HP Universal CMDB

Per Sistemi operativi Windows e Red Hat Enterprise Linux

Versione software: 10.00

Protezione avanzata di HP Universal CMDB e Configuration Manager

Data di rilascio del documento: giugno 2012

Data di rilascio del software: giugno 2012

Informazioni legali

Garanzia

Le uniche garanzie riconosciute per i prodotti e servizi HP sono stabilite nelle dichiarazioni di garanzia esplicite allegate a tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato in modo da costituire una garanzia aggiuntiva. HP non è responsabile di errori e omissioni editoriali o tecnici contenuti nel presente documento.

Le informazioni contenute nella presente documentazione sono soggette a modifiche senza preavviso.

Legenda dei diritti riservati

Questo software per computer è riservato. Per il possesso, l'uso o la copia è necessario disporre di una licenza HP valida. In conformità con le disposizioni FAR 12.211 e 12.212, il software commerciale, la documentazione del software e i dati tecnici per gli articoli commerciali sono concessi in licenza al governo degli Stati Uniti alle condizioni di licenza commerciale standard del fornitore.

Informazioni sul copyright

Informazioni sui marchi

Adobe™ è un marchio di Adobe Systems Incorporated.

Microsoft® e Windows® sono marchi registrati negli Stati Uniti di Microsoft Corporation.

UNIX® è un marchio registrato di The Open Group.

Aggiornamenti della documentazione

La pagina del titolo del presente documento contiene le seguenti informazioni di identificazione:

- Numero di versione software, che indica la versione del software.
- Data di rilascio del documento, che varia ad ogni aggiornamento del documento.
- Data di rilascio del software, che indica la data di rilascio di questa versione del software.

Per verificare l'esistenza di aggiornamenti recenti o per accertarsi di utilizzare la versione più recente del documento, visitare il sito:

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

Questo sito richiede la registrazione e l'accesso come utente HP Passport. Per registrarsi come utente HP Passport, andare all'indirizzo:

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

Oppure fare clic sul collegamento **New user registration** nella pagina di accesso di HP Passport.

È inoltre possibile ricevere versioni nuove o aggiornate abbonandosi all'apposito servizio di assistenza. Per informazioni, contattare il rappresentante commerciale di HP.

Assistenza

Visitare il sito Web dell'assistenza online HP Software all'indirizzo:

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

Questo sito Web fornisce informazioni di contatto e dettagli sui prodotti, servizi e assistenza offerti da HP Software.

L'assistenza online di HP Software fornisce ai clienti funzionalità di auto-risoluzione dei problemi e costituisce un modo efficiente e veloce per accedere agli strumenti di assistenza tecnica interattiva necessari per gestire il proprio business. Nel sito Web dell'assistenza è possibile usufruire dei seguenti vantaggi:

- Ricerca di documenti nelle Knowledge Base
- Invio e consultazione di casi di assistenza e richieste di miglioramenti
- Download di patch software
- Gestione di contratti di assistenza
- Ricerca di recapiti di assistenza HP
- Esame delle informazioni relative ai servizi disponibili
- Partecipazione a forum di discussione con altri utenti del software
- Ricerca e iscrizione a eventi di formazione software

La maggior parte delle aree di assistenza richiede la registrazione e l'accesso come utente HP Passport. In molti casi è inoltre necessario disporre di un contratto di assistenza. Per registrarsi come utente HP Passport, andare all'indirizzo:

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

Per ulteriori informazioni sui livelli di accesso, visitare:

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

Sommario

Capitolo 1

Introduzione alla protezione avanzata

Questo capitolo comprende:

Panoramica della Protezione avanzata

Questa sezione introduce il concetto di applicazione HP Universal CMDB sicura ed esamina la pianificazione e l'architettura necessaria per implementare la protezione. Si consiglia vivamente di leggere questa sezione prima di procedere a esaminare la protezione avanzata presentata nelle seguenti sezioni.

HP Universal CMDB è progettato in modo da poter essere parte di un'architettura sicura, ed è quindi in grado di resistere alle minacce poste alla sicurezza a cui potrebbe essere esposto.

Le linee guida della protezione avanzata presentano la configurazione necessaria per poter implementare HP Universal CMDB in modo che abbia una protezione maggiore.

Le informazioni per la protezione avanzata offerta si riferiscono principalmente agli amministratori di HP Universal CMDB che devono familiarizzare con le impostazioni e raccomandazioni relative alla protezione avanzata prima di iniziare le procedure di protezione avanzata.

Si consiglia di utilizzare un proxy inverso con HP Universal CMDB per ottenere un'architettura sicura. Per i dettagli sulla configurazione di un proxy inverso da utilizzare con HP Universal CMDB, consultare "Utilizzo di un proxy inverso" a pagina 34.

Se con HP Universal CMDB si deve utilizzare un tipo di architettura sicura diversa da quella descritta in questo documento, rivolgersi all'Assistenza software HP per stabilire quale sia la migliore architettura in tal caso.

Per i dettagli sulla protezione avanzata della sonda del flusso di dati, consultare "Protezione avanzata della sonda del flusso di dati" a pagina 62.

Nota:

- Le procedure di protezione avanzata si basano sul presupposto che si stanno implementando solo le istruzioni fornitein questi capitoli, e che non si stanno eseguendo altri passaggi relativi alla protezione avanzata documentati altrove.
- Laddove le procedure di protezione avanzata pongono l'attenzione su una particolare architettura distribuita, ciò non implica che questa sia l'architettura che meglio di adatta alle necessità dell'organizzazione.
- Si presume che le procedure incluse nei capitoli seguenti siano state eseguite su computer dedicati ad HP Universal CMDB. L'uso di computer per scopi diversi oltre a HP Universal CMDB potrebbe determinare problemi.
- Le informazioni relative alla protezione avanzata fornite in questa sezione non sono intese come guida per la creazione della valutazione del rischio di protezione per i sistemi informatizzati.

