die Option **Cluster** aus. Klicken Sie auf die Schaltfläche **Neues Cluster**, um ein neues Cluster zu erstellen.

d Geben Sie im Feld **Server hinzufügen** den Computernamen für einen der Server ein, die Sie installiert haben. Klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Vorgang für die anderen Server.

e Wählen Sie in der Liste der Servernamen den Server aus, der zum aktiven Server werden soll. Klicken Sie auf **Aktivieren**.

f Klicken Sie auf **OK**.

g Beantworten Sie die Frage, ob alle vorhandenen Kunden auf den aktiven Server umgeschaltet werden sollen, mit **Ja**.

Hinweis: Um den Benutzer oder Server zu ändern, klicken Sie auf den Link **Abmelden**, um sich im Serververwaltungs-Tool abzumelden.

---

h Starten Sie den passiven Server und führen Sie die Datei **server_management.bat** auf diesem Server aus.

Hinweis: Wenn Sie einen UCMDB Server mit dem Serververwaltungs-Tool von einem aktiven in einen passiven Server umwandeln, kann Datenbankinkonsistenz auftreten. Um dies zu verhindern, halten Sie den UCMDB Server auf dem aktiven Computer an. Nach einer kurzen Zeitspanne (etwa einer Minute) wird der passive Server zum aktiven Server.

Alle Server in einem Cluster müssen denselben Port für HTTP, HTTPS usw. aufweisen. Sie können für die zwei Server keine unterschiedlichen Ports konfigurieren.

---

3 Konfigurieren des Servers

a Wählen Sie die Kategorie **Verwaltung** > **Infrastructure Settings Manager** > **Allgemeine Einstellungen** aus.

b Suchen Sie die folgenden Einstellungen und ändern Sie sie:

- **Frontend-URL aus Einstellungen aktiviert?** muss den Wert **True** aufweisen.
- Als **Frontend-URL** muss der Load Balancer-URL angegeben sein. Das erforderliche Format lautet **URL://<Servername>:<Port>**.

4 Konfigurieren des Load Balancer

Definieren Sie die virtuelle IP für die zwei HP Universal CMDB Server mit der folgenden Konfiguration:

- Wählen Sie den in den Infrastruktureinstellungen definierten Port aus.
- Stellen Sie sicher, dass eine Round-Robin-Richtlinie für die Server besteht.
- Stellen Sie sicher, dass Sticky Sessions beibehalten werden.
- Stellen Sie sicher, dass die virtuelle IP für jedes Cluster konfiguriert ist.

➤ Die Keep-Alive-Adresse für die Sitzung lautet: **http://<UCMDB Server:Port>/ping?clusterId=<Cluster-ID>**. Ein aktiver Server im Cluster gibt HTTP-Antwort 200 zurück (OK). Ein passiver Server gibt HTTP-Antwort 503 zurück (Service nicht verfügbar).

Hinweis: Der Load Balancer muss unbedingt die Cluster-ID in der Keep-Alive-Anfrage angeben, da ein Server zu mehreren Clustern gehören kann und in einem davon aktiv und im anderen passiv ist.

---

5 Konfigurieren der Probe

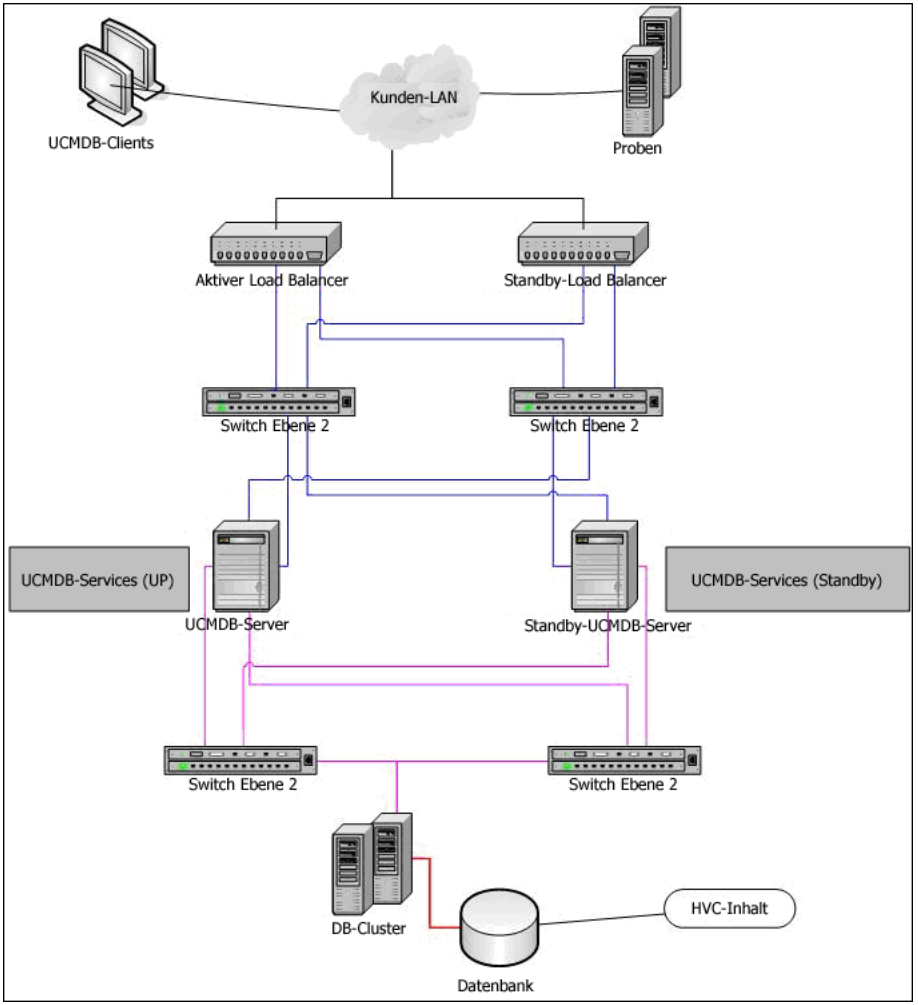
a Führen Sie die Probe-Installation auf dem Probe-Computer mit der virtuellen IP-Adresse des Load Balancer als HP Universal CMDB Server-Name aus.

b Starten Sie die Probe.

Konfigurieren der Netzwerkhochverfügbarkeit

Für die Bereitstellung von Netzwerkhochverfügbarkeit verbinden Sie die Load Balancer und Datenbanken über Switches mit den Servern und verwenden dabei Intel-Netzwerkkarten und Spanning Tree (für Windows).

Konfigurationsdiagramm der Lösung für vollständige Netzwerkredundanz:



Konfigurieren der vollständigen Site

- Das Backend-Netzwerk sollte auf der Hauptschnittstelle definiert sein (der an den Servernamen gebundenen Schnittstelle). Ist dies nicht der Fall, bearbeiten Sie die Datei etc/hosts, um die Backend-Schnittstelle als an den Servernamen gebunden zu definieren.
- Währen der Serverinstallation sollte der Backend-Hostname bzw. die Backend-IP als HP Universal CMDB Server/IP definiert werden.

17

HP Universal CMDB – Planen großer Kapazitäten

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

Planen großer Kapazitäten – Übersicht

Die Standardkonfiguration von HP Universal CMDB eignet sich für eine Bereitstellung mit mehr als 25 Millionen Objekten und Links. Für eine größere Bereitstellung müssen Sie die folgende Konfiguration implementieren:

- Erhöhen Sie die Heap-Größe der CMDB auf 8 GB. Weitere Informationen finden Sie unter "Konfigurieren von UCMDB Server" auf Seite 289.
- Wenn Sie mit einer Oracle-Datenbank arbeiten, richten Sie den globalen Systembereich (SGA) der Oracle-Datenbank wie folgt ein: 4 GB unterstützt, 8 GB empfohlen. Weitere Informationen finden Sie unter "Konfigurieren der Oracle-Datenbank" auf Seite 290.

In der folgenden Tabelle ist die maximal unterstützte Anzahl an CIs und Links in einer UCMDB-Bereitstelllung aufgeführt:

Datenbank/ Betriebssystem	Windows	Linux
MS SQL Server	40 Millionen CIs und Links	12,5 Millionen CIs und Links
Oracle	40 Millionen CIs und Links (Erforderliche Konfiguration wie in diesem Abschnitt beschrieben)	40 Millionen CIs und Links (Erforderliche Konfiguration wie in diesem Abschnitt beschrieben)

Für weitere Informationen:

- Informationen zu den Änderungen, die Sie an der Systemkonfiguration vornehmen müssen, um diese Kapazität zu unterstützen, finden Sie unter "Konfigurieren von UCMDB Server" auf Seite 289.

- Informationen zum Steigern der Leistung finden Sie unter "Konfigurieren der Oracle-Datenbank" auf Seite 290.
- Informationen zum Aufbau des Kapazitätstests finden Sie unter "Aufbau des Systemtests" auf Seite 291.
- Informationen zu den Leistungsergebnissen von Systemtestläufen für UCMDB 9.02 finden Sie unter "Ergebnisse des Systemtests" auf Seite 292.

Verwaltete Knoten und Knoten-zugehörige CIs

Bei der Kapazitätsplanung müssen Sie unter anderem das Verhältnis zwischen den verwalteten Knoten in der CMDB und den Knoten-zugehörigen CIs berücksichtigen. Zu den Knoten-zugehörigen CIs zählen alle CIs mit Typen, die Unterklassen der Applikationsressourcen, Knotenelemente oder aktiven Software sind.

In der folgenden Tabelle ist die Anzahl an Knoten-zugehörigen CIs aufgeführt, die Sie für jeden verwalteten Knoten in der Umgebung erkennen können. Diese Anzahl hängt von der Größe Ihrer Bereitstellung und der Anzahl an verwalteten Knoten ab. Je mehr verwaltete Knoten in der CMDB vorhanden sind, desto weniger Knoten-zugehörige CIs können Sie für jeden verwalteten Knoten erkennen.

Beispiel: Wenn Sie in einer Unternehmensbereitstellung 89.600 verwaltete Knoten ausführen, können Sie 160 Host-zugehörige CIs für jeden verwalteten Host erkennen. Wenn Sie nur 28.000 verwaltete Hosts ausführen, können Sie 500 Ressourcen-CIs für jeden verwalteten Host erkennen.

Bereitstellung	Anzahl an verwalteten Hosts/Host-zugehörigen CIs
Enterprise	89600/160 - 28800/500
Standard	9000/160 – 3000/500
Klein	4500/160 – 1000/500

Hinweis: Die Zahlen in der Tabelle enthalten nur CIs und keine Links.

Aufgaben

Konfigurieren von UCMDB Server

Damit das System 40 Millionen CIs und Links unterstützt, müssen Sie auf dem UCMDB Server die folgenden Parameter aktualisieren:

Windows:

- **C:\hp\UCMDB\UCMDBServer\bin\wrapper-platform.conf**

  wrapper.java.initmemory=2048

  wrapper.java.maxmemory=8192

- **C:\hp\UCMDB\UCMDBServer\conf\settings.override.properties**

  dal.object.condition.max.result.size=50000000

  dal.use.memory.instead.temp.table.high.threshold.oracle=6000000

  dal.joinf.max.result.size=4000000

Linux:

- **opt/hp/UCMDB/UCMDBServer/bin/wrapper-platform.conf**

  wrapper.java.initmemory=2048

  wrapper.java.maxmemory=8192

- **opt/hp/UCMDB/UCMDBServer/bin/settings.override.properties**

  dal.object.condition.max.result.size=50000000

  dal.use.memory.instead.temp.table.high.threshold.oracle=6000000

  dal.joinf.max.result.size=4000000

Konfigurieren der Oracle-Datenbank

Wenn Sie mit einem System arbeiten, das 40 Millionen Objekte und Links enthält, können Sie die Leistung steigern, indem Sie den globalen Systembereich (SGA) von Oracle von 6 GB auf 8 GB vergrößern (d. h. auf die empfohlene Konfiguration). Dadurch steigt die Leistung sowohl bei der TQL-Berechnung für einige TQL-Typen als auch bei der Ausführung von Dateneingabevorgängen im System.

Referenz

Aufbau des Systemtests

Für den Systemtest wurde eine Systemkapazität von 40 Millionen CIs und Links verwendet.

Für den Test wurde die folgende Hardware verwendet:

Rolle	Computertyp	CPU	Speicher	VM/ SWAP	Betriebssystem + Drittanbieter-SW
CMDB	HP Proliant BL460c G6	2 x Intel Xeon-Vierkernprozessor mit 2,533 GHz	16 GB	Windows: 24 GB Linux: 16 GB	Win2008R2 64-Bit Red Hat Enterprise Linux Server Release 5.5
Data Flow Probe	HP ProLiant DL 140 G2	2 x CPU mit 3,0 GHz	2 MB	3 MB	Windows 2003 Server EE
Datenbank	HP Proliant BL460c G6	2 x Intel Xeon-Vierkernprozessor mit 2,933 GHz	32 GB	51 GB	Win2008R2 64-Bit REHL 5.4

Für den Test wurde die folgende Softwareversion verwendet:

- Oracle Database 11g, Release 11.2.0.1.0

Im Rahmen des Systemtests wurden die folgenden Geschäfts-Flows getestet:

- **TQL-Berechnung**

  TQLs wurden in Untergruppen aufgeteilt. Dies erfolgte abhängig von der Ergebnisgröße (<100, <1000 oder <10000), abhängig vom Datensatz, den die TQL abruft, und abhängig von der TQL-Konfiguration:

  - Wie-Bedingung
  - Wie (ohne Groß-/Kleinschreibung)

- Perspektive
- Unterschiedliche Anzahl an Hierarchien in den TQL-Ergebnissen (1 - 5)
- Verbund
- Unterdiagramm
- JoinF

- **Dateneingabe**

  Zu den Dateneingabeszenarien beim Systemtest zählten Einfügen, Aktualisieren und Löschen.

- **Enrichments**

  Zu den Enrichment-Szenarien zählten Einfügen, Aktualisieren und Löschen.

Ergebnisse des Systemtests

In einem Belastungstest über 24 Stunden mit einem Szenario, das Abfragen, Dateneingabe und Enrichments umfasste, wurden die folgenden Ergebnisse erzielt:

- Das System blieb über den gesamten Testlauf stabil. Es wurden keine Neustarts, Speicher-Leaks oder andere Probleme festgestellt.
- Die Systemleistung war akzeptabel. Für die meisten TQLs lag die 90 %-Perzentile unter 1 Sekunde Berechnungszeit.

Teil VI

Härten von HP Universal CMDB

18

Einführung zum Härten

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Härten – Übersicht

In diesem Abschnitt wird das Konzept sicherer HP Universal CMDB-Anwendungen 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 321.

Wenn Sie für HP Universal CMDB eine andere als die in diesem Dokument beschriebene sichere Architektur einsetzen müssen, wenden Sie sich an HP Software Support, 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 361.

Wichtig:

- Bei den Härtungsprozeduren wird davon ausgegangen, dass Sie nur die in diesen Abschnitten 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 Abschnitten 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 Abschnitt 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 305 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.

Aufgaben

Bereitstellen von HP Universal CMDB 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 305.

➤ **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 321.

Hinweis: Wenn der UCMDB Server für die Verbindung mit einem Reverse-Proxy konfiguriert ist, wird die gegenseitige Authentifizierung mithilfe von SSL zwischen dem Reverse-Proxy-Server und der Data Flow Probe nicht unterstützt. Weitere Informationen finden Sie unter "Aktivieren von SSL zwischen UCMDB Server und Data Flow Probe mit gegenseitiger Authentifizierung" auf Seite 367.

Ändern des Systembenutzernamens oder Kennworts für die JMX-Konsole

Die JMX-Konsole verwendet Systembenutzer, d. h. kundenübergreifende Benutzer in einer Mehrmandantenumgebung. 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=Security Services** und klicken Sie auf den Link, um die Seite **Operations** zu öffnen.

4 Suchen Sie den Vorgang **changeSystemUserPassword**.

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

   Unter 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).

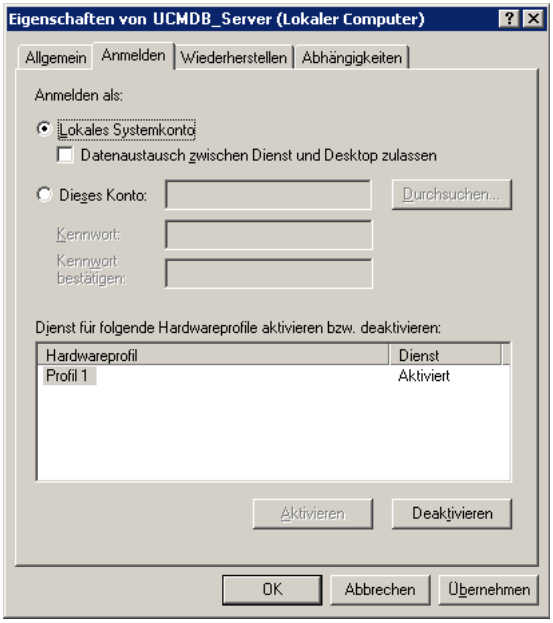
Der Benutzer, den Sie für die Ausführung des Services zuweisen, muss über die folgenden Berechtigungen verfügen:

- 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" auf Seite 125.
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" auf Seite 125.

19

Aktivieren der SSL-Kommunikation

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Aufgaben

Aktivieren von SSL auf dem Servercomputer mit einem selbstsignierten Zertifikat

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, entfernen Sie den alten Key Store des Servers 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.

Einschränkung: 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 316.

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

---

5 Neustarten des Servers

6 Anzeige HP Universal CMDB

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

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

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

1 Voraussetzungen

Bevor Sie mit der folgenden Prozedur beginnen, entfernen Sie 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 316.

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://<UCMDB Server-Name oder -IP-Adresse>:8443/ucmdb-ui**.

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

Aktivieren von SSL auf den Clientcomputern

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

Wichtig: 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.certi
```

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=Server 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** > **Infrastructure Settings Manager** 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.

Einschränkung: 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**.

20

Verwenden eines Reverse-Proxy

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

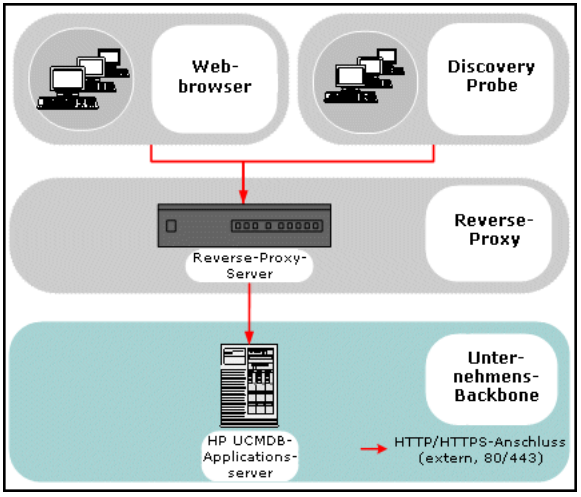
Reverse-Proxy – Übersicht

Hinweis: Im Folgenden werden die Sicherheitsauswirkungen von Reverse-Proxys beschrieben und Sie finden Anweisungen für die Verwendung eines Reverse-Proxy mit HP Universal CMDB. Es werden nur die Sicherheitsaspekte eines Reverse-Proxy besprochen, aber keine anderen Themen wie Caching und Load Balancing.

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.

HP Universal CMDB unterstützt 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 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 "Apache 2.0.x – Beispielkonfiguration" auf Seite 327.

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 kann sich der Applikationsserver auf einem separaten Computer im internen Netzwerk befinden.

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.

Aufgaben

Konfigurieren eines Reverse-Proxy über die Infrastruktureinstellungen

In der folgenden Prozedur wird erklärt, wie Sie mithilfe der Infrastruktureinstellungen eine Reverse-Proxy-Konfiguration aktivieren:

So aktivieren Sie eine Reverse-Proxy-Konfiguration:

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/**.
3. Ändern Sie den Wert für **Frontend-URL aus Einstellungen aktiviert?** in **True**.

Wichtig: Nachdem Sie diese Änderung vorgenommen haben, können Sie nicht mehr direkt von einem Client auf den HP Universal CMDB Server zugreifen. Sie können jedoch die Reverse-Proxy-Konfiguration über die JMX-Konsole auf dem Servercomputer ändern. Weitere Informationen finden Sie unter "Konfigurieren eines Reverse-Proxy mit der JMX-Konsole" auf Seite 326.

Konfigurieren eines Reverse-Proxy mit der JMX-Konsole

In der folgenden Prozedur wird erklärt, wie Sie die Reverse-Proxy-Konfiguration mithilfe der JMX-Konsole auf dem HP Universal CMDB Server-Computer ändern.

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**.

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

4. Klicken Sie auf **Invoke**.

5. Zum Aktivieren oder Deaktivieren dieser Einstellung verwenden Sie die Methode **enableUseFrontendURLBySettings** bzw. **disableUseFrontendURLBySettings**.

6. Zum Anzeigen des Werts für diese Einstellung verwenden Sie die Methode **showFrontendURLInSettings**.

Apache 2.0.x – Beispielkonfiguration

Das folgende Beispiel zeigt eine Konfigurationsdatei für die Verwendung eines Apache 2.0.x-Reverse-Proxy in einem Fall, in dem sowohl Data Flow Probes als auch Applikationsbenutzer eine Verbindung zu HP Universal CMDB herstellen.

Hinweis:

- Im folgenden Beispiel lautet der DNS-Name des HP Universal CMDB-Computers **UCMDB_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

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 /site http://UCMDB_server/status
ProxyPassReverse /site http://UCMDB_server/status
ProxyPass /site http://UCMDB_server/jmx-console
ProxyPassReverse /site http://UCMDB_server/jmx-console
ProxyPass /site http://UCMDB_server/axis2
ProxyPassReverse /site http://UCMDB_server/axis2
ProxyPass /site http://UCMDB_server/icons
ProxyPassReverse /site http://UCMDB_server/icons
ProxyPass /site http://UCMDB_server/ucmdb-api
ProxyPassReverse /site http://UCMDB_server/ucmdb-api
ProxyPass /site http://UCMDB_server/ucmdb-docs
ProxyPassReverse /site http://UCMDB_server/ucmdb-docs
ProxyPass /site http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /site http://UCMDB_server/ucmdb-api/8.0
```

4 Speichern Sie Ihre Änderungen.

21

Verwalten der Data Flow-Anmeldeinformationen

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

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 unter "Fenster "Data Flow Probe einrichten"" auf Seite 60.

Der Speicher mit den Anmeldeinformationen wird von der Komponente „Confidential Manager“ (CM) verwaltet. Weitere Informationen finden Sie unter "Confidential Manager" auf Seite 407.

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

Die CM-Client-Authentifizierung auf dem CM-Server basiert auf einer LW-SSO-Komponente. Vor der Verbindung zum CM-Server sendet der CM-Client zunächst ein LW-SSO-Cookie. Der CM-Server prüft das Cookie und beginnt nach erfolgreicher Prüfung die Kommunikation mit dem CM-Client. Weitere Informationen zu LW-SSO finden Sie unter "Konfigurieren der LW-SSO-Einstellungen auf dem UCMDB-Server" auf Seite 336.

Die Kommunikation zwischen dem CM-Client und dem CM-Server ist verschlüsselt. Informationen zum Aktualisieren der Verschlüsselungskonfiguration finden Sie unter "Konfigurieren der CM-Kommunikationsverschlüsselung auf dem UCMDB-Server" auf Seite 337.

Der CM-Client behält die Anmeldeinformationen in einem lokalen Cache. Der CM-Client ist so konfiguriert, dass alle Anmeldeinformationen vom CM-Server heruntergeladen und in einem Cache gespeichert werden. Änderungen an den Anmeldeinformationen werden automatisch in regelmäßigen Abständen vom CM-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 CM-Client auf der Probe" auf Seite 343. Informationen zum Aktualisieren der Cache-Verschlüsselung finden Sie unter "Konfigurieren der Cache-Verschlüsselung für den CM-Client auf der Probe" auf Seite 344.

Informationen zur Fehlerbehebung finden Sie unter "Ändern der Meldungsebene für die CM-Client-Protokolldatei" auf Seite 349.

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 346.

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:

➤ "Synchronisieren aller Proben mit Konfigurationsänderungen" auf Seite 333

➤ "Sicheres Speichern auf der Probe" auf Seite 334

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 des Confidential Manager (CM) zu einem Teil des Manager-Prozesses. Anmeldeinformationen werden im Cache gespeichert und nur vom Probe Manager verwendet. Für den Zugriff auf den CM-Server im UCMDB-System wird die CM-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 CM-Server lädt der CM-Client alle relevanten Anmeldeinformationen herunter (alle in der Probe-Domäne konfigurierten Anmeldeinformationen). Nach der ersten erfolgreichen Kommunikation wird der CM-Client kontinuierlich mit dem CM-Server synchronisiert. Die Synchronisierung erfolgt in Intervallen von einer Minute, wobei nur die Abweichungen zwischen dem CM-Server und dem CM-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 CM-Client eine sofortige Benachrichtigung vom UCMDB-Server und führt eine zusätzliche Synchronisierung durch.

Synchronisieren aller Proben mit Konfigurationsänderungen

Für die erfolgreiche Kommunikation muss der CM-Client mit der Authentifizierungskonfiguration (LW-SSO-Init-Zeichenkette) und der Verschlüsselungskonfiguration (CM-Kommunikationsverschlüsselung) des CM 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 CM-Kommunikation und an der CM-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 UCMDB Server und 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 351.

Hinweis:

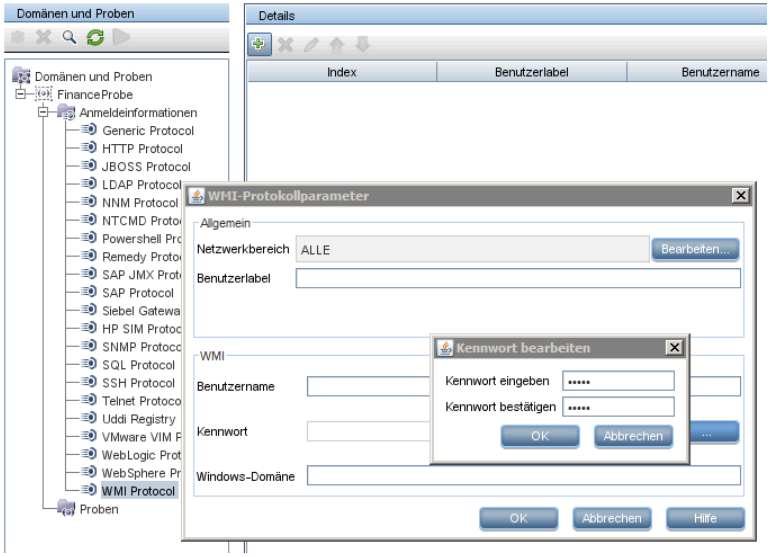
- Aufgrund des Überwachungsintervalls von 15 Sekunden kann es vorkommen, dass der CM-Client auf der Probe über eine Zeitspanne von 15 Sekunden nicht mit der neuesten Konfiguration aktualisiert wird.
- Wenn Sie die automatische Synchronisierung der Kommunikations- und Authentifizierungskonfiguration für CM zwischen dem UCMDB-Server und der Data Flow Probe deaktivieren, sollten Sie jedes Mal, wenn Sie die Kommunikations- und Authentifizierungskonfiguration für CM auf dem UCMDB-Server ändern, auch alle Proben mit der neuen Konfiguration aktualisieren. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339.

Sicheres Speichern auf der Probe

Alle sensiblen Informationen (wie z. B. die Kommunikations- und Authentifizierungskonfiguration für CM und der Verschlüsselungsschlüssel) werden auf der Probe in einem sicheren Speicher in der Datei **secured_storage.bin** aufbewahrt, 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 (Datenrichtung: CMDB an HP Universal CMDB)

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 (Datenrichtung: HP Universal CMDB an CMDB)

- 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.

Aufgaben

Konfigurieren der CM-Clientauthentifizierung und -Verschlüsselung auf dem UCMDB-Server

Diese Aufgabe umfasst folgende Schritte:

- "Konfigurieren der LW-SSO-Einstellungen auf dem UCMDB-Server" auf Seite 336
- "Konfigurieren der CM-Kommunikationsverschlüsselung auf dem UCMDB-Server" auf Seite 337

Konfigurieren der LW-SSO-Einstellungen auf dem UCMDB-Server

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), außer wenn der UCMDB-Server so konfiguriert ist, dass dieser Vorgang nicht automatisch erfolgt. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339.

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 CM-Kommunikationsverschlüsselung auf dem UCMDB-Server

In dieser Prozedur wird beschrieben, wie Sie die Einstellungen für die CM-Kommunikationsverschlüsselung ändern. Diese Einstellungen bestimmen, wie die Kommunikation zwischen dem CM-Client und dem CM-Server verschlüsselt wird. Diese Änderung wird automatisch an die Proben gesendet (als verschlüsselte Zeichenkette), außer wenn der UCMDB-Server so konfiguriert ist, dass dieser Vorgang nicht automatisch erfolgt. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339.

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 CM-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.

   Weitere Informationen zu den Werten, die aktualisiert werden können, finden Sie unter "CM-Verschlüsselungseinstellungen" auf Seite 358.

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 CM-Clientauthentifizierung und -Verschlüsselung auf der Probe

Diese Aufgabe umfasst folgende Schritte:

- "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339
- "Konfigurieren der CM-Clientauthentifizierung und -Verschlüsselung auf der Probe" auf Seite 340
- "Konfigurieren der CM-Kommunikationsverschlüsselung auf der Probe" auf Seite 341

Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben

Standardmäßig ist der UCMDB-Server so konfiguriert, dass die CM/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 CM/LW-SSO-Konfigurationsdateien nicht automatisch an alle Proben gesendet werden. In diesem Fall sind Sie selbst dafür verantwortlich, alle Proben manuell mit den neuen CM/LW-SSO-Einstellungen zu aktualisieren.

So deaktivieren Sie die automatische Synchronisierung der CM/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 zum Speichern.
5. Starten Sie den UCMDB -Server neu.

Konfigurieren der CM-Clientauthentifizierung und -Verschlüsselung auf der Probe

Diese Prozedur ist relevant, wenn der UCMDB-Server so konfiguriert wurde, dass CM/LW-SSO-Konfigurationen und -Einstellungen nicht automatisch an die Proben gesendet werden. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339.

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

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/jmx-console**.