Protezione avanzata, preparazioni

- Valutare il rischio di protezione/stato della protezione per le reti generiche, e utilizzare le conclusioni quando si decide come integrare al meglio HP Universal CMDB nella rete.
- Sviluppare una buona conoscenza del framework tecnico di HP Universal CMDB e delle funzionalità di protezione di HP Universal CMDB.
- Riesaminare tutte le linee guida relative alla protezione avanzata.
- Verificare che HP Universal CMDB sia completamente funzionante prima di avviare le procedure di protezione avanzata.
- Seguire in ordine cronologico i passaggi delle procedure relative alla protezione avanzata in ciascun capitolo. Se si decide ad esempio di configurare il server HP Universal CMDB per supportare il protocollo SSL, leggere "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pagina 18 e poi seguire tutte le istruzioni in ordine cronologico.
- HP Universal CMDB non supporta l'autenticazione di base con password vuote. Non utilizzare una password vuota quando si impostano i parametri di connessione con autenticazione di base.

Suggerimento: stampare le procedure di protezione avanzata e verificarle al momento dell'implementazione.

Distribuzione di UCMDB in un'architettura protetta

Si consiglia di adottare alcune misure per la distribuzione sicura dei server HP Universal CMDB:

- **Architettura DMZ con utilizzo di un firewall**

  L'architettura sicura a cui si riferisce questo documento è una tipica architettura DMZ che utilizza una periferica che funge da firewall. Il concetto di base di questa architettura è la creazione di una separazione completa ed evitare l'accesso diretto tra i client HP Universal CMDB e i server HP Universal CMDB.

- **Browser sicuro**

  Internet Explorer FireFox in un ambiente Windows devono essere configurati per la gestione sicura degli script Java, delle applet e dei cookie.

- **Protocollo di comunicazione SSL**

  Il protocollo Secure Sockets Layer protegge la connessione tra il client e il server. Gli URL che richiedono una connessione SSL utilizzano una versione protetta (HTTPS) di Hypertext Transfer Protocol. Per i dettagli consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pagina 18.

- **Architettura del proxy inverso**

  Una delle soluzioni più protette e consigliate suggerisce la distribuzione di HP Universal CMDB utilizzando un proxy inverso. HP Universal CMDB supporta completamente l'architettura del proxy inverso protetta. Per i dettagli consultare "Utilizzo di un proxy inverso" a pagina 34.

Accesso al sistema

Protezione avanzata accesso Java JMX

Nota: La procedura qui descritta può essere utilizzata anche per JMX della sonda del flusso di dati.

Al fine di garantire che la porta JMX RMI sia accessibile solo quando vengono specificate le credenziali utente, attenersi alla seguente procedura:

1. Nel file **wrapper.conf** sul server, che si trova in **C:\hp\UCMDB\UCMDBServer\bin**, impostare quanto segue:

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

   Questa impostazione prevede la richiesta di autenticazione da JMX.

   - **Per JMX della sonda del flusso di dati**, eseguire quanto segue:

     Nei file **WrapperGateway.conf** e **WrapperManager.conf**, che si trovano in **C:\hp\UCMDB\DataFlowProbe\bin**, impostare quanto segue:

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

2. Rinominare il file **jmxremote.password.template** (che si trova in: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) in **jmxremote.password**.

Nota: per JMX della sonda del flusso di dati, questo file si trova in: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. In **jmxremote.password**, aggiungere le password per questi ruoli **monitorRole** e **controlRole**.

   Ad esempio:

   monitorRole QED

   controlRole R&D

   assegna la password **QED** a **monitorRole** e la password **R&D** a **controlRole**.

   Nota: Accertarsi che solo il proprietario abbia letto e sottoscritto le autorizzazioni in **jmxremote.password**, poiché contiene le password in chiaro. Il proprietario del file deve essere lo stesso utente che è in esecuzione sul server UCMDB.

4. Nel file **jmxremote.access** (che si trova in **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), assegnare l'accesso al **monitorRole** e **controlRole**.

   Ad esempio:

   monitorRole readonly

   controlRole readwrite

   assegna l'accesso in sola lettura a **monitorRole** e l'accesso in lettura/scrittura a **controlRole**.

   Nota: per JMX della sonda del flusso di dati, questo file si trova in: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Proteggere i file come segue:

   - **Solo per Windows:** eseguire i seguenti comandi dalla riga di comando per proteggere i file:

     cacls jmxremote.password /P <username>:F

     cacls jmxremote.access /P <username>:R

     dove **<userrname>** è il proprietario del file visibile nelle proprietà di entrambi i file. Aprire le proprietà di questi file e assicurarsi che siano corrette e che possiedano un solo proprietario.

   - **Per i sistemi operativi Solaris e Linux:** impostare le autorizzazioni del file per il file della password eseguendo:

     chmod 600 jmxremote.password

6. **Per gli upgrade dei Service Pack, le migrazioni del server e il ripristino di emergenza:** assegnare la proprietà del file **jmxremote.access** (che si trova in **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) all'utente del sistema operativo che esegue l'installazione dell'aggiornamento o della migrazione.

   Nota: per JMX della sonda del flusso di dati, questo file si trova in:

C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management.

Cambiare il nome utente o la password di sistema per la JMX Console

La JMX Console utilizza gli utenti di sistema, ovvero utenti di più clienti in un ambiente a multi-titolarità. È possibile accedere alla JMX Console con qualsiasi nome utente di sistema. Il nome e la password predefiniti sono **sysadmin/sysadmin**.

La password può essere cambiata tramite la JMX Console o tramite lo strumento Server Management.

Per cambiare il nome utente o la password di sistema tramite la JMX Console:

1. Avviare il browser Web e specificare il seguente indirizzo: **http://localhost.<domain_name>:8080/jmx-console**.
2. Immettere le credenziali di autenticazione della JMX Console, che per impostazione predefinita sono:
   - Nome di accesso = **sysadmin**
   - Password = **sysadmin**
3. Individuare **UCMDB:service=Authorization Services** e fare clic sul collegamento per aprire la pagina Operazioni.
4. Individuare l'operazione **resetPassword**.
   - Nel campo **userName** immettere **sysadmin**.
   - Nel campo **password** immettere la nuova password.
5. Fare clic su **Invoke** per salvare il cambiamento.