---

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 CM-Kommunikationsverschlüsselung auf der Probe

Diese Prozedur ist relevant, wenn der UCMDB-Server so konfiguriert wurde, dass CM/LW-SSO-Konfigurationen und -Einstellungen nicht automatisch an die Proben gesendet werden. Weitere Informationen finden Sie unter "Deaktivieren der automatischen Synchronisierung der CM-Clientauthentifizierung und -Verschlüsselung zwischen dem UCMDB-Server und den Proben" auf Seite 339.

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

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/jmx-console**.

---

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 CM-Kommunikationsverschlüsselung auf dem UCMDB-Server" auf Seite 337. Informationen zu den Werten, die aktualisiert werden können, finden Sie unter "CM-Verschlüsselungseinstellungen" auf Seite 358.

---

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

b **setTransportEncryptionAlgorithm** ändert CM-Einstellungen 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 CM-Einstellungen 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 CM-Einstellungen 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 "CM-Verschlüsselungseinstellungen" auf Seite 358.

Konfigurieren des Client-Cache für Confidential Manager (CM)

Diese Aufgabe umfasst folgende Schritte:

- "Konfigurieren des Cache-Modus für den CM-Client auf der Probe" auf Seite 343
- "Konfigurieren der Cache-Verschlüsselung für den CM-Client auf der Probe" auf Seite 344

Konfigurieren des Cache-Modus für den CM-Client auf der Probe

Der CM-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 **DiscoveryProbe.properties** in einem Texteditor. Diese Datei befindet sich im Verzeichnis **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 **DiscoveryProbe.properties**.
4. Starten Sie die Probe neu.

Konfigurieren der Cache-Verschlüsselung für den CM-Client auf der Probe

In dieser Prozedur wird beschrieben, wie Sie die Verschlüsselungseinstellungen für die Cache-Datei im CM-Client-Dateisystem ändern. Beachten Sie, dass die Cache-Datei im CM-Client-Dateisystem 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/jmx-console**.

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/jmx-console**.

---

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 "CM-Verschlüsselungseinstellungen" auf Seite 358.

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.
- **Bei 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.

Wichtig: 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 impvvom 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 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 Version 8.02 exportiert wurde, geben Sie den Dateinamen **key.bin** ein. Diese Datei muss sich im Verzeichnis **c:\hp\UCMDB\UCMDBServer\conf\discovery\<Kundenverzeichnis>** befinden, zusammen mit der zu importierenden Datei.

8. Klicken Sie auf **Invoke**, um die Anmeldeinformationen zu importieren.

Ändern der Meldungsebene für die CM-Client-Protokolldatei

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

➤ "CM-Client-Protokolldatei" auf Seite 349

➤ "LW-SSO-Protokolldatei" auf Seite 350

CM-Client-Protokolldatei

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

Das Protokoll enthält Informationsmeldungen, die zwischen dem CM-Server und dem CM-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 Verzeichnis **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 Konfigurationen für die CM-Kommunikation und -Authentifizierung 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" auf Seite 352
- "Aktualisieren eines Verschlüsselungsschlüssels auf einem UCMDB-Server" auf Seite 354
- "Aktualisieren eines Verschlüsselungsschlüssels auf einer Probe" auf Seite 355
- "Manuelles Ändern des Verschlüsselungsschlüssels, wenn Probe Manager und Probe Gateway auf separaten Computern installiert sind" auf Seite 356
- "Erzeugen eines neuen Verschlüsselungsschlüssels" auf Seite 352

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. 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**.

Wichtig: 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.

Wichtig: 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 den 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/jmx-console**.

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/jmx-console.

---

3 Klicken Sie in der Probe-Domäne auf **type=MainProbe**, um die Seite **JMX MBEAN View** zu öffnen.

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**.

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 Gateway-Service (**Start** > **Programme** > **HP UCMDB** > **Probe Gateway**).

2 Importieren Sie den Schlüssel vom Server über die JMX-Konsole des Probe Gateway. Weitere Informationen finden Sie unter "Erzeugen eines neuen Verschlüsselungsschlüssels" auf Seite 352.

3 Halten Sie nach dem erfolgreichen Importieren des Verschlüsselungsschlüssels den Probe Gateway-Service an.

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 das Verzeichnis $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.

Referenz

CM-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 CM-Client und dem CM-Server sowie für die Verschlüsselung des CM-Client-Cache.

Name der UCMDB-CM-Einstellung	Name der Probe-CM-Einstellung	Beschreibung der Einstellung	Mögliche Werte	Standardwert
cryptoSource	Encryption Library name	Diese Einstellung definiert, welche Verschlüsselungs-bibliothek verwendet wird.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBECompatibilityMode	Support previous lightweight cryptography versions	Diese Einstellung definiert, ob vorherige schwache Kryptographie unterstützt wird oder nicht.	true, false	true
engineName	Engine name	Name des Verschlüsselungs-mechanismus	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Länge des Verschlüsselungs-schlüssels in Bit	Für AES – 128, 192 oder 256; Für DES – 64; Für 3DES – 192; Für Blowfish – eine beliebige Zahl zwischen 32 und 448	256

Name der UCMDB-CM-Einstellung	Name der Probe-CM-Einstellung	Beschreibung der Einstellung	Mögliche Werte	Standardwert
algorithmPadding 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
pbeDigestAlgorithm	PBE digest algorithm	Hashing-Typ	SHA1, SHA256, MD5	SHA1
useMacWithCrypto	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

22

Härten der Data Flow Probe

Dieses Kapitel umfasst die folgenden Themen:

Aufgaben

Referenz

Aufgaben

Einrichten des verschlüsselten Kennworts für die MySQL-Datenbank

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

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 Argument aus, z. B. **set_dbuser_password <mein_Kennwort>**.

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 auf Seite 362 beschrieben.

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

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

  Beispiel:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,6
1,61
```

- **appilog.agent.local.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 mit einem Kennwort, das als Argument für das Skript bereitgestellt wird, neu erstellt.

Nachdem Sie ein Kennwort eingerichtet haben, ruft das Skript **clearProbeData.bat** bei jeder Ausführung das Datenbankkennwort als Argument ab.

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 **DiscoveryProbe.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\DiscoveryProbe.properties** hinzu.

appilog.agent.Probe.JMX.BasicAuth.Pwd

Beispiel:

```
appilog.agent.Probe.JMX.BasicAuth.User=admin
appilog.agent.Probe.JMX.BasicAuth.Pwd=-85,-9,-61,11,105,-93,-81,118
```

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

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

b Testen Sie das Ergebnis in einem Webbrowser.

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

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

Wichtig: 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:

- **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 Zertifikatsauthentifizierung" auf Seite 368.
- **Serverauthentifizierung**. Dieser Modus verwendet SSL und die Probe authentifiziert das UCMDB Server-Zertifikat. Weitere Informationen finden Sie unter "Aktivieren von SSL mit Serverauthentifizierung" auf Seite 374.

➤ **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.

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 Data Flow Probe-Trust Store bei der Nutzung von Serverauthentifizierung das UCMDB Server-Zertifikat enthalten).

Aktivieren der gegenseitigen 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.

Hinweis: In den folgenden Anweisungen wird der Key Store **cKeyStoreFile** als Probe-Key Store verwendet. Dabei handelt es sich um einen vordefinierten Client-Key Store der UCMDB-Installation. Weitere Informationen finden Sie unter "Standard-Key Store und -Trust Store von UCMDB und Data Flow Probe" auf Seite 383. Es wird jedoch empfohlen, dass Sie einen neuen, einzigartigen 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 380.

---

1 Stellen Sie sicher, dass sowohl UCMDB als auch die Data Flow Probe ausgeführt werden. Wenn die Probe im separaten Modus installiert wurde, beziehen sich diese Anweisungen auf das Probe Gateway.

2 Härten Sie den Data Flow Probe-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.

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 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 Kehren Sie zur Seite **Operations** zurück.

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 den Key Store, der als Probe-Key Store verwendet werden soll, an den folgenden Speicherort im Dateisystem der Data Flow Probe: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Hinweis:

- Wenn Sie einen neuen Key Store erstellt haben, verwenden Sie dessen Namen. Andernfalls verwenden Sie **cKeyStoreFile**.
- Wenn Sie den Standard-Client-Key Store (**cKeyStoreFile**) verwenden, fahren Sie mit Schritt 6 auf Seite 371 fort.

---

4 Exportieren Sie das Probe-Zertifikat aus dem Key Store.

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

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias clientcert -
keystore <pKeyStoreFile> -file
C:\HP\UCMDB\DataFlowProbe\conf\security\probe.cert
```

b Geben Sie das Key Store-Kennwort ein (**pKeyStorePass**).

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

5 Importieren Sie das exportierte Probe-Zertifikat in den UCMDB-Trust Store.

a Kopieren Sie auf dem UCMDB-Computer die erstellte Datei **probe.cert** 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
<sTrustStoreFile> -file C:\HP\UCMDB\UCMDBServer\conf\security\probe.cert -
alias probecert
```

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

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.

6 Exportieren Sie das UCMDB-Zertifikat aus dem Key Store.

a Führen Sie auf dem UCMDB-Computer den folgenden Befehl aus:

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

b Geben Sie das Key Store-Kennwort ein (**sKeyStorePass**).

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

7 Importieren Sie das exportierte UCMDB-Zertifikat in den Probe-Trust Store.

a Kopieren Sie auf dem Probe-Computer die erstellte Datei **server.cert** in das folgende Data Flow Probe-Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf\security**

b Führen Sie folgenden Befehl aus:

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

c Geben Sie das Kennwort für den Data Flow Probe-Trust Store ein (**pTrustStorePass**).

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.

8 Aktualisieren Sie die Probe-Datei **ssl.properties** im folgenden Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf\security**

a Definieren Sie den Key Store-Pfad in der Eigenschaft **javax.net.ssl.keyStore** (**pKeyStoreFile**). Informationen zu einer Einschränkung finden Sie unter "Einschränkung bei der gegenseitigen Authentifizierung" auf Seite 373.

b Definieren Sie das Key Store-Kennwort in der Eigenschaft **javax.net.ssl.keyStorePassword** (**pKeyStorePass** in verschlüsselter Form).

c Definieren Sie den Trust Store-Pfad in der Eigenschaft **javax.net.ssl.trustStore** (**pTrustStoreFile**).

d Definieren Sie das Trust Store-Kennwort in der Eigenschaft **javax.net.ssl.trustStorePassword** (**pTrustStorePass** in verschlüsselter Form).

Hinweis: Die Eigenschaften für das Key Store-Kennwort und das Trust Store-Kennwort sind verschlüsselt. Anweisungen zur Verschlüsselung finden Sie unter "Verschlüsseln der Kennwörter für den Key Store und Trust Store der Probe" auf Seite 381.

---

9 Aktualisieren Sie die Datei **DiscoveryProbe.properties** im folgenden Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf**.

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

b Aktualisieren Sie die Eigenschaft **serverPortHttps** in die relevante Portnummer, wie in Schritt 2 auf Seite 369 beschrieben.

10 Starten Sie den UCMDB Server und die Data Flow Probe neu.

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

So aktivieren Sie Serverauthentifizierung:

1. Stellen Sie sicher, dass sowohl UCMDB als auch die Data Flow Probe ausgeführt werden. Wenn die Probe im separaten Modus installiert wurde, beziehen sich diese Anweisungen auf das Probe Gateway.
2. Härten Sie den Data Flow Probe-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.

   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 HTTPS-Portnummer. Die Standardeinstellung lautet 8443 und sollte aktiviert sein.

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

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

      Die folgende Meldung wird angezeigt:

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

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

g Um den Confidential Manager-Connector dem Modus mit gegenseitiger Authentifizierung 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 Exportieren Sie das UCMDB-Zertifikat aus dem Key Store.

a Führen Sie auf dem UCMDB-Computer den folgenden Befehl aus:

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

b Geben Sie das Key Store-Kennwort ein (**sKeyStorePass**).

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

4 Importieren Sie das exportierte UCMDB-Zertifikat in den Probe-Trust Store.

a Kopieren Sie auf dem Probe-Computer die erstellte Datei **server.cert** in das folgende Data Flow Probe-Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf\security**

b Führen Sie folgenden Befehl aus:

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

c Geben Sie das Kennwort für den Data Flow Probe-Trust Store ein (**pTrustStorePass**).

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 Aktualisieren Sie die Probe-Datei **ssl.properties** im folgenden Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf\security**

a Definieren Sie den Trust Store-Pfad in der Eigenschaft **javax.net.ssl.trustStore** (**pTrustStoreFile**).

b Definieren Sie das Trust Store-Kennwort in der Eigenschaft **javax.net.ssl.trustStorePassword** (**pTrustStorePass** in verschlüsselter Form).

Hinweis: Die Eigenschaft für das Trust Store-Kennwort ist verschlüsselt. Anweisungen zur Verschlüsselung finden Sie unter "Verschlüsseln der Kennwörter für den Key Store und Trust Store der Probe" auf Seite 381.

---

6 Aktualisieren Sie die Datei **DiscoveryProbe.properties** im folgenden Verzeichnis: **C:\HP\UCMDB\DataFlowProbe\conf**

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

b Aktualisieren Sie die Eigenschaft **serverPortHttps** in die relevante Portnummer, wie in Schritt 2 auf Seite 374 beschrieben.

7 Starten Sie den UCMDB Server und die Data Flow Probe neu.

Aktivieren von Authentifizierung auf der Data Flow Probe mit HTTP-Standardauthentifizierung

---

Wichtig:

- Das Aktivieren von Authentifizierung auf der Data Flow Probe in Form der Standardauthentifizierung ist die am wenigsten geeignete Methode. Es wird empfohlen, dass Sie die gegenseitige Authentifizierung nutzen, die eine deutlich höhere Sicherheit gewährleistet (da sie Datenverschlüsselung und Zertifikatsauthentifizierung kombiniert). Weitere Informationen finden Sie unter "Aktivieren von SSL zwischen UCMDB Server und Data Flow Probe mit gegenseitiger Authentifizierung" auf Seite 367.
- Wenn SSL nicht aktiviert ist, werden Anmeldeinformationen als Klartext an UCMDB übermittelt.

So richten Sie die Standardauthentifizierung ein:

1. Suchen Sie die folgende Datei: **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**.
2. Entfernen Sie die Kommentarzeichen (#) aus den folgenden Eigenschaften und geben Sie die relevanten Anmeldeinformationen ein:

```
appilog.agent.Probe.BasicAuth.Realm=
appilog.agent.Probe.BasicAuth.User=
appilog.agent.Probe.BasicAuth.Pwd=
```

Die Anmeldeinformationen sollten mit denen übereinstimmen, die auf dem UCMDB-Server definiert wurden.

Verbinden der Data Flow Probe über einen Reverse-Proxy

Führen Sie die folgende Prozedur aus, um die Data Flow Probe über einen Reverse-Proxy zu verbinden.

Hinweis: Die gegenseitige Authentifizierung mit Verwendung von SSL zwischen dem UCMDB-Server und der Data Flow Probe wird nicht unterstützt, wenn die Verbindung über einen Reverse-Proxy hergestellt wird.

So konfigurieren Sie die Data Flow Probe für die Verwendung eines Reverse-Proxy:

1. Bearbeiten Sie die Datei **discoveryProbe.properties** (im Verzeichnis **C:\hp\UCMDB\DataFlowProbe\conf**).
2. Geben Sie für die Eigenschaft **serverName** die IP-Adresse oder den DNS-Namen des Reverse-Proxy-Servers an.
3. Geben Sie für die Eigenschaften **serverPort** und **serverPortHttps** die Ports des Reverse-Proxy-Servers an.
4. Speichern Sie die Datei.

Die folgende Proxy-Server-Konfiguration ist erforderlich, wenn nur Data Flow Probes über einen Reverse-Proxy mit HP Universal CMDB verbunden sind:

Anfragen für... auf dem Reverse-Proxy-Server	Proxy-Anfrage wird verarbeitet von:
/mam-collectors	http://[HP Universal CMDB Server]/mam-collectors

Die folgende Konfiguration ist erforderlich, wenn ein SOAP-Adapter für die Replizierung über einen Reverse-Proxy auf eine sichere (gehärtete) HP Universal CMDB verwendet wird:

Anfragen für... auf dem Reverse-Proxy-Server	Proxy-Anfrage wird verarbeitet von:
/axis2	http://[HP Universal CMDB Server]/axis2

Verbinden von Data Flow Probes und Webclients über einen Reverse-Proxy

Die folgende Konfiguration ist erforderlich, wenn sowohl Data Flow Probes als auch Applikationsbenutzer über einen Reverse-Proxy mit HP Universal CMDB verbunden werden:

Anfragen für... auf dem Reverse-Proxy-Server	Proxy-Anfrage wird verarbeitet von:
/mam	[HP Universal CMDB Server]/mam
/mam_images	[HP Universal CMDB Server]/mam_images
/mam-collectors	[HP Universal CMDB Server]/mam-collectors
/ucmdb	[HP Universal CMDB Server]/ucmdb
/site	[HP Universal CMDB Server]/site

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\DiscoveryProbe.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 329.

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**.

Referenz

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

Dieser Abschnitt umfasst die folgenden Themen:

UCMDB

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**.			

23

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

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Referenz

Konzepte

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 Anwendungen innerhalb der konfigurierten Gruppe von Softwaresystemen vertrauen der Authentifizierung und bei einem Wechsel zwischen den Anwendungen ist keine weitere Authentifizierung erforderlich.

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

Dieser Abschnitt umfasst die folgenden Themen:

Ablauf des LW-SSO-Tokens

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

Empfohlene Konfiguration für den Ablauf des LW-SSO-Tokens

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

GMT-Zeit

Alle Anwendungen, 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.

Referenz

Systemanforderungen für LW-SSO

In der folgenden Tabelle sind die LW-SSO-Konfigurationsanforderungen aufgeführt:

Anwendung	Version	Kommentare
Java	1.5 oder höher	
HTTP-Servlets-API	2.1 oder höher	
Internet Explorer	6.0 oder höher	Der Browser sollte HTTP-Sitzungscookies und die HTTP-302-Weiterleitungsfunktion unterstützen.
FireFox	2.0 oder 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	

Anwendung	Version	Kommentare
Spring Security-Authentifizierung	Spring Security 2.0.4	
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 Anwendung erstellt ein Token und jede Anwendung, die denselben initString-Parameter verwendet, überprüft das Token.

Vorsicht:

- 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 Anwendungen 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 Anwendung, die das schwächste Authentifizierungsframework verwendet und ein LW-SSO-Token ausgibt, dem von anderen integrierten Anwendungen vertraut wird, bestimmt die Ebene Authentifizierungssicherheit für alle Anwendungen.

  Nur Anwendungen, 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 Anwendung, die LW-SSO verwendet, ein Token ausgeben, dem alle anderen Anwendungen vertrauen, die denselben **initString**-Parameter aufweisen. Dieses potenzielle Risiko spielt eine Rolle, wenn sich eine Anwendung, die einen gemeinsamen initString-Parameter verwendet, an einem nicht vertrauenswürdigen Speicherort befindet oder von dort darauf zugegriffen werden kann.
- **Benutzerzuordnung (Synchronisation).** Das LW-SSO-Framework stellt nicht sicher, dass die Benutzerzuordnung zwischen den integrierten Anwendungen erfolgt. Aus diesem Grund muss die integrierte Anwendung die Benutzerzuordnung überwachen. Es empfiehlt sich, für alle integrierten Anwendungen denselben Benutzerregistrierungseintrag (wie LDAP/AD) freizugeben.

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

Darüber hinaus kann in Fällen, in denen sich ein Benutzer bei einer Annwendung (AppA) anmeldet und auf eine zweite Anwendung (AppB) zugreift, die Benutzercontainer oder Anwendungsauthentifizierung 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 Anwendung (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

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 Anwendung 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 Anwendungsumleitungsbefehle beim Abmeldeverfahren zu verringern, sofern möglich.

Einschränkungen

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

- **Clientzugriff auf die Anwendung**.

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

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

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

- **LW-SSO-Framework-Integration.** Anwendungen 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 Anwendungen und bietet keine Unterstützung für die Eingabe eines URLs in ein Browserfenster, sofern sich nicht beide Anwendungen 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 Anwendung nicht (nur die **HTTP GET**-Anforderung wird unterstützt). Wenn Ihre Anwendung beispielsweise einen HTTP-Link zu einer zweiten Anwendung 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 Anwendung in einer Domäne in eine andere Anwendung 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 Zone für Intranet/Vertrauenswürdige Sites auf Ihrem Computer hinzu (wechseln Sie in Microsoft Internet Explorer zu **Extras** > **Internetoptionen** > **Sicherheit** > **Lokales Intranet** > **Sites** > **Erweitert**). Die Cookies werden daraufhin akzeptiert.

Vorsicht: 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 Anwendung bei der Abmeldung von der ersten Anwendung nicht von der zweiten Anwendung abgemeldet.
  - Der Ablauf des SAML2-Tokens spiegelt sich nicht in der Sitzungsverwaltung der Anwendung wider.

    Entsprechend erfolgt, wenn das SAML2-Token für den Zugriff auf eine zweite Anwendung verwendet wird, die Sitzungsverwaltung für jede Anwendung 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, unterstützt aber nicht die Eingabe eines URL in einem Browserfenster, da in diesem Fall die HTTP-Referrerkopfzeile fehlt.

24

Authentifizierung bei der Anmeldung in HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Einrichten einer Authentifizierungsmethode

Zum Durchführen von Authentifizierung können Sie wie folgt vorgehen:

- **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 unter "LDAP-Zuordnung" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

  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 (dies ist standardmäßig der Fall), 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.

Aufgaben

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. Speichern Sie die neuen Werte. Um einen Eintrag durch den Standardwert zu ersetzen, klicken Sie auf **Standardeinstellung**.

8 Ordnen Sie LDAP-Benutzergruppen zu UCMDB-Benutzerrollen zu. Weitere Informationen finden Sie unter "Authentifizierung bei der Anmeldung in HP Universal CMDB" auf Seite 397.

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 400.

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. Diese Zertifizierungsstelle ist in der Java Runtime-Umgebung enthalten.

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 möglicherweise zu den vertrauenswürdigen Zertifizierungsstellen in Java hinzufügen.

Weitere Informationen zum Konfigurieren der HP Universal CMDB-Plattform für die Kommunikation über SSL finden Sie unter "Aktivieren der SSL-Kommunikation" auf Seite 305.

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 Seite 402.

---

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 der Anmeldung in HP Universal CMDB mit LW-SSO

Verwenden Sie zum Aktivieren von LW-SSO für HP Universal CMDB eine der folgenden Prozeduren:

Aktivieren von LW-SSO über die JMX-Konsole

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**. Legen Sie zusätzliche LW-SSO-Konfigurationsparameter mit den jeweiligen Methoden fest. Weitere Informationen zu zusätzlichen Parametern finden Sie unter "LW-SSO-Authentifizierung – Übersicht" auf Seite 386.
7. Um die LW-SSO-Konfiguration so anzuzeigen, wie sie im Einstellungsmechanismus gespeichert ist, rufen Sie die Methode **retrieveConfigurationFromSettings** auf.
8. Um die tatsächlich geladene LW-SSO-Konfiguration anzuzeigen, rufen Sie die Methode **retrieveConfiguration** auf.

Aktivieren von LW-SSO über die UCMDB-Infrastruktureinstellungen

1. Melden Sie sich in HP Universal CMDB an.
2. Wählen Sie die Kategorie **Verwaltung** > **Infrastructure Settings Manager** > **Allgemeine Einstellungen** aus.

3 Geben Sie für die Optionen **LW-SSO-Domäne** und **LW-SSO-Init-Zeichenkette** den Domänennamen bzw. den Wert des initString-Parameters ein.

4 Ändern Sie **LW-SSO-Aktivierungs-Status** in **True**.

5 Optional. Legen Sie zusätzliche LW-SSO-Konfigurationsparameter über die jeweiligen Einstellungseinträge fest. Weitere Informationen zu zusätzlichen Parametern finden Sie unter "LW-SSO-Authentifizierung – Übersicht" auf Seite 386.

6 Starten Sie den Server neu.

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.

25

Confidential Manager

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Referenz

Konzepte

Confidential Manager – Übersicht

Der Confidential Manager (CM) 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.

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

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

CM verschlüsselt Anmeldeinformationen während der Übertragung, im Client-Cache, im persistenten Speicher und im Arbeitsspeicher. CM verwendet symmetrische Kryptographie für die Übertragung von Anmeldeinformationen zwischen dem CM-Client und dem CM-Server und nutzt dabei einen gemeinsamen geheimen Schlüssel. CM 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 329.

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 414. Durch diese Parametereinstellung steigt jedoch die Größe der Datenbank an.
- Um Provider für hohe Kundensicherheit zu nutzen, können Sie den JCE-Modus verwenden.

Aufgaben

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://<UCMDB Server-Hostname oder -IP>:8080/jmx-console**.

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

2. Klicken Sie unter UCMDB auf **UCMDB:service=Server 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 CM-Serverkonfiguration 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 414 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**. In der Standardeinstellung sind alle Kunden ausgewählt.

- **resource**. Der Ressourcenname. In der Standardeinstellung ist der Stammordner ausgewählt.
- **permission**. Wählen Sie zwischen allen Berechtigungen, Erstellen, Lesen, Aktualisieren und Löschen 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 wie der UCMDB Server ausgeführt wird und daher keine Krypto-Konfiguration für die Übertragung erfordert.)
- Die CM-Replizierung ist standardmäßig nicht konfiguriert, kann aber bei Bedarf konfiguriert werden.
- Wird die CM-Replizierung aktiviert und die Übertragungseinstellung **initString** oder eine andere Krypto-Eigenschaft des Master geändert, müssen die Änderungen auch für alle Slaves durchgeführt werden.

Referenz

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 CM 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 CM-Serverkonfiguration hat den folgenden Namen: **CM_CONFIGURATION**.
- Die Standardkonfigurationsdatei des CM-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 410.

Parameter	Beschreibung	Empfohlener Wert
encryptTransportMode	Verschlüsselung der übertragenen Daten: ➤ true ➤ false	true
encryptDecryptInitString	Kennwort für die Verschlüsselung	Länger als 8 Zeichen
cryptoSource	Bibliothek für die Umsetzung der Verschlüsselung: ➤ lw ➤ jce ➤ windowsDPAPI ➤ lwJCECompatible	lw
lwJCEPBECompatibilityMode	Unterstützung für schwache Kryptographie vorheriger Versionen: ➤ true ➤ false	true
cipherType	Der Verschlüsselungstyp, den CM verwendet. CM unterstützt nur einen Wert: **symmetricBlockCipher**	symmetric BlockCipher

Parameter	Beschreibung	Empfohlener Wert
engineName	➤ AES ➤ Blowfish ➤ DES ➤ 3DES ➤ Null (keine Verschlüsselung)	AES
algorithmModeName	Modus des Blockverschlüsselungsalgorithmus: ➤ CBC	CBC
algorithmPaddingName	Auffüllstandards: ➤ PKCS7Padding ➤ PKCS5Padding	PKCS7Padding
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

Parameter	Beschreibung	Empfohlener Wert
useMacWithCrypto	Bestimmt, ob MAC mit der Kryptographie verwendet wird: ➤ true ➤ false	false
macType	Typ des Message Authentication Code (MAC): ➤ hmac	hmac
macKeySize	Abhängig vom MAC-Algorithmus	256
macHashName	Der Hash-MAC-Algorithmus: ➤ SHA256	SHA256

Teil VII

Notfallwiederherstellung

26

Einrichten der Notfallwiederherstellung

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Notfallwiederherstellung – Übersicht

Im Folgenden werden die Grundsätze und Richtlinien für das Einrichten eines Notfallwiederherstellungssystems beschrieben. Außerdem werden die erforderlichen Schritte erklärt, durch die ein sekundäres HP Universal CMDB-System zum neuen primären System wird. Dieser Abschnitt gilt für eine typische HP Universal CMDB-Umgebung mit einem HP Universal CMDB Server und einem Datenbankserver, der HP Universal CMDB-Datenbankschemas enthält.

Hinweis:

- In diesem Abschnitt erhalten Sie einen allgemeinen Überblick über die Konzepte zum Einrichten einer Notfallwiederherstellung.
- Die Notfallwiederherstellung beinhaltet manuelle Schritte, durch die verschiedene Konfigurationsdateien und Aktualisierungen in die HP Universal CMDB-Datenbankschemas verschoben werden. Diese Prozedur erfordert mindestens einen HP Universal CMDB-Administrator und einen Datenbankadministrator, der sich mit den HP Universal CMDB-Datenbanken und -Schemas auskennt.
- Für HP Universal CMDB gibt es eine Reihe unterschiedlicher Bereitstellungen und Konfigurationen. Um sicherzustellen, dass das Notfallwiederherstellungsszenario in einer bestimmten Umgebung funktioniert, muss es gründlich getestet und dokumentiert werden. Wenden Sie sich an HP Professional Services, um geeignete Best Practices für den Entwurf und den Ausfallsicherungs-Workflow des Notfallwiederherstellungsszenarios zu bestimmen.

Aufgaben

Vorbereiten der Notfallwiederherstellungsumgebung

Die Vorbereitung der Notfallwiederherstellungsumgebung umfasst die folgenden Phasen:

- "Installieren der HP Universal CMDB-Software in der Ausfallsicherungsumgebung" auf Seite 421
- "Konfigurieren der System- und Datensicherung" auf Seite 422

Installieren der HP Universal CMDB-Software in der Ausfallsicherungsumgebung

Installieren Sie eine zweite Instanz von HP Universal CMDB, die mit der aktuellen Produktionsumgebung übereinstimmt.

- Installieren Sie exakt dieselbe Version von HP Universal CMDB in Ihrer Sicherungsumgebung wie in Ihrer Produktionsumgebung.
- Um Probleme mit abweichenden Kapazitäten und Bereitstellungen zu vermeiden, sollte die Sicherungsumgebung genau der Produktionsumgebung entsprechen.
- Führen Sie nicht das Dienstprogramm für die Server- und Datenbankkonfiguration aus und erstellen Sie keine Datenbanken.
- Starten Sie nicht das Sicherungssystem.

Hinweis: Die Notfallwiederherstellungsumgebung sollte der HP Universal CMDB-Produktionsumgebung möglichst ähnlich sein. Hardware, Bereitstellung und Versionen sollten abgestimmt sein, um einen Funktionsverlust bei der Umstellung auf das Ausfallsicherungssystem zu vermeiden.

Konfigurieren der System- und Datensicherung

In dieser Phase kopieren Sie die Konfigurationsverzeichnisse in die Ausfallsicherungsinstanz und konfigurieren den Datenbankprotokollversand.

Kopieren der Konfigurationsverzeichnisse in die Ausfallsicherungsinstanz

Kopieren Sie alle Dateien, die in den folgenden Verzeichnissen geändert wurden, aus der HP Universal CMDB-Produktionsinstanz auf denselben Servertyp in der Ausfallsicherungsinstanz:

- UCMDBServer\conf
- UCMDBServer\content\

Kopieren Sie auch alle anderen Dateien oder Verzeichnisse im System, die angepasst wurden.

Hinweis: Es wird empfohlen, dass Sie mindestens täglich eine Sicherung der HP Universal CMDB Server vornehmen. Je nach Anzahl und Häufigkeit der Konfigurationsänderungen sollten Sie eventuell ein kürzeres Intervall wählen, um einen größeren Verlust von Konfigurationsänderungen zu vermeiden, falls die Produktionsinstanz ausfällt.

Microsoft SQL Server – Konfigurieren des Datenbankprotokollversands

Damit immer die neuesten Überwachungs- und Konfigurationsdaten verfügbar sind, müssen Sie den Protokollversand aktivieren, um die Zeitdauer von Datenlücken zu minimieren. Durch den Protokollversand können Sie eine exakte Kopie der ursprünglichen Datenbank erstellen, die nur aufgrund der Zeitverzögerung durch den Kopier- und Ladevorgang nicht ganz aktuell ist. Anschließend können Sie den Standby-Datenbankserver als neuen primären Datenbankserver nutzen, wenn der ursprüngliche primäre Datenbankserver ausfällt. Wenn der ursprüngliche primäre Server wieder verfügbar ist, können Sie ihn als neuen Standby-Server verwenden, d. h. die Serverrollen umkehren.

Der Protokollversand muss für die folgenden HP Universal CMDB-Datenbanken konfiguriert werden:

- HP Universal CMDB-Datenbank
- HP Universal CMDB History-Datenbank

Die einzelnen Schritte zum Konfigurieren des Protokollversands werden in diesem Abschnitt nicht beschrieben. Der HP Universal CMDB-Datenbankadministrator kann die folgenden Links nutzen, um den Protokollversand für die jeweilige Version der Datenbanksoftware zu konfigurieren, die in der HP Universal CMDB-Umgebung verwendet wird:

Microsoft SQL Server 2000:

- support.microsoft.com/default.aspx?scid=http://support.microsoft.com/support/sql/content/2000papers/LogShippingFinal.asp
- www.microsoft.com/technet/prodtechnol/sql/2000/maintain/logship1.mspx

Microsoft SQL Server 2005:

- msdn2.microsoft.com/en-us/library/ms188625.aspx
- msdn2.microsoft.com/en-us/library/ms190016.aspx
- msdn2.microsoft.com/en-us/library/ms187016.aspx

Oracle – Konfigurieren der Standby-Datenbank (Data Guard)

Oracle stellt Protokolle nur auf der Datenbankebene bereit und nicht für jedes Schema. Dies bedeutet, dass Sie keine Standby-Datenbank auf Schemaebene einrichten können und stattdessen Kopien der Produktionssystemdatenbanken auf dem Sicherungssystem erstellen müssen.

Hinweis: HP empfiehlt, Oracle 11i als Oracle-Datenbankplattform zu verwenden, damit Data Guard genutzt werden kann.

Die einzelnen Schritte zum Konfigurieren einer Standby-Datenbank werden in diesem Abschnitt nicht beschrieben. Der HP Universal CMDB-Datenbankadministrator kann den folgenden Link verwenden, um eine Standby-Datenbank für Oracle 11i zu konfigurieren:

http://download.oracle.com/docs/cd/B19306_01/server.102/b14239/toc.htm

Nach der erfolgreichen Konfiguration der Sicherungsdatenbank sollte die HP Universal CMDB-Ausfallsicherungsdatenbank mit der HP Universal CMDB-Produktionsdatenbank synchronisiert werden.

Vorbereiten der HP Universal CMDB-Ausfallsicherungsinstanz auf die Aktivierung

Wenn die Aktivierung der Ausfallsicherungsinstanz bevorsteht, führen Sie in der Ausfallsicherungsumgebung die folgenden Schritte durch:

- Aktivieren Sie das Sicherungssystem, einschließlich der Datenbank.
- Stellen Sie sicher, dass die neuesten Datenbankprotokolle in den Datenbanken der Ausfallsicherungsumgebung aktualisiert wurden.
- Führen Sie die Bereinigungsprozedur beim Starten aus, um alle Lokalisierungen in den Datenbanken zu entfernen. Weitere Informationen finden Sie unter "Ausführen der Bereinigungsprozedur beim Starten" auf Seite 425.

Ausführen der Bereinigungsprozedur beim Starten

Durch diese Prozedur werden alle computereigenen Referenzen in den Konfigurationen aus der Produktionsinstanz entfernt. Dies ist erforderlich, um die Datenbank auf dem Sicherungssystem zurückzusetzen.

Hinweis:

- Vor dem Starten der Aktivierungsprozeduren sollte der HP Universal CMDB-Administrator sicherstellen, dass die richtige Lizenz auf die Ausfallsicherungsinstanz angewendet wurde.
- HP empfiehlt, dass ein erfahrener Datenbankadministrator die SQL-Anweisungen dieser Prozedur ausführt.

---

1 Leeren und Aktualisieren der Tabellen:

```
update CUSTOMER_REGISTRATION set CLUSTER_ID=null;
truncate table CLUSTER_SERVER;
truncate table SERVER;
truncate table CLUSTERS;
```

2 Ausführen des Dienstprogramms für die Server- und Datenbankkonfiguration.

Führen Sie das Dienstprogramm für die Server- und Datenbankkonfiguration auf jedem Computer aus, um die erforderlichen Tabellen in der Datenbank wieder zu initialisieren. Zum Ausführen des Dienstprogramms für die Server- und Datenbankkonfiguration wählen Sie **Start** > **Alle Programme** > **HP UCMDB** > **Konfigurationsassistenten für HP Universal CMDB starten** aus.

Hinweis:

- Stellen Sie beim Ausführen des Dienstprogramms für die Server- und Datenbankkonfiguration sicher, dass Sie wieder eine Verbindung zu denselben Datenbanken herstellen, die für die Ausfallsicherungsumgebung erstellt wurden (d. h. in die die Sicherungsdaten gesendet wurden). Wenn Sie das Dienstprogramm auf der Produktionsinstanz ausführen, gehen möglicherweise alle Konfigurationsdaten verloren.
- Wenn Sie aufgefordert werden, im Dienstprogramm für die Server- und Datenbankkonfiguration die Datenbanken anzugeben, stellen Sie sicher, dass Sie die Namen der neuen Datenbanken in der Ausfallsicherungsumgebung eingeben.

3 Starten der Server.

Zum Ausführen der Notfallwiederherstellung auf einem Hochverfügbarkeitssystem starten Sie einen der HP Universal CMDB Server, konfigurieren Sie auf diesem Server mit dem Systemkonfigurations-Tool ein Cluster und fügen Sie neue Ausfallsicherungsserver zu diesem Cluster hinzu.

4 Hochfahren der Sicherungsumgebung.

Starten Sie HP Universal CMDB in der Ausfallsicherungsumgebung.

Teil VIII

Erste Schritte in HP Universal CMDB

27

Zugreifen auf HP Universal CMDB über den IIS-Webserver

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Zugreifen auf HP Universal CMDB über IIS – Übersicht

Im Folgenden wird beschrieben, wie Sie über den Microsoft IIS-Webserver (Internet Information Services) auf HP Universal CMDB zugreifen.

Sie können den IIS-Webserver so einrichten, dass Endbenutzer und Clients von HP Universal CMDB (beispielsweise die Data Flow Probe) über den IIS-Webserver auf das System zugreifen können. Durch diese Konfiguration verwenden Endbenutzer und Clients von HP Universal CMDB den URL des IIS-Computers für den Zugriff auf UCMDB und nicht den URL des UCMDB-Computers.

Dieser Abschnitt umfasst die folgenden Themen:

➤ "Erforderliche Software für die Integration" auf Seite 430

➤ "Unterstützte Konfigurationen" auf Seite 430

Erforderliche Software für die Integration

In der folgenden Tabelle ist die erforderliche Software für die Integration aufgeführt:

IIS Web Server	Version 6.0, 7.X
HP Universal CMDB Server	Version 9.02 oder höher

Unterstützte Konfigurationen

Die folgenden Konfigurationen werden für diese Integration unterstützt:

➤ Windows 2003/8 64-Bit, HP Universal CMDB 9.02 oder höher und IIS 6 oder 7.X auf **demselben** Server.

➤ Windows 2003/8 64-Bit, HP Universal CMDB 9.02 oder höher und IIS 6 oder 7.X auf **separaten** Servern.

Aufgaben

Einrichten von IIS für den Zugriff auf UCMDB – Windows 2003

In diesem Abschnitt wird die Prozedur für die Integration von HP Universal CMDB und IIS unter Windows 2003 beschrieben.

So integrieren Sie HP Universal CMDB und IIS manuell:

1 Wenn sich der HP Universal CMDB Server nicht auf demselben Computer wie IIS befindet, kopieren Sie alle Dateien aus dem Verzeichnis **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** in den Ordner **c:\ucmdb_iis** auf dem IIS-Computer. Ändern Sie auf dem IIS-Computer die folgenden Dateien:

a Ändern Sie in der Datei **workers.properties.minimal** die Zeichenkette **worker.localAjp.host=localhost** in den UCMDB Server-Hostnamen.

b In der Datei **isapi_redirect.properties**:

➤ Die Einstellung **log_file** muss auf den Ordner mit den Integrationsprotokollen verweisen, z. B. **c:\ucmdb_iis\isapi.log**.

➤ Die Einstellung **worker_file** muss den Speicherort der Datei **workers.properties.minimal** enthalten, z. B. **C:\ucmdb_iis\workers.properties.minimal**.

➤ Die Einstellung **worker_mount_file** muss den Speicherort der Datei **uriworkermap.properties** enthalten, z. B. **C:mdb_iis\uriworkermap.properties**.

2 Wenn sich der HP Universal CMDB Server auf demselben Computer wie IIS befindet, ändern Sie die Datei **isapi_redirect.properties** im Verzeichnis **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** wie folgt:

a Die Einstellung **log_file** muss auf den Ordner mit den Integrationsprotokollen verweisen, z. B. **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.

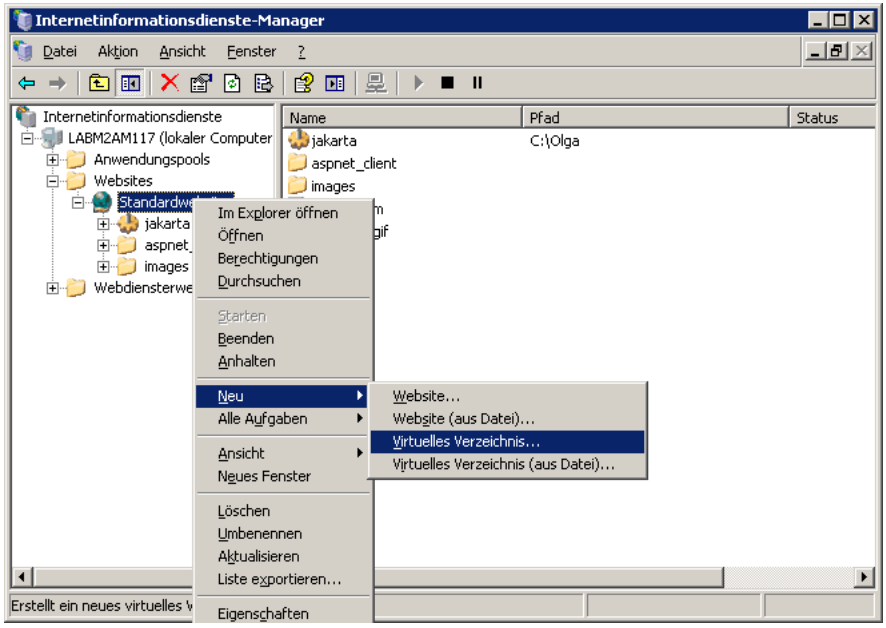
b Die Einstellung **worker_file** muss den Speicherort der Datei **workers.properties.minimal** enthalten, z. B. **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\workers.properties.minimal**.

c Die Einstellung **worker_mount_file** muss den Speicherort der Datei **uriworkermap.properties** enthalten, z. B. **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.properties**.

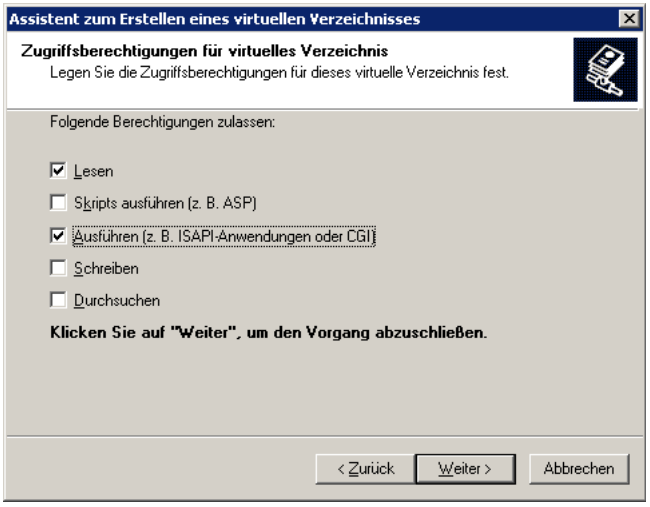
3 Ändern Sie die Zeichenkette **worker.localAjp.host=localhost** in den UCMDB Server-Hostnamen (wenn sich der HP Universal CMDB Server nicht auf demselben Computer wie IIS befindet).

4 Öffnen Sie die IIS-Verwaltungskonsole. Führen Sie **inetmgr** über die Befehlszeile aus.

5 Fügen Sie ein neues virtuelles Verzeichnis zu Ihrer IIS-Website für **Windows 2003/IIS6** hinzu:



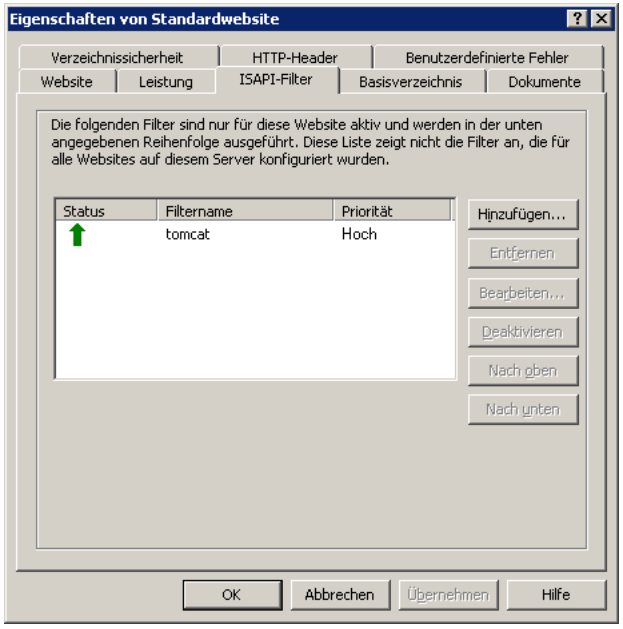
6 Der Assistent für das Erstellen eines virtuellen Verzeichnisses wird angezeigt. Der Alias des virtuellen Verzeichnisses muss **jakarta** lauten. Der physische Pfad muss **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** lauten. Wenn der UCMDB Server und der IIS-Server auf separaten Computern ausgeführt werden, muss der Pfad dem Verzeichnis auf dem IIS-Computer entsprechen. Erlauben Sie einen Zugriff vom Typ **Ausführen** auf das neue virtuelle Verzeichnis:



7 Öffnen Sie das Dialogfeld mit den Eigenschaften der Standardwebsite und fügen Sie **isapi_redirect.dll** als ISAPI-Filter zu Ihrer IIS-Website hinzu. Der Name des Filters sollte seiner Aufgabe entsprechen (z. B. **tomcat**) und die ausführbare Datei muss **isapi_redirect.dll** lauten. Wenn der UCMDB Server und der IIS-Server auf separaten Computern ausgeführt werden, muss als ausführbare Datei **isapi_redirect.dll** in dem Verzeichnis festgelegt sein, in das Sie die Datei auf dem IIS-Computer kopiert haben.

8 Öffnen Sie **Webdiensterweiterungen**, wählen Sie **Alle unbekannten ISAPI-Erweiterungen** aus der Liste aus und klicken Sie auf **Zulassen**.

9 Starten Sie IIS neu (durch Anhalten und Starten des IIS-Services) und stellen Sie sicher, dass der Filter **tomcat** mit einem grünen Pfeil nach oben markiert ist:



Einrichten von IIS für den Zugriff auf UCMDB – Windows 2008

In diesem Abschnitt wird die Prozedur für die Integration von HP Universal CMDB und IIS unter Windows 2008 beschrieben.

So integrieren Sie HP Universal CMDB und IIS manuell:

1 Wenn sich der HP Universal CMDB Server nicht auf demselben Computer wie IIS befindet, kopieren Sie alle Dateien aus dem Verzeichnis **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** in den Ordner **c:\ucmdb_iis** auf dem IIS-Computer. Ändern Sie auf dem IIS-Computer die folgenden Dateien:

a Ändern Sie in der Datei **workers.properties.minimal** die Zeichenkette **worker.localAjp.host=localhost** in den UCMDB Server-Hostnamen.

b In der Datei **isapi_redirect.properties**:

- Die Einstellung **log_file** muss auf den Ordner mit den Integrationsprotokollen verweisen, z. B. **c:\ucmdb_iis\isapi.log**.
- Die Einstellung **worker_file** muss den Speicherort der Datei **workers.properties.minimal** enthalten, z. B. **C:\ucmdb_iis\workers.properties.minimal**.
- Die Einstellung **worker_mount_file** muss den Speicherort der Datei **uriworkermap.properties** enthalten, z. B. **C:mdb_iis\uriworkermap.properties**.

2 Wenn sich der HP Universal CMDB Server auf demselben Computer wie IIS befindet, ändern Sie die Datei **isapi_redirect.properties** im Verzeichnis **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** wie folgt:

a Die Einstellung **log_file** muss auf den Ordner mit den Integrationsprotokollen verweisen, z. B. **C:\hp\UCMDB\UCMDBServer\runtime\log\isapi.log**.

b Die Einstellung **worker_file** muss den Speicherort der Datei **workers.properties.minimal** enthalten, z. B. **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\workers.properties.minimal**.

c Die Einstellung **worker_mount_file** muss den Speicherort der Datei **uriworkermap.properties** enthalten, z. B. **C:\hp\UCMDB\UCMDBServer\tools\iis_integration\uriworkermap.properties**.

3 Ändern Sie die Zeichenkette **worker.localAjp.host=localhost** in den UCMDB Server-Hostnamen (wenn sich der HP Universal CMDB Server nicht auf demselben Computer wie IIS befindet).

4 Öffnen Sie die IIS-Verwaltungskonsole. Führen Sie **inetmgr** über die Befehlszeile aus.

5 Doppelklicken Sie auf **ISAPI**-Filter.

6 Klicken Sie im Hauptfenster der IIS-Verwaltungskonsole mit der rechten Maustaste und wählen Sie **Hinzufügen** aus.

7 Fügen Sie **isapi_redirect.dll** als ISAPI-Filter zu Ihrer IIS-Website hinzu. Der Name des Filters sollte seiner Aufgabe entsprechen (z. B. **tomcat**) und die ausführbare Datei muss **isapi_redirect.dll** lauten. Wenn der UCMDB Server und der IIS-Server auf separaten Computern ausgeführt werden, muss als ausführbare Datei **isapi_redirect.dll** in dem Verzeichnis festgelegt sein, in das Sie die Datei auf dem IIS-Computer kopiert haben.

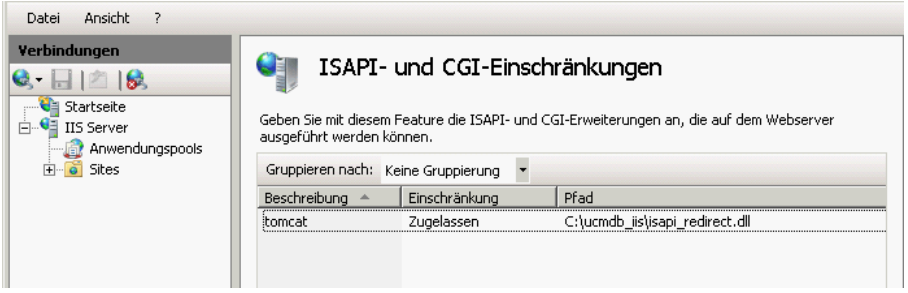
8 Fügen Sie ein neues virtuelles Verzeichnis zu Ihrer IIS-Website hinzu. Der Alias des virtuellen Verzeichnisses muss **jakarta** lauten. Das virtuelle Verzeichnis muss auf **C:\hp\UCMDB\UCMDBServer\tools\iis_integration** verweisen (wenn sich der Ordner auf demselben Server wie UCMDB befindet) oder auf das Verzeichnis, in das **iis_integration** kopiert wurde, falls es sich auf einem anderen Server befindet.

9 Wählen Sie im Ausschnitt **Verbindungen** den Namen des IIS-Servers aus.

10 Doppelklicken Sie auf **ISAPI- und CGI-Einschränkungen**.

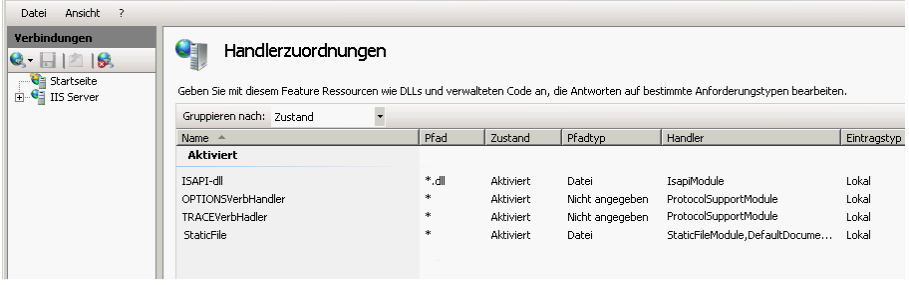
11 Klicken Sie mit der rechten Maustaste und geben Sie dieselben Informationen ein, die Sie zuvor in Schritt 7 hinzugefügt haben.

12 Aktivieren Sie das Kontrollkästchen, damit der **Pfad** ausgeführt werden kann.



13 Öffnen Sie **Handlerzuordnungen**.

14 Wählen Sie **ISAPI-DLL** aus. Klicken Sie mit der rechten Maustaste und wählen Sie **Featureberechtigungen bearbeiten** aus. Klicken Sie auf **Ausführen**.



15 Starten Sie IIS neu.

16 Rufen Sie in UCMDB die Infrastruktureinstellungen auf (**Verwaltung> Infrastructure Settings Manager > Allgemeine Einstellungen**). Ändern Sie die Option **AJP-Verbindungen aktivieren** in **True** und starten Sie den UCMDB Server neu.

Fehlerbehebung und Einschränkungen

Sie können die JMX-Konsole nicht über IIS öffnen. Dies bedeutet, dass die Standardauthentifizierung von Jetty nicht übergeben werden kann.

Konfigurieren der Data Flow Probe

Ändern Sie zum Konfigurieren der Data Flow Probe die folgenden Zeichenketten in der folgenden Datei: **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**:

- serverName = <IIS-Hostname>
- serverPort = <IIS-HTTP-Port>, Standardeinstellung 80

Nun kann der IIS-URL (beispielsweise **http://<IIS-Hostname>/ucmdb**) für den Zugriff auf UCMDB, die JMX-Konsole, das UCMDB SDK usw. verwendet werden.

28

Zugreifen auf HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Aufgaben

Konzepte

Zugreifen auf HP Universal CMDB – Übersicht

Sie greifen auf HP Universal CMDB mithilfe eines unterstützten Webbrowsers von einem beliebigen Computer mit einer Netzwerkverbindung (Intranet oder Internet) zum HP Universal CMDB Server zu. Die jeweilige Zugriffsebene für einen Benutzer hängt von seinen Berechtigungen ab. Weitere Informationen zum Gewähren von Benutzerberechtigungen finden Sie unter "Einrichten von Benutzern" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Weitere Informationen zu den Webbrowseranforderungen sowie den Mindestanforderungen zum Anzeigen von HP Universal CMDB finden Sie unter "HP Universal CMDB – Unterstützungsmatrix" auf Seite 35.

Weitere Informationen zum sicheren Zugriff auf HP Universal CMDB finden Sie in Teil VI, "Härten von HP Universal CMDB".

Informationen zu den Strategien für die Anmeldeauthentifizierung, die Sie in HP Universal CMDB verwenden können, finden Sie unter "Einrichten einer Authentifizierungsmethode" auf Seite 398.

Informationen zur Fehlerbehebung bei der Anmeldung finden Sie unter "Fehlerbehebung bei der Anmeldung" auf Seite 47.

Tipp: Klicken Sie auf der Anmeldeseite auf die Schaltfläche **Hilfe**, um ausführliche Hilfe zur Anmeldung abzurufen.

Lokaler Installationsmodus

Im lokalen Installationsmodus wird UCMDB so geladen, dass die Ladezeit für das Applet deutlich kürzer ausfällt. Im lokalen Installationsmodus werden die Applet-Dateien (JAR-Dateien) in ein lokales Verzeichnis mit dem Namen **UcmdbAppletJars** geladen, das sich unter dem temporären Verzeichnis der Umgebung befindet. Die Klassen werden mithilfe eines angepassten Klassenladeprogramms geladen, das schneller arbeitet, aber nicht die Signatur der signierten JAR-Dateien überprüft. Daher wird der lokale Installationsmodus als unsicherer Modus betrachtet.

Aktivieren Sie zum Auswählen des lokalen Installationsmodus das Kontrollkästchen **Lokalen Installationsmodus aktivieren** auf dem Anmeldebildschirm. Dieses Kontrollkästchen wird nur angezeigt, wenn Sie im Infrastructure Settings Manager für die Einstellung **Erlaubnis für lokalen Installationsmodus** den Wert **True** festgelegt haben. Sie können den Standardstatus des Kontrollkästchens über die Einstellung **Anfangsstatus für lokalen Installationsmodus** festlegen. Wenn die Einstellung den Wert **True** aufweist, ist das Kontrollkästchen standardmäßig aktiviert. Wenn die Einstellung den Wert **False** aufweist, ist das Kontrollkästchen standardmäßig deaktiviert.

Hinweis: Wenn Sie das Kontrollkästchen **Anmeldedaten auf diesem Computer speichern** bei der Anmeldung aktivieren, weist das Kontrollkästchen **Lokalen Installationsmodus aktivieren** bei der nächsten Anmeldung denselben Status auf, unabhängig von der Infrastruktureinstellung.

Für HP Software-as-a-Service-Kunden werden die Installationseinstellungen pro Kunde vorgenommen.

Aufgaben

Zugreifen auf HP Universal CMDB und seine Komponenten

In diesem Abschnitt wird der Zugriff auf die HP Universal CMDB-Komponenten beschrieben.

1 Geben Sie im Webbrowser den URL für den HP Universal CMDB Server ein, beispielsweise **http://<Servername oder IP-Adresse>.<Domänenname>:8080**, wobei **<Servername oder IP-Adresse>.<Domänenname>** für den vollqualifizierten Domänennamen (FQDN) von HP Universal CMDB Server steht.

Wenn HP Universal CMDB für die Verwendung über einen Reverse-Proxy eingerichtet wurde, geben Sie **https://<Proxy_Server_Name>:443** ein, wobei **Proxy_Server_Name** für den Namen oder die IP-Adresse des Proxy-Servers steht.

Wenn auf Ihrem Computer nicht die richtige Java-Version installiert ist, können Sie die Version von sun.com oder vom UCMDB Server herunterladen. (Wenn Sie sich anmelden, ohne Java zu installieren, können Sie keine Seiten anzeigen, die nur mit einem Java-Applet ordnungsgemäß angezeigt werden.) Weitere Informationen finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 48.

2 Klicken Sie auf einen Link, um mit HP Universal CMDB zu arbeiten:

a **UCMDB Application**. Öffnet die Anmeldeseite. Weitere Informationen finden Sie unter "Anmelden bei HP Universal CMDB" auf Seite 445.

Hinweis: Sie können die Anmeldeseite auch aufrufen, indem Sie **http://<Servername oder IP-Adresse>.<Domänenname>:8080/ucmdb** eingeben.

---

b **Server Status**. Öffnet die Seite mit dem Server-Status. Weitere Informationen finden Sie unter "HP Universal CMDB-Services" auf Seite 123.

c **JMX Console**. Durch diese Option können Sie CMDB-Vorgänge über die Benutzeroberfläche der JMX-Konsole durchführen.

d **API Connection Test**. Zeigt Informationen zum HP Universal CMDB Server an, die Sie beim Ausführen einer API für die CMDB verwenden können.

e **API Client Download**. Lädt die UCMDB-API-JAR-Datei herunter.

f **API Reference**. Öffnet die HP UCMDB-API-Referenzdokumentation.

Anmelden bei HP Universal CMDB

1 Geben Sie die Standardanmeldeparameter für den Superuser ein:

- **Benutzeranmeldung**=admin, **Benutzerkennwort**=admin.
- Wenn HP Universal CMDB in einer Umgebung mit mehreren Kunden oder Status installiert ist (z. B. HP Software-as-a-Service oder Amber), wird das Feld **Kunde** angezeigt. Wählen Sie den Kundennamen in der Liste aus.
- Wählen Sie **In neuem Fenster öffnen** aus, um die Applikation in einem anderen Browserfenster zu öffnen.
- **Anmeldedaten auf diesem Computer speichern**: Wählen Sie diese Option für die automatische Anmeldung aus. Dadurch müssen Sie beim nächsten Anmelden in UCMDB nicht mehr Ihren Benutzernamen und Ihr Kennwort eingeben.
- **Lokalen Installationsmodus aktivieren**: Wählen Sie diese Option aus, um UCMDB im lokalen Installationsmodus zu laden. Weitere Informationen finden Sie unter "Lokaler Installationsmodus" auf Seite 443.

2 Klicken Sie auf **Anmelden**. Nach der Anmeldung wird der Benutzername oben rechts auf dem Bildschirm angezeigt.

3 (Empfohlen) Ändern Sie umgehend das Kennwort des Superuser, um nicht autorisierte Zugriffe zu verhindern. Informationen zum Ändern des Kennworts finden Sie unter "Dialogfeld "Kennwort zurücksetzen"" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

4 (Empfohlen) Erstellen Sie zusätzliche Administrationsbenutzer, damit HP Universal CMDB-Administratoren auf das System zugreifen können. Informationen zum Erstellen von Benutzern im HP Universal CMDB-System finden Sie unter "Assistent zum Hinzufügen neuer Benutzer" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Abmelden

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

So melden Sie sich ab:

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

Aktivieren der automatischen Anmeldung

Mithilfe erweiterter Anmeldeoptionen können Sie die Anmeldung automatisieren, den Anmeldezugriff einschränken und direkte Anmeldefunktionen für bestimmte Seiten in HP Universal CMDB bereitstellen.

Wenn Sie die automatische Anmeldung auf der Anmeldeseite aktivieren und der Benutzer das nächste Mal den URL für den Zugriff auf HP Universal CMDB eingibt, geschieht Folgendes: Die Anmeldeseite wird nicht geöffnet, der Anmeldename und das Kennwort müssen nicht eingegeben werden und die für den Benutzer festgelegte Standardseite wird automatisch geöffnet.

So aktivieren Sie die automatische Anmeldung:

1 Wählen Sie auf der HP Universal CMDB-Anmeldeseite die Option **Anmeldedaten auf diesem Computer speichern** aus.

2 Klicken Sie am Ende der Sitzung nicht auf **Abmelden** oben in der Seite, sondern schließen Sie das Browserfenster.

Durch das Abmelden wird die Option für die automatische Anmeldung deaktiviert und Sie müssen beim nächsten Zugriff auf HP Universal CMDB wieder den Benutzernamen und das Kennwort eingeben.

Richtlinien für die Verwendung der automatischen Anmeldung

Beachten Sie Folgendes, wenn Sie diese Option verwenden:

- Wenn Sie oben in der HP Universal CMDB-Seite auf **Abmelden** klicken, wird diese Option deaktiviert. Wenn sich ein Benutzer abmeldet und das nächste Mal anmeldet, wird die Anmeldeseite geöffnet und der Benutzer muss einen Anmeldenamen und ein Kennwort eingeben. Dies kann hilfreich sein, wenn sich ein anderer Benutzer auf demselben Computer mit einem anderen Benutzernamen und Kennwort anmelden muss.
- Diese Option stellt möglicherweise ein Sicherheitsrisiko dar und sollte mit Vorsicht verwendet werden.

Ändern der Standardzeitbegrenzung für die Abmeldung wegen Benutzerinaktivität

HP Universal CMDB enthält eine automatische Abmeldefunktion, durch die eine Abmeldung erfolgt, wenn das System über eine festgelegte Zeitspanne inaktiv ist. Die Standardzeitspanne beträgt 1440 Minuten (24 Stunden). Nach dieser Zeit wird eine Meldung angezeigt, in der die letzten 30 Sekunden bis zur Abmeldung heruntergezählt werden.

In dieser Aufgabe wird beschrieben, wie Sie die Zeitspanne anpassen, in der UCMDB auch ohne Benutzereingabe weiter ausgeführt wird, bevor die automatische Abmeldung erfolgt.

So ändern Sie die Standardzeitspanne bis zur Abmeldung:

1. Wählen Sie **Verwaltung** > **Infrastructure Settings Manager** > **Allgemeine Einstellungen** > **Maximal zulässige Inaktivität** aus.
2. Geben Sie in der Spalte **Wert** einen Wert ein.

3 Geben Sie ein neues Zeitintervall in Minuten ein. Alle Werte für **Maximal zulässige Inaktivität** befinden sich im Fenster **Eigenschaften**. Klicken Sie mit der rechten Maustaste auf die Eigenschaften für **Maximal zulässige Inaktivität** oder doppelklicken Sie auf die Einstellung **Maximal zulässige Inaktivität**.

29

Navigieren in HP Universal CMDB

Dieses Kapitel umfasst die folgenden Themen:

Konzepte

Referenz

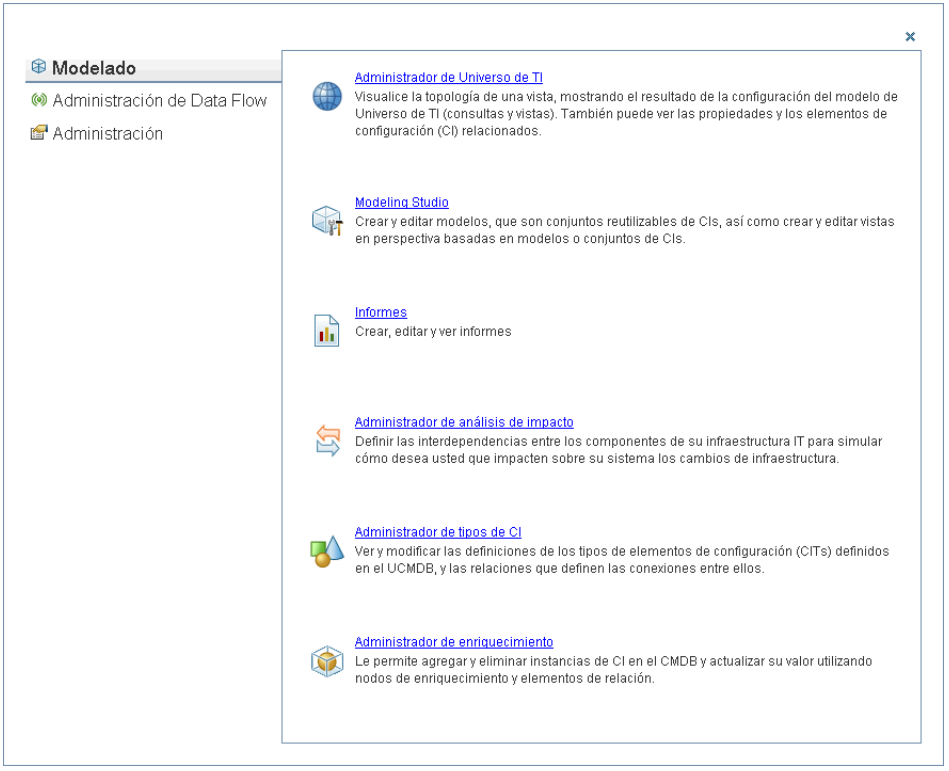
Konzepte

Navigieren in der HP Universal CMDB-Benutzeroberfläche