Per cambiare il nome utente o la password di sistema tramite lo strumento Server Management:

1. **Per Windows:** eseguire il seguente file: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   Per Linux: eseguire **server_management.sh** che si trova nella cartella seguente: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Accedere allo strumento con le credenziali di autenticazione: **sysadmin/sysadmin**.
3. Fare clic sul collegamento Utenti.
4. Selezionare l'utente di sistema e fare clic su **Cambiare la password per l'utente connesso**.
5. Selezionare la password precedente e la nuova, quindi fare clic su **OK**.

Cambio dell'utente del servizio di HP Universal CMDB Server.

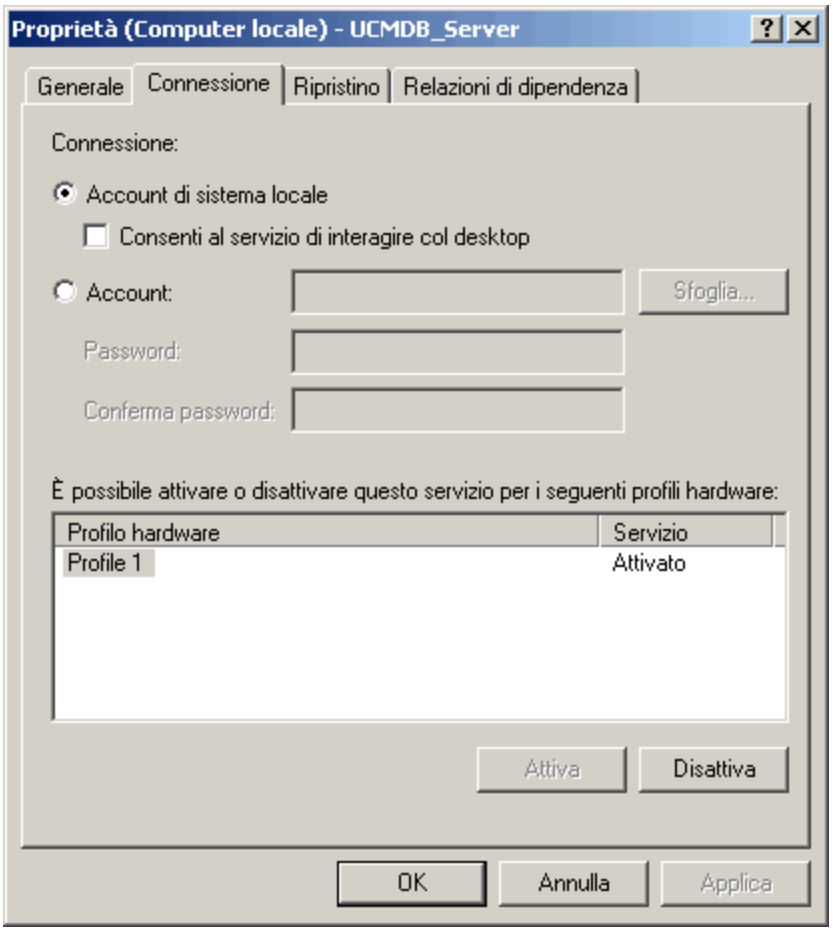
Su una piattaforma Windows il servizio HP Universal CMDB che esegue tutti i servizi e i processi di HP Universal CMDB viene installato quando si esegue l'utilità di configurazione del server e del database. Per impostazione predefinita, questo servizio viene eseguito mediante l'utente sistema locale. È possibile che si renda necessario assegnare un utente diverso per eseguire il servizio (ad esempio se si utilizza l'autenticazione NTLM).

L'utente assegnato per eseguire il servizio deve disporre delle autorizzazioni seguenti:

- autorizzazioni sufficienti per il database (come definito dall'amministratore del database)
- autorizzazioni sufficienti di rete
- autorizzazioni di amministratore sul server locale

Per cambiare l'utente del servizio:

1. Disabilitare dal menu Start di HP Universal CMDB (**Start >Programmi > HP UCMDB > Arresta server HP Universal CMDB**) oppure arrestando il servizio del server di HP Universal CMDB. Per i dettagli consultare "Avvio e arresto del servizio di HP Universal CMDB Server" a pagina 1.
2. Nella finestra **Servizi** di Windows, fare doppio clic su **UCMDB_Server**. Si aprirà la finestra di dialogo **Proprietà (computer locale) - UCMDB_Server**.
3. Fare clic sulla scheda Connessione.



4. Selezionare **Account** quindi Sfoglia per selezionare un altro utente dall'elenco degli utenti validi sul computer.
5. Immettere la password di Windows per l'utente selezionato e confermare la password.
6. Fare clic su **Applica** per salvare le impostazioni quindi su **OK** per chiudere la finestra di dialogo.
7. Abilitare HP Universal CMDB dal menu Start (**Start > Tutti i programmi > HP UCMDB > Avvia HP Universal CMDB Server**) oppure avviando il servizio del server di HP Universal CMDB. Per i dettagli consultare "Avvio e arresto del servizio di HP Universal CMDB Server" a pagina 1.

Crittografare la password del database per Configuration Manager

La password del database CM viene archiviata nel file **>\conf\database.properties** della directory di installazione di **<Configuration Manager**. Per crittografare la password, il nostro algoritmo di crittografia predefinito è conforme agli standard della FIPS 140-2.

La crittografia viene eseguito utilizzando una chiave, tramite la quale la password viene crittografata. La stessa chiave viene crittografata utilizzando un'altra chiave, conosciuta come chiave master. Entrambe le chiavi vengono crittografate utilizzando lo stesso algoritmo. Per

informazioni sui parametri utilizzati nel processo di crittografia, consultare "Parametri per la crittografia della password del database di Configuration Manager" nel seguito

Attenzione: Se viene cambiato l'algoritmo di crittografia, tutte le password crittografate in precedenza non saranno più utilizzabili.

Per cambiare la crittografia della password del database:

1. Eliminare il file **<Configuration Manager installation directory>\conf \encryption.properties** e modificare i seguenti campi:
   - **engineName.** Immettere il nome dell'algoritmo di crittografia.
   - **keySize.** Immettere la dimensione della chiave master per l'algoritmo selezionato.
2. Eseguire lo script **generate-keys.bat**, che crea il seguente file: **<Configuration Manager installation directory>\security\encrypt_repository** e genera la chiave di crittografia.
3. Eseguire l'utilità **bin\encrypt-password.bat** per crittografare la password. Impostare il flag **-h** per visualizzare le opzioni disponibili.
4. Copiare il risultato dell'utilità di crittografia della password e incollare la crittografia nel file **conf\database.properties**.

Parametri per la crittografia della password del database di Configuration Manager

La seguente tabella elenca i parametri inclusi nel file **encryption.properties** utilizzato per la crittografia della password del database di CM. Per i dettagli sulla crittografia della password del database, consultare "Crittografare la password del database per Configuration Manager" alla pagina precedente.

Parametro	Descrizione
cryptoSource	Indica l'infrastruttura che implementa l'algoritmo di crittografia. Le opzioni disponibili sono: • **lw.** Utilizza l'implementazione Bouncy Castle lightweight (opzione predefinita) • **jce.** Java Cryptography Enhancement (infrastruttura di crittografia Java standard)
storageType	Indica il tipo di archivio chiavi. Attualmente, è supportato solo **file binario**.
binaryFileStorageName	Indica il punto nel file dove è archiviata la chiave master.
cipherType	Il tipo di crittografia. Attualmente, è supportato solo **symmetricBlockCipher**.
engineName	Il nome dell'algoritmo di crittografia.

Parametro	Descrizione
	Sono disponibili le seguenti opzioni: • **AES.** American Encryption Standard. Questa crittografia è conforme a FIPS 140-2. (opzione predefinita) • **Blowfish** • **DES** • **3DES.** (conforme a FIPS 140-2) • **Null**. Nessuna crittografia
keySize	La dimensione della chiave master. La dimensione è determinata dall'algoritmo: • **AES.** 128, 192, o 256 (opzione predefinita: 256) • **Blowfish.** 0-400 • **DES.** 56 • **3DES.** 156
encodingMode	La codifica ASCII dei risultati di crittografia binari. Sono disponibili le seguenti opzioni: • **Base64** (opzione predefinita) • **Base64Url** • **Hex**
algorithmModeName	La modalità dell'algoritmo. Attualmente, è supportato solo **CBC**.
algorithmPaddingName	L'algoritmo di riempimento utilizzato. Sono disponibili le seguenti opzioni: • **PKCS7Padding** (opzione predefinita) • **PKCS5Padding**
jceProviderName	Il nome dell'algoritmo di crittografia JCE. **Nota:** rilevante solo quando crytpSource è jce. Per lw, è utilizzato engineName.

Capitolo 2

Abilitazione della comunicazione Secure Sockets Layer (SSL)

Questo capitolo comprende:

Attivare SSL sul computer server con certificato autofirmato - UCMDB

Queste sezioni illustrano come configurare HP Universal CMDB per supportare la comunicazione utilizzando il canale Secure Sockets Layer (SSL).

HP Universal CMDB utilizza 6.1 come server Web predefinito.

1. **Prerequisites**

   a. Prima di avviare la procedura seguente, rimuovere il **server.keystore** precedente che si trova in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

   b. Collocare il keystore di HP Universal CMDB (tipo JKS) nella cartella **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Generare un Keystore server**

   a. Creare un keystore (tipo JKS) con un certificato autofirmato e corrispondente alla chiave privata:

   - Da **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** eseguire il comando seguente:

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

     Si apre la finestra di dialogo della console.

   - Immettere la password del keystore. Se la password è cambiata, eseguire l'operazione JMX **changeKeystorePassword** in **UCMDB:service=Security Services**. Se la password non è stata cambiata, utilizzare la password predefinita **hppass**.

   - Rispondere alla domanda **Quali sono nome e cognome?** Immettere il nome server Web di HP Universal CMDB. Immettere gli altri parametri in relazione alla propria organizzazione.

   - Immettere la password della chiave. La password della chiave DEVE essere la stessa della password keystore.

     Viene creato un keystore JKS con il nome **server.keystore** con un certificato server con il nome **hpcert**.

   b. Esportare il certificato autofirmato in un file.

   Da **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** eseguire il comando seguente:

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

3. **Collocare il certificato nell'archivio dati attendibile del client**

   Dopo avere generato **server.keystore** e avere esportato il certificato del server, per ogni client che deve comunicare con HP Universal CMDB tramite protocollo SSL utilizzando questo certificato autofirmato, collocare il certificato nell'archivio dati attendibile del client.

   Nota: in **server.keystore** può essere presente un solo certificato server.

4. **Disabilitare la porta 8080 HTTP**

   Per i dettagli consultare "Abilitare o disabilitare le porte HTTP/HTTPS" a pagina 28.

   Nota: verificare che la comunicazione HTTPS funzioni prima di chiudere la porta HTTP.

5. **Riavviare il server**

6. **Visualizzare HP Universal CMDB**

   Per verificare che il server UCMDB sia protetto, immettere l'URL seguente nel browser Web: **https://<nome server UCMDB o indirizzo IP>:8443/ucmdb-ui**.

Abilitare SSL sul Computer server con certificato autofirmato - Configuration Manager

Queste sezioni illustrano come configurare Configuration Manager per supportare l'autenticazione e la crittografia utilizzando il canale Secure Sockets Layer (SSL).

Configuration Manager utilizza Tomcat 7.0.19 come server applicazioni.

Nota: Tutti i percorsi delle directory e dei file dipendono da piattaforma specifica, sistema operativo e preferenze di installazione.

1. ## Prerequisites

   Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** nella cartella **<Configuration Manager installation directory>\java\windows\x86_64\lib\security** o nella cartella **<Configuration Manager installation directory>\java\linux\x86_64\lib\security** (o quella rilevante), se esistente.

2. ## Generare un Keystore server

   Creare un keystore (tipo JKS) con un certificato autofirmato e corrispondente alla chiave privata:

   - Dalla directory bin dell'installazione Java nella directory di installazione di Configuration Manager eseguire il seguente comando:

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

     Si apre la finestra di dialogo della console.

   - Immettere la password del keystore. Se la password è stata cambiata, cambiarla manualmente nel file.
   - Rispondere alla domanda **Quali sono nome e cognome?** Immettere il nome server Web di Configuration Manager. Immettere gli altri parametri in relazione alla propria organizzazione.
   - Immettere la password della chiave. La password della chiave DEVE essere la stessa della password keystore.

     Viene creato un keystore JKS con il nome **tomcat.keystore** con un certificato server con il nome **hpcert**.

3. ## Collocare il certificato nell'archivio dati attendibile del client

   Aggiungere il certificato all'archivio dati attendibile del client in Internet Explorer sul computer (**Strumenti > Opzioni Internet > Contenuti > Certificati**). In caso contrario, verrà chiesto di eseguire questa procedura al primo utilizzo di Configuration Manager.

Limitazione: in **tomcat.keystore** può essere presente un solo certificato server.

4. **Modificare il file server.xml**

   Aprire il file **server.xml**, disponibile in **<Configuration Manager installation directory>\servers\server-0\conf**. Individuare la sezione che inizia con

   ```
   Porta connettore="8143"
   ```

   visualizzata nei commenti. Attivare lo script rimuovendo il commento e aggiungendo i seguenti attributi al connettore HTTPS:

   ```
   keystoreFile="<tomcat.keystore file location>"
   ```
   (fare riferimento al passaggio 2)
   ```
   keystorePass="<password>"
   ```

   Impostare come commento la seguente riga:

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

   Nota: Non bloccare la porta di connessione HTTP. È possibile usare un firewall per bloccare la comunicazione HTTP.

5. **Riavviare il server**

   Riavviare il server di Configuration Manager.

6. **Verificare la protezione del server**

   Per verificare che Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://<nome server o indirizzo IP di Configuration Manager>:8143/cnc**.

   Suggerimento: Se non si riesce a stabilire una connessione, provare ad utilizzare un browser diverso o ad aggiornare il browser alla versione più recente.

Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione - UCMDB

Per utilizzare un certificato emesso da un'Autorità di certificazione (CA), il keystore deve essere nel formato Java. L'esempio di seguito spiega come formattare il keystore per un computer Windows.

1. **Prerequisites**

   Prima di avviare la procedura seguente, rimuovere il **server.keystore** precedente che si trova in **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. **Generare un Keystore server**

a. Generare un certificato CA firmato e installarlo in Windows.

b. Esportare il certificato in un file ***.pfx** (incluse le chiavi private) utilizzando Microsoft Management Console (**mmc.exe**).

Immettere qualsiasi stringa come la password per il file **pfx**. (Questa password viene chiesta quando si converte il tipo keystore in un keystore JAVA.) Il file **.pfx** ora contiene un certificato pubblico e una chiave privata e la password è protetta.

c. Copiare il file **.pfx** creato nella seguente cartella: **C:\hp\UCMDB\UCMDBServer\conf\security**.

d. Aprire il prompt dei comandi e cambiare la directory in **C:\hp\UCMDB\UCMDBServer\bin\jre\bin.**

Cambiare il tipo di keystore da **PKCS12** a un keystore **JAVA** eseguendo il seguente comando:

```
keytool -importkeystore -srckeystore
c:\hp\UCMDB\UCMDBServer\conf\security\<pfx file name> -
srcstoretype PKCS12 -destkeystore server.keystore
```

Viene chiesta l'origine della password keystore (**.pfx**). È la password fornita durante la creazione del file **pfx** nel passaggio).

e. Immettere la password del keystore di destinazione. Deve essere la stessa password definita in precedenza nel metodo JMX **changeKeystorePassword** in Security Services. Se la password non è stata cambiata, utilizzare la password predefinita **hppass**.

f. Dopo aver generato il certificato, disabilitare la porta 8080 HTTP. Per i dettagli consultare "Abilitare o disabilitare le porte HTTP/HTTPS" a pagina 28.

g. Se è stata utilizzata una password diversa da **hppass** oppure la password utilizzata per il file **.pfx**, eseguire il metodo JMX **changeKeystorePassword** e accertarsi che la chiave abbia la stessa password.

> **Nota:** verificare che la comunicazione HTTPS funzioni prima di chiudere la porta HTTP.

3. **Riavviare il server**

4. **Verificare la protezione del server**

Per verificare che il server UCMDB sia protetto, immettere l'URL seguente nel browser Web: **https://<nome server UCMDB o indirizzo IP>:8443/ucmdb-ui**.

> **Attenzione:** in **server.keystore** può essere presente un solo certificato server.

Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione - Configuration Manager

In Configuration Manager, per utilizzare un certificato emesso da un'Autorità di certificazione (CA), il keystore deve essere nel formato Java. L'esempio di seguito spiega come formattare il keystore per un computer Windows.

1. ## Prerequisites

   Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** nella cartella **<Configuration Manager installation directory>\java\windows\x86_64\lib\security** o nella cartella **<Configuration Manager installation directory>\java\linux\x86_64\lib\security** (o quella rilevante), se esistente.

2. ## Generare un Keystore server

   a. Generare un certificato CA firmato e installarlo in Windows.

   b. Esportare il certificato in un file ***.pfx** (incluse le chiavi private) utilizzando Microsoft Management Console (**mmc.exe**).

   Immettere qualsiasi stringa come la password per il file **pfx**. (Questa password viene chiesta quando si converte il tipo keystore in un keystore JAVA.)
   Il file **.pfx** ora contiene un certificato pubblico e una chiave privata e la password è protetta.

   Copiare il file **.pfx** creato nella seguente cartella: **<Configuration Manager installation directory>\java\lib\security**.

   c. Aprire il prompt dei comandi e cambiare la directory nella **<Configuration Manager installation directory>\java\bin**.

   Cambiare il tipo di keystore da **PKCS12** a un keystore **JAVA** eseguendo il seguente comando:

   ```
   keytool -importkeystore -srckeystore <Configuration Manager
   installation directory>\conf\security\<pfx file name> -
   srcstoretype PKCS12 -destkeystore tomcat.keystore
   ```

   Viene chiesta l'origine della password keystore (**.pfx**). È la password fornita durante la creazione del file pfx nel passaggio b.

3. ## Modificare il file server.xml

   Aprire il file **server.xml**, disponibile in **<Configuration Manager installation directory>\servers\server-0\conf**. Individuare la sezione che inizia con

   ```
   Porta connettore="8143"
   ```

   visualizzata nei commenti. Attivare lo script rimuovendo il delimitatore e aggiungendo le due righe seguenti:

   ```
   keystoreFile="../../java/lib/security/tomcat.keystore"
   keystorePass="password" />
   ```

Impostare come commento la seguente riga:

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

Nota: Non bloccare la porta di connessione HTTP. È possibile usare un firewall per bloccare la comunicazione HTTP.

4. **Riavviare il server**

   Riavviare il server di Configuration Manager.

5. **Verificare la protezione del server**

   Per verificare che Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://<nome server o indirizzo IP di Configuration Manager>:8143/cnc**.

Limitazione: In **tomcat.keystore** può essere presente un solo certificato server.

Nota: I percorsi delle directory e dei file dipendono da piattaforma specifica, sistema operativo e preferenze di installazione.

Ad esempio: `java/{os name}/lib`.

Abilitare SSL sui client - UCMDB

Se il certificato utilizzato dal server Web di HP Universal CMDB è pubblicato da un'Autorità di certificazione (CA) conosciuta, molto probabilmente il browser Web è in grado di convalidare il certificato senza ulteriori azioni.

Se il CA non è ritenuto affidabile dal browser Web, importare l'intero percorso attendibile del certificato oppure importare il certificato utilizzato da HP Universal CMDB in modo esplicito nell'archivio dati attendibile del browser.

Negli esempi seguenti viene illustrato come importare il certificato autofirmato **hpcert** nell'archivio dati attendibile di Windows che deve utilizzare Internet Explorer.

Per importare un certificato nell'archivio dati attendibile di Windows:

1. Individuare e rinominare il certificato **hpcert** in **hpcert.cer**.

   In Esplora risorse, l'icona mostra che il file è un certificato di protezione.

2. Fare doppio clic su **hpcert.cer** per aprire la finestra di dialogo Certificato Internet Explorer.
3. Seguire le istruzioni per abilitare l'affidabilità installando il certificato con la procedura guidata per l'importazione del certificato.

Nota: un altro metodo per importare il certificato emesso dal server UCMDB nel browser Web consiste nell'accesso a UCMDB e l'installazione del certificato quando viene visualizzato l'avviso di certificato non attendibile.

Abilitare SSL con un certificato client - Configuration Manager

Se il certificato utilizzato dal server Web di Configuration Manager è pubblicato da un'Autorità di certificazione (CA) conosciuta, molto probabilmente il browser Web è in grado di convalidare il certificato senza ulteriori azioni.

Se il CA non è ritenuto affidabile dall'archivio dati attendibile del server, importare il certificato CA nell'archivio dati attendibile del server.

Negli esempi seguenti viene illustrato come importare il certificato autofirmato **hpcert** nell'archivio dati attendibile del server (cacerts).

Per importare un certificato nell'archivio dati attendibile del server:

1. Sul computer client, individuare e rinominare il certificato **hpcert** in **hpcert.cer**.
2. Copiare **hpcert.cer** sul computer server nella cartella **<<Configuration Manager installation directory>\java\bin**.
3. Sul server, importare il certificato CA nell'archivio dati attendibile (cacerts) utilizzando l'utilità keytool con il seguente comando:

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

4. Modificare il file **server.xml** (disponibile nella cartella **<<Configuration Manager installation directory>\servers\server-0\conf**) come specificato di seguito:
   a. Apportare le modifiche descritte in "Modificare il file server.xml" a pagina 23.
   b. Eseguire le modifiche, aggiungere i seguenti attributi al connettore HTTPS:

      ```
      truststoreFile="../../java/lib/security/cacerts"
      truststorePass="changeit" />
      ```

   c. Impostare `clientAuth="true"`.
5. Verificare la protezione del server così come descritto in "Verificare la protezione del server" alla pagina precedente.

Abilitare SSL sull'SDK del client

È possibile utilizzare il trasporto HTTPS tra l'SDK del client e del server:

1. Sul computer client, nel prodotto che incorpora l'SDK del client, individuare l'impostazione del trasporto e accertarsi che sia configurata su HTTPS e non su HTTP.
2. Scaricare il certificato CA/certificato pubblico autofirmato nel computer client e importarlo nell'archivio dati attendibile **cacerts** sul JRE che si sta connettendo al server.

   Utilizzare il comando seguente:

```
Keytool -import -alias <nome CA> -trustcacerts -file <percorso
certificato pubblico del server> -keystore <percorso dell'archivio
dati attendibile cacerts di jre (ad es. x:\program
files\java\jre\lib\security\cacerts)>
```

Abilitare l'autenticazione reciproca del certificato per SDK

Questa modalità utilizza il protocollo SSL e consente l'autenticazione del server da parte di UCMDB e l'autenticazione del client da parte del client UCMDB-API. Sia il server sia il client UCMDB-API inviano i certificati all'altra entità per l'autenticazione.

Nota: il metodo seguente per l'abilitazione del protocollo SSL su SDK con l'autenticazione reciproca è il metodo più sicuro ed è quindi la modalità di comunicazione consigliata.

1. Protezione avanzata del connettore del client UCMDB-API in UCMDB:
   a. Per accedere alla JMX Console di UCMDB: Avviare il browser Web e specificare il seguente indirizzo: **http://<nome del computer UCMDB oppure IP>:8080/jmx-console**. È necessario accedere con nome utente e password (il valore predefinito è sysadmin/sysadmin).
   b. Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
   c. Individuare l'operazione **PortsDetails** e fare clic su **Invoke**. Prendere nota dell'HTTPS con il numero di porta di autenticazione del client. Il valore predefinito è 8444 e deve essere abilitato.
   d. Tornare alla pagina Operazioni.
   e. Per mappare il connettore di ucmdb-api alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:
      - **componentName**: ucmdb-api
      - **isHTTPSWithClientAuth**: true
      - Tutti gli altri flag: false

      Viene visualizzato il messaggio seguente:

      ```
      Operazione riuscita. Il componente ucmdb-api è ora mappato a:
      porte HTTPS_CLIENT_AUTH.
      ```
   f. Tornare alla pagina Operazioni.
2. Accertarsi che JRE che esegue il client UCMDB-API abbia un keystore contenente un certificato del client.
3. Esportare il certificato di UCMDB-API dal rispettivo keystore.
4. Importare il certificato del client UCMDB-API esportato nel truststore del server UCMDB.

a. Nel computer di UCMDB copiare il file creato del certificato del client UCMDB-API nella directory seguente su UCMDB:

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

b. Eseguire il seguente comando:

C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <certificato esportato del client UCMDB-api> - alias ucmdb-api

c. Immettere la password del truststore del server UCMDB (valore predefinito **hppass**).

d. Quando viene chiesto **Trust this certificate?** premere **y** e quindi **Invio**.

e. Accertarsi che l'output sia il **Certificato** è stato aggiunto al keystore.

5. Esportare il certificato del server UCMDB dal keystore del server.

a. Nel computer di UCMDB eseguire il comando seguente:

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

b. Immettere la password del truststore del server UCMDB (valore predefinito **hppass**).

c. Verificare che il certificato venga creato nella directory seguente:

C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

6. Importare il certificato di UCMDB esportato nel JRE del truststore del client UCMDB-API.
7. Riavviare il server UCMDB e il client UCMDB-API.
8. Per la connessione dal client UCMDB-API al server UCMDB-API utilizzare il codice seguente:

```
UcmdbServiceProvider provider =
UcmdbServiceFactory.getServiceProvider("https", <SOME_HOST_NAME>,
<HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER (default:8444)>));
UcmdbService ucmdbService = provider.connect
(provider.createCertificateCredentials(<TheClientKeystore. e.g:
"c:\\client.keystore">, <KeystorePassword>),
provider.createClientContext(<ClientIdentification>));
```

Cambiare le password del keystore del server

Dopo aver installato il server, la porta HTTPS è aperta e l'archivio è protetto da una password debole (valore predefinito **hppass**). Per utilizzare soltanto il protocollo SSL è necessario cambiare la password.

La procedura seguente spiega come cambiare soltanto la password di **server.keystore**. Per cambiare la password del **server.truststore** si segue la stessa procedura.

Nota: è necessario eseguire ogni passaggio della procedura.

1. Avviare il server UCMDB.
2. Eseguire la modifica della password nella JMX Console.
   a. Avviare il browser Web e specificare l'indirizzo del server come segue: **http://<nome host del server UCMDB oppure IP>:8080/jmx-console**.

      Potrebbe essere necessario effettuare l'accesso con nome utente e password.

   b. In UCMDB fare clic su **UCMDB:service=Security Services** per aprire la pagina Operazioni.

   c. Individuare ed eseguire l'operazione **changeKeystorePassword**.

      Questo campo non può essere vuoto e deve essere lungo almeno sei caratteri. La password viene cambiata soltanto nel database.
3. Arrestare il server UCMDB.
4. Eseguire i comandi.

   Da **C:\hp\UCMDB\UCMBServer\bin\jre\bin** eseguire i comandi seguenti:

   a. Cambiare le password dell'archivio:

      keytool -storepasswd -new <new_keystore_pass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_ keystore_pass>

   b. Il comando seguente visualizza la chiave interna del keystore. Il primo parametro è l'alias. Salvare questo parametro per il comando successivo:

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

   c. Cambiare la password della chiave (se l'archivio non è vuoto):

      keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   d. Immettere la nuova password.
5. Avviare il server UCMDB.
6. Ripetere la procedura per il truststore del server.

Abilitare o disabilitare le porte HTTP/HTTPS

È possibile abilitare o disabilitare le porte HTTP e HTTPS dall'interfaccia utente o dalla JMX Console.

Per abilitare o disabilitare le porte HTTP/HTTPS dall'interfaccia utente:

1. Accedere ad HP Universal CMDB.
2. Selezionare **Amministrazione > Impostazioni infrastruttura**.
3. Immettere **http** oppure **https** nella casella **Filtro** (per nome) per visualizzare le impostazioni HTTP.
   - **Abilita connessioni HTTP(S)**. **True**: la porta è abilitata. **False**: la porta è disabilitata.

4. Riavviare il server per applicare il cambiamento.

> **Attenzione:** la porta HTTPS è aperta per impostazioni predefinita; la chiusura di questa porta impedisce il funzionamento di **Server_Management.bat**.

Per abilitare o disabilitare le porte HTTP/HTTPS dalla JMX Console:

1. Avviare il browser Web e specificare il seguente indirizzo: http://localhost.<domain_ name>:8080/jmx-console.
2. Immettere le credenziali di autenticazione della JMX Console, che per impostazione predefinita sono:
   - Nome di accesso = **sysadmin**
   - Password = **sysadmin**
3. Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
4. Per abilitare o disabilitare la porta HTTP individuare l'operazione **HTTPSetEnable** e impostare il valore.
   - **True:** la porta è abilitata.
   - **False:** la porta è disabilitata.
5. Per abilitare o disabilitare la porta HTTPS individuare l'operazione **HTTPSSetEnable** e impostare il valore.
   - **True:** la porta è abilitata.
   - **False:** la porta è disabilitata.
6. Per abilitare o disabilitare la porta HTTPS con l'autenticazione del client, individuare l'operazione **HTTPSClientAuthSetEnable** e impostare il valore.
   - **True:** la porta è abilitata.
   - **False:** la porta è disabilitata.

Mappare i componenti Web di UCMDB alle porte

È possibile configurare il mapping di ciascun componente di UCMDB alle porte disponibili dalla JMX Console.

Per visualizzare le configurazioni del componente corrente:

1. Avviare il browser Web e specificare il seguente indirizzo: **http://localhost.<domain_ name>:8080/jmx-console**.
2. Immettere le credenziali di autenticazione della JMX Console, che per impostazione predefinita sono:

   Nome di accesso = **sysadmin**

Password = **sysadmin**

3. Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
4. Individuare il metodo **ComponentsConfigurations** e fare clic su **Invoke**.
5. Per ogni componente vengono visualizzate le porte valide e le porte al momento mappate.

Per mappare i componenti:

1. Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
2. Individuare il metodo **mapComponentToConnectors**.
3. Immettere un nome del componente nella casella Value. Selezionare **True** oppure **False** per ciascuna delle porte corrispondenti alla selezione. Fare clic su **Invoke**. Il componente selezionato viene mappato alle porte selezionate. È possibile trovare i nomi dei componenti richiamando il metodo **serverComponentsNames**.
4. Ripetere la procedura per ciascun componente rilevante.

Nota:

- Ogni componente deve essere mappato ad almeno una porta. Se non viene mappato a una porta, il componente viene mappato alla porta HTTP per impostazione predefinita.
- Se un componente si mappa alla porta HTTPS e alla porta HTTPS con autenticazione del client, solo l'opzione di autenticazione del client viene mappata (l'altra opzione è ridondante in questo caso).

È inoltre possibile cambiare il valore assegnato a ciascuna delle porte.

Per impostare i valori delle porte:

1. Individuare **UCMDB:service=Ports Management Services** e fare clic sul collegamento per aprire la pagina Operazioni.
2. Per impostare un valore per la porta HTTP, individuare il metodo **HTTPSetPort** e immettere un valore nella casella **Valore**. Fare clic su **Invoke**.
3. Per impostare un valore per la porta HTTPS, individuare il metodo **HTTPSSetPort** e immettere un valore nella casella **Valore**. Fare clic su **Invoke**.
4. Per impostare un valore per la porta HTTPS con autenticazione del client, individuare il metodo **HTTPSClientAuthSetPort** e immettere un valore nella casella **Valore**. Fare clic su **Invoke**.

Configurazione di Configuration Manager per utilizzare UCMDB con SSL

È possibile configurare Configuration Manager per utilizzare UCMDB con Secure Sockets Layer (SSL). Il connettore SSL sulla porta 8443 è abilitato per impostazione predefinita in UCMDB.

1. Scegliere **<UCMDB installation directory>\bin\jre\bin** ed eseguire il seguente comando:

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

2. Copiare il file certificato in una posizione temporanea sul computer locale di Configuration Manager.

3. Eseguire una nuova installazione o riconfigurare un'installazione esistente di Configuration Manager. Per le istruzioni, consultare le sezioni pertinenti nella *Guida alla distribuzione di HP Universal CMDB* interattiva.

   Nella schermata di configurazione di UCMDB, impostare il protocollo in HTTPS e scegliere il file certificato copiato nel passaggio 2.

Per configurare Configuration Manager in modo da operare con altri prodotti (ad esempio con piattaforme per il bilanciamento del carico) utilizzando SSL, importare il certificato di protezione del prodotto nel truststore di Configuration Manager (truststore jre predefinito) eseguendo il seguente comando:

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

Abilitare l'adattatore KPI UCMDB da utilizzare con SSL

È possibile configurare le informazioni sull'adattatore KPI UCMDB da inviare con Secure Sockets Layer (SSL).

1. Esportare il certificato di Configuration Manager:

   ```
   <CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
   <CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
   <keystore pass> -file <certificate file name>
   ```

2. Importare il certificato esportato da Configuration Manager nel truststore di UCMDB come segue:

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

3. Importare il certificato esportato da Configuration Manager nel truststore della sonda come segue:

   a. Aprire il prompt dei comandi ed eseguire il comando:

      ```
      <DataFlowProbe dir>\bin\jre\bin\keytool.exe -import -v -keystore
      <DataFlowProbe dir>\conf\security\MAMTrustStoreExp.jks -file
      <certificatefile> -alias tomcat
      ```

   b. Immettere la password del keystore: logomania

c. Quando viene chiesto **Trust this certificate?**, premere **y** e quindi **Invio**.

Viene visualizzato il messaggio seguente:

> **Il certificato è stato aggiunto al keystore.**

Per ulteriori informazioni sulla protezione avanzata della sonda del flusso di dati, consultare "Protezione avanzata della sonda del flusso di dati" a pagina 62.

4. Riavviare UCMDB, la sonda del flusso di dati e Configuration Manager.

Configurazione del supporto SSL per UCMDB Browser

> **Nota:** Le istruzioni fornite in questa sezione si riferiscono alla versione 1.7 di UCMDB Browser. Se si utilizza una versione più recente di UCMDB Browser, aggiornata separatamente dal resto della suite di prodotti UCMDB, per tale versione consultare la sezione sulla configurazione del supporto SSL in *UCMDB Browser Installation and Configuration Guide*.

Per installare l'assistenza SSL sul Tomcat:

1. Creare un file keystore per archiviare la chiave privata e il certificato autofirmato del server eseguendo uno dei seguenti comandi:
   - Per Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - Per Unix: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   Per entrambe i comandi, utilizzare il valore della password **changeit** (per tutti gli altri campi nella finestra di dialogo che si apre, è possibile utilizzare qualsiasi valore).
2. Rimuovere i commenti dalla voce **SSL HTTP/1.1 Connector** in **$CATALINA_BASE/conf/server.xml**, dove **$CATALINA_BASE** è la directory in cui si è installato il Tomcat.

   > **Nota:** Per una descrizione completa su come configurare **server.xml** per l'uso di SSL, consultare il sito ufficiale Apache Tomcat: http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html
3. Riavviare il server Tomcat.

Per utilizzare il protocollo HTTPS per la connessione al server UCMDB:

1. in **ucmdb_browser_config.xml**, assegnare il valore **https** al tag**<protocol>** e assegnare il valore della porta HTTPS al server UCMDB (8443 per impostazione predefinita) al tag **<port>.**
2. Scaricare il certificato