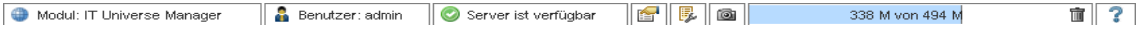
HP Universal CMDB wird in einem Webbrowser ausgeführt. Sie bewegen sich in HP Universal CMDB mit den folgenden Navigationsfunktionen:

➤ **Navigationsleiste.** Ermöglicht die schnelle Navigation zwischen Modulen. Klicken Sie im unteren Teil der Leiste auf die Kategorie und wählen Sie im oberen Teil der Leiste das Modulsymbol aus.

➤ **Übersichtskarte.** Sie können für jede Kategorie eine Karte mit Kurzbeschreibungen zu jedem enthaltenen Modul anzeigen, indem Sie **Manager** > **Übersichtskarte** auswählen.



➤ **Statusleiste.** Stellt Informationen zur CMDB-Applikation bereit und ermöglicht die Konfiguration bestimmter Aspekte Ihrer Schnittstelle.



➤ **Pfeile zum Ausblenden/Einblenden.** Ermöglichen das Aus- oder Einblenden von Ausschnitten mit einem einzigen Mausklick.

Hinweis: Die Webbrowser-Funktion **Zurück** wird in HP Universal CMDB nicht unterstützt. Durch die Funktion **Zurück** wird der aktuelle Kontext nicht immer in den vorherigen Kontext zurückgeändert. Um zum vorherigen Kontext zurückzukehren, verwenden Sie die Breadcrumb-Funktion.

Verwenden der HP Universal CMDB-Dokumentation

In den folgenden Abschnitten wird beschrieben, wie Sie in der HP Universal CMDB-Dokumentation navigieren und diese verwenden.

Navigieren in der UCMDB-Hilfe

Bei der UCMDB-Hilfe handelt es sich um ein integriertes Hilfesystem, in dem Sie wie folgt navigieren können:

- **Über die Startseite.** Zum Aufrufen der Startseite wählen Sie im Hilfemenü die Option **UCMDB-Hilfe** aus.

  Die Startseite enthält Links auf die einzelnen Handbücher, die entweder in der UCMDB-Hilfe enthalten sind oder im PDF-Format vorliegen.

- **Über den Navigationsausschnitt.** Um den Navigationsausschnitt aufzurufen, wenn er nicht angezeigt wird, klicken Sie auf die Schaltfläche für Suchen und Navigieren.

Der Navigationsausschnitt ist in die folgenden Registerkarten unterteilt:

- **Registerkarte "Inhalt".** Auf der Registerkarte **Inhalt** sind die verschiedenen Handbücher in einer hierarchischen Baumstruktur angeordnet, damit Sie direkt zu einem bestimmten Handbuch oder Thema navigieren können.
- **Registerkarte "Index".** Auf der Registerkarte **Index** können Sie ein bestimmtes Thema auswählen, das angezeigt werden soll. Doppelklicken Sie auf den Indexeintrag, um die zugehörige Seite anzuzeigen. Wenn Ihre Auswahl in mehreren Dokumenten vorkommt, wird ein Dialogfeld angezeigt, in dem Sie einen Kontext auswählen können.
- **Registerkarte "Suchen".** Auf der Registerkarte **Suchen** können Sie nach bestimmten Themen oder Schlüsselwörtern suchen. Die Ergebnisse werden in einer Rangfolge angezeigt.
- **Registerkarte "Favoriten".** Auf der Registerkarte **Favoriten** können Sie bestimmte Seiten zum schnellen Nachschlagen speichern. Die Registerkarte **Favoriten** ist nur verfügbar, wenn Sie die Java-Implementierung der UCMDB-Hilfe verwenden. Wenn Ihr Browser kein Java unterstützt, wird automatisch die JavaScript-Implementierung verwendet und die Registerkarte **Favoriten** wird nicht angezeigt.

Funktionen der Dokumentationsbibliothek

Die folgenden Funktionen sind oben im Hauptfenster der Dokumentationsbibliothek verfügbar.

- **Schaltfläche zum Suchen und Navigieren.** Klicken Sie auf diese Schaltfläche, um den Navigationsausschnitt mit den Registerkarten **Inhalt**, **Index**, **Suchen** und **Favoriten** anzuzeigen. Weitere Informationen zum Navigationsausschnitt finden Sie unter "Verwenden der HP Universal CMDB-Dokumentation" auf Seite 452. Diese Schaltfläche wird nur angezeigt, wenn der Navigationsausschnitt geschlossen ist.

- **Schaltfläche zum Anzeigen im Inhalt.** Klicken Sie auf diese Schaltfläche, um auf der Registerkarte **Inhalt** den Eintrag für die derzeit angezeigte Seite zu markieren. Diese Schaltfläche wird nur angezeigt, wenn der Navigationsausschnitt offen ist.

- **Schaltflächen zum Vor- und Zurückblättern.** Klicken Sie auf diese Schaltflächen, um im derzeit angezeigten Handbuch vor- oder zurückzublättern.

- **Schaltfläche zum Senden von Dokumentations-Feedback an HP.** Klicken Sie auf diese Schaltfläche, um Ihren E-Mail-Client zu öffnen und Feedback an HP zu senden. Dadurch wird eine E-Mail-Nachricht geöffnet, in der die Felder **An** und **Betreff** bereits ausgefüllt sind; im Nachrichtentext befindet sich ein Link auf die aktuelle Seite. Ergänzen Sie die E-Mail durch Ihr Feedback. Beachten Sie, dass auf dem Computer ein E-Mail-Client konfiguriert sein muss, um diese Funktion zu nutzen.

- **Schaltfläche zum Drucken.** Klicken Sie auf diese Schaltfläche, um die derzeit angezeigte Seite auszudrucken.

Organisation von Informationen in Themen

Das Material in den meisten Handbüchern der Dokumentationsbibliothek ist nach Thementypen organisiert. Es gibt drei Hauptthementypen: Konzepte, Aufgaben und Referenz. Diese Thementypen sind durch unterschiedliche Symbole gekennzeichnet. Im Folgenden finden Sie eine Erklärung zu jedem Thementyp sowie das zugehörige Symbol:

- **Konzepte**. Konzeptthemen enthalten Hintergrund-, beschreibende oder konzeptionelle Informationen. Durch Konzeptthemen erhalten Sie allgemeine Informationen über den Zweck und die Funktionsweise einer Funktion.

- **Aufgaben**. Aufgabenthemen enthalten eine schrittweise Anleitung, wie Sie bestimmte Aufgaben ausführen müssen, die zum Verwalten oder Verwenden der Software häufig benötigt werden. Aufgabenthemen umfassen außerdem Szenarien für bestimmte Aufgaben. Befolgen Sie die in Aufgabenthemen aufgeführten Schritte, um eine Aufgabe durchzuführen.

- **Referenz**. Referenzthemen enthalten detaillierte Listen und Erklärungen für Parameter, gängige Elemente der Benutzeroberfläche und anderes Referenzmaterial. Referenzthemen sind hilfreich, wenn Sie spezielle Referenzinformationen für einen bestimmten Kontext suchen.

- **Benutzeroberfläche**. Benutzeroberflächenthemen sind eine spezielle Form von Referenzthemen und werden hauptsächlich für kontextabhängige Hilfe verwendet. Durch Hilfe-Links in der Software werden in der Regel die Benutzeroberflächenthemen geöffnet.

- **Fehlerbehebung und Einschränkungen**. Fehlerbehebungs- und Einschränkungsthemen sind eine spezielle Form von Referenzthemen, in denen Fehlerbehebungsinformationen und Einschränkungen für eine Funktion aufgeführt sind. Fehlerbehebungs- und Einschränkungsthemen sind hilfreich, wenn die Software ein unerwartetes Verhalten aufweist. Sie sollten sich über die Einschränkungen für eine Funktion informieren, bevor Sie die Funktion verwenden.

Referenz

Menüs und Optionen

Die folgenden Kategorien sind im unteren Teil der Navigationsleiste verfügbar:

Kategorie	Beschreibung
Modeling Studio	Klicken Sie auf diese Option, um das Modelliermenü zu öffnen, über das Sie ein Modell Ihres IT Universe in der CMDB erstellen und verwalten. Weitere Informationen finden Sie im Abschnitt zur Modellierung im *HP Universal CMDB – Modellierungshandbuch* (PDF).
Data Flow Management	Klicken Sie auf diese Option, um das Menü für Data Flow Management (DFM) zu öffnen. Über dieses Menü richten Sie den DFM-Prozess ein und führen ihn aus, um das IT Universe-Modell mit Konfigurationselementen (CIs) aufzufüllen. Außerdem arbeiten Sie über dieses Menü mit Integration Studio. Weitere Informationen finden Sie im *HP Universal CMDB – Handbuch zur Datenflussverwaltung* (PDF). Weitere Informationen zum DFM-Inhalt finden Sie im *HP Universal CMDB Discovery and Integration Content Guide* (PDF).
Verwaltung	Klicken Sie auf diese Option, um das Verwaltungsmenü zu öffnen, über das Sie Infrastruktureinstellungen, Benutzer, Rollen, Berechtigungen und Zeitpläne konfigurieren und mit dem Package Manager arbeiten. Weitere Informationen finden Sie im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

Hilfemenü

Über das Hilfemenü von HP Universal CMDB können Sie auf die folgenden Online-Ressourcen zugreifen:

- **Hilfe zu dieser Seite.** Öffnet das Thema der UCMDB-Hilfe, in dem die aktuelle Seite oder der aktuelle Kontext beschrieben ist.
- **UCMDB-Hilfe.** Öffnet die Startseite. Die Startseite enthält direkte Links auf die Haupthilfethemen.
- **Fehlerbehebung & Wissensdatenbank.** Öffnet auf der HP Software Support-Website direkt die Startseite der HP Software-Wissensdatenbank. Der URL dieser Website lautet http://support.openview.hp.com.
- **HP Software-Unterstützung.** Öffnet die HP Software Support-Website. Auf dieser Site können Sie die Wissensdatenbank durchsuchen und eigene Artikel hinzufügen, Benutzerdiskussionsforen durchsuchen und eigene Beiträge veröffentlichen, Supportanfragen einreichen, Patches und aktualisierte Dokumentation herunterladen und vieles mehr. Der URL dieser Website lautet http://support.openview.hp.com.
- **HP Software-Website.** Öffnet die HP Software-Website, die Informationen und Ressourcen zu Produkten und Services von HP Software enthält. Der URL dieser Website lautet http://www.hp.com/managementsoftware.
- **Neues.** Öffnet das Dokument, in dem neue Funktionen und Erweiterungen der Version beschrieben werden.
- **DDM Content-Hilfe.** Beschreibt den vordefinierten Standardinhalt: was bei der Discovery erkannt wird, die erforderlichen Anmeldeinformationen für Discovery, Fehlerbehebung der Discovery-Ergebnisse und Verwendung von Integrationsadaptern.
- **Über HP Universal CMDB.** Öffnet das Dialogfeld mit Informationen zu HP Universal CMDB, darunter Version, Lizenz, Patch und Drittanbieterhinweise.

Hinweis: Informationen zu Hochverfügbarkeit finden Sie unter "Installieren im Hochverfügbarkeitsmodus" auf Seite 275.

30

Verfügbare Fehlerbehebungsressourcen

Dieses Kapitel umfasst die folgenden Themen:

Fehlerbehebungsressourcen

- **Fehlerbehebung bei der Installation.** Mit diesen Lösungen beheben Sie häufige Probleme, die beim Installieren von HP Universal CMDB auftreten können. Weitere Informationen finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 48.
- **Fehlerbehebung bei der Anmeldung.** Damit beheben Sie mögliche Ursachen von Fehlern beim Anmelden in HP Universal CMDB. Weitere Informationen finden Sie unter "Fehlerbehebung und Einschränkungen" auf Seite 48.
- **HP Software Self-Solve-Wissensdatenbank.** Darin können Sie nach bestimmten Fehlerbehebungsinformationen zu einer Vielzahl von Themen suchen. Die HP Software Self-Solve-Wissensdatenbank befindet sich auf der HP Software Support-Website und wird aufgerufen, indem Sie im HP Universal CMDB-Hilfemenü die Option **Fehlerbehebung & Wissensdatenbank** auswählen.

  Beachten Sie, dass nur registrierte Kunden auf die Ressourcen der HP Software Support-Website zugreifen können. Noch nicht registrierte Kunden können sich auf dieser Site registrieren.
- **HP Universal CMDB-Protokolldateien.** Damit können Sie CMDB-Laufzeitprobleme beheben. Weitere Informationen finden Sie unter "CMDB-Protokolldateien" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

- **Data Flow Management-Protokolldateien.** Damit können Sie Probleme beim Data Flow Management beheben. Weitere Informationen finden Sie unter "DFM-Protokolldateien" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).
- **Abfrageprotokolldateien.** Damit können Sie Definitionen von Abfrageparameter-Protokolldateien anzeigen. Weitere Informationen finden Sie unter "CMDB-Protokolldateien" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

31

Arbeiten mit nicht englischen Gebietsschemas

Dieses Kapitel umfasst die folgenden Themen:

Referenz

Referenz

Installations- und Bereitstellungsaspekte

- Wenn Sie die japanische, chinesische oder koreanische Sprache in Ihrem Browser verwenden, müssen Sie sicherstellen, dass ostasiatische Sprachen für den HP Universal CMDB Server installiert sind. Wählen Sie auf dem Computer, auf dem der HP Universal CMDB Server installiert ist, **Systemsteuerung** > **Regions- und Sprachoptionen** > **Sprachen** > **Dateien für ostasiatische Sprachen installieren** aus.
- Die Installation von HP Universal CMDB in einer I18N-Umgebung wird nur auf einer Windows-Plattform unterstützt. Andere Plattformen (z. B. Solaris, UNIX, Linux usw.) werden nicht unterstützt. Weitere Informationen zum Installieren von HP Universal CMDB auf einer Windows-Plattform finden Sie unter "Installieren von HP Universal CMDB auf einer Windows-Plattform" auf Seite 73.
- Beim Anmelden in HP Universal CMDB darf das Benutzerkennwort keine japanischen oder chinesischen Zeichen enthalten, wenn der UCMDB Server auf einem Windows 2003-Computer mit japanischem oder chinesischem Betriebssystem installiert ist.
- Der Installationspfad aller HP Universal CMDB-Komponenten darf keine nicht englischen Zeichen enthalten.
- Der Upgrade-Assistent für die Versionen 9.00 und 9.01 unterstützt nur die englische Benutzeroberfläche. (Das Upgrade selbst funktioniert ordnungsgemäß.)

Aspekte der Datenbankumgebung

- Um in einer HP Universal CMDB-Umgebung zu arbeiten, die nicht englischsprachig ist, können Sie entweder eine Oracle Server-Datenbank oder eine Microsoft SQL Server-Datenbank verwenden. Die regionalen Spracheinstellungen im Windows-Betriebssystem der Datenbank müssen mit den UCMDB Server-Einstellungen übereinstimmen. Wenn Sie eine Oracle Server-Datenbank verwenden, kann die Datenbankcodierung auch UTF-8 oder AL32UTF-8 lauten; dadurch werden sowohl nicht englische Sprachen als auch mehrere Sprachen unterstützt.
- Wenn Sie eine neue Oracle-Instanz in einer Oracle-Datenbank erstellen, müssen Sie den Zeichensatz für die Instanz festlegen. Alle Zeichendaten, einschließlich der Daten im Daten-Dictionary, werden im Zeichensatz der Instanz gespeichert. Weitere Informationen zum Arbeiten mit Oracle-Datenbanken finden Sie unter "HP Universal CMDB Installation on a Solaris Platform".
- Der Database Query Monitor kann mit einer Oracle-Datenbank verbunden werden, aber die Oracle-Benutzernamen und -Kennwörter dürfen nur englische Zeichen enthalten.

Administrationsaspekte

- Damit nicht englische Zeichen unterstützt werden, muss die Codierung der HP Universal CMDB-Datenbanken entweder UTF-8 oder AL32UTF-8 lauten oder auf die jeweilige Sprache festgelegt sein. Weitere Informationen finden Sie unter "Aspekte der Datenbankumgebung" auf Seite 463.

Report-Aspekte

- HP Universal CMDB unterstützt für benutzerdefinierte Reports keine Namen mit mehr als 50 Multibyte-Zeichen.
- Reports, die aus HP Universal CMDB in Excel heruntergeladen werden, können unter einem Betriebssystem mit anderer Sprache als der Datensprache nicht ordnungsgemäß angezeigt werden.

Wenn Sie Microsoft Office Version 2007 oder höher verwenden und die neuesten Aktualisierungen installiert haben, ist dieser Aspekt nicht relevant, weil die Daten im Unicode-Format gespeichert werden.

- Wenn ein Report in einer Gebietssprache erstellt und per E-Mail aus einer anderen Gebietssprache gesendet wird, enthält der Report Systeminformationen in den Sprachen des Servers und des ursprünglichen Gebietsschemas.
- Wenn der Name einer Report-Datei Multibyte-Zeichen enthält (z. B. japanische, chinesische oder koreanische Zeichen) und der Report als E-Mail-Anhang versendet wird, kann der Name nicht mehr gelesen werden.
- Standardmäßig werden UTF-8-codierte CSV-Dokumente in Excel nicht ordnungsgemäß geöffnet. Nachdem Sie einen Report als CSV-Datei gespeichert haben, können Sie ihn in Excel wie folgt importieren:

  a Wählen Sie im Menü **Daten** die Option **Externe Daten importieren** aus und klicken Sie auf **Daten importieren**.

  b Klicken Sie im Feld **Dateien vom Typ** auf **Textdateien**.

  c Suchen Sie im Feld **Suchen in** die Textdatei, die als externer Datenbereich importiert werden soll, und doppelklicken Sie darauf.

  d Um anzugeben, wie der Text in Spalten unterteilt wird, befolgen Sie die Anweisungen des Textimport-Assistenten und klicken auf **Fertig stellen**.

- Wenn Sie eine CI-Instanz in eine PDF-Datei exportieren, werden Multibyte-Zeichen (z. B. japanisch, chinesisch, koreanisch usw.) nicht in der PDF-Datei angezeigt.

Unterstützung für mehrsprachige Benutzeroberfläche

Hinweis: Die folgende Unterstützungsmatrix gilt für Version 9.00 (aber nicht für Version 9.01 oder andere kleinere Patches).

Die HP Universal CMDB-Benutzeroberfläche kann im Webbrowser in den folgenden Sprachen angezeigt werden:

Sprache	Lokalisierte Benutzer-oberfläche	Lokalisierte Materialien	Verfügbarkeit
Englisch	Ja	Ja	Teil der ursprünglichen Produktversion
Französisch	Ja		Teil der ursprünglichen Produktversion
Japanisch	Ja	Ja	Media Pack B
Koreanisch	Ja		Teil der ursprünglichen Produktversion
Vereinfachtes Chinesisch	Ja		Teil der ursprünglichen Produktversion
Niederländisch	Ja		Media Pack A
Deutsch	Ja		Teil der ursprünglichen Produktversion
Portugiesisch	Ja		Media Pack A
Russisch	Ja		Media Pack A
Spanisch	Ja		Teil der ursprünglichen Produktversion
Italienisch	Ja		Media Pack A

Hinweis: Ergänzende Media Packs werden innerhalb von 90 Tagen nach der Produkteinführung bereitgestellt.

Über die Spracheinstellung Ihres Browsers können Sie auswählen, in welcher Sprache HP Universal CMDB angezeigt wird. Die ausgewählte Spracheinstellung gilt nur für den lokalen Computer (den Client-Computer) und nicht für den HP Universal CMDB Server-Computer oder für andere Benutzer, die auf denselben HP Universal CMDB-Computer zugreifen.

So richten Sie die Anzeige von HP Universal CMDB in einer bestimmten Sprache ein:

1. Installieren Sie die erforderlichen Schriftarten für die Sprache auf dem lokalen Computer, falls diese noch nicht installiert sind. Wenn Sie in Ihrem Webbrowser eine Sprache auswählen, deren Schriftarten noch nicht installiert wurden, zeigt HP Universal CMDB die Zeichen als Quadrate an.
2. Wenn Sie in HP Universal CMDB angemeldet sind, müssen Sie sich abmelden. Klicken Sie oben im HP Universal CMDB-Fenster auf **Abmelden**.

   Schließen Sie alle offenen Browserfenster oder leeren Sie alternativ den Cache.
3. Wenn HP Universal CMDB in Internet Explorer ausgeführt wird, konfigurieren Sie den Webbrowser auf Ihrem lokalen Computer, um die Sprache auszuwählen, in der HP Universal CMDB angezeigt wird (**Extras** > **Internetoptionen**).

   a Klicken Sie auf die Schaltfläche **Sprachen** und markieren Sie im Dialogfeld **Spracheinstellung** die Sprache, in der Sie HP Universal CMDB anzeigen möchten.

   b Wird die gewünschte Sprache nicht im Dialogfeld aufgeführt, klicken Sie auf **Hinzufügen**, um die Liste der Sprachen anzuzeigen. Wählen Sie die Sprache aus, die Sie hinzufügen möchten, und klicken Sie auf **OK**.

   c Klicken Sie auf **Nach oben**, um die ausgewählte Sprache in die erste Zeile zu verschieben.

d Klicken Sie auf **OK**, um die Einstellungen zu speichern.

e Zeigen Sie das HP Universal CMDB-Anmeldefenster an.

f Wählen Sie in Internet Explorer in der Menüleiste **Ansicht** > **Aktualisieren** aus. HP Universal CMDB wird aktualisiert, um die Benutzeroberfläche in der ausgewählten Sprache anzuzeigen.

Hinweis: Weitere Informationen zum Anzeigen von Webseiten in einer anderen Sprache in Internet Explorer finden Sie unter http://support.microsoft.com/kb/306872/en-us.

Hinweise und Einschränkungen

- Es werden keine Sprachpakete installiert. Alle übersetzten Sprachen, die mit der ursprünglichen Version bereitgestellt werden, sind in die mehrsprachige Benutzeroberfläche (Multi-Lingual User Interface – MLU) von HP Universal CMDB integriert.
- Daten behalten immer ihre Eingabesprache, selbst wenn die Sprache des Webbrowsers geändert wird. Die Änderung der Sprache des Webbrowsers auf dem lokalen Computer wirkt sich nicht auf die Sprache der Dateneingabedefinitionen und -konfigurationen aus.
- Wenn sich Server und Client hinsichtlich Gebietsschema unterscheiden und der Package-Name nicht-englische Zeichen enthält, können Sie kein Package bereitstellen. Weitere Informationen finden Sie unter "Package Manager" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).
- Wenn Server und Client nicht dasselbe Gebietsschema aufweisen, können Sie kein Package erstellen, das Ressourcen (z. B. Ansichten und TQL-Abfragen) mit nicht englischen Zeichen im Namen enthält. Weitere Informationen finden Sie unter "Package Manager" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).
- Sie können unter **Benutzer und Rollen** keinen neuen Benutzer erstellen, dessen Name mehr als 20 ostasiatische Zeichen enthält. Weitere Informationen finden Sie unter "Benutzer und Rollen" im *HP Universal CMDB – Verwaltungshandbuch* (PDF).

- In Modeling Studio können Sie keine neue Ansicht erstellen, deren Name mehr als 18 japanische Zeichen enthält. Weitere Informationen finden Sie unter "Modeling Studio" im *HP Universal CMDB – Modellierungshandbuch* (PDF).
- Die folgenden Seiten werden nur auf Englisch angezeigt. Sie wurden nicht in andere Sprachen übersetzt. Weitere Informationen finden Sie unter "Arbeiten mit nicht englischen Gebietsschemas" auf Seite 461.
  - HTML-Seite mit HP Universal CMDB Server-Status
  - HP Universal CMDB-Anmeldeseite
  - Seite der JMX-Konsole
  - Seite für API-Verbindungstest
- Wenn Sie auf dem Client-Computer eine Sprache auswählen, die die mehrsprachige UCMDB-Benutzeroberfläche nicht unterstützt, wird HP Universal CMDB mit derselben Gebietssprache angezeigt wie auf dem UCDMB Server-Computer.

Index

I

J

K

L

M

N

O

P

R

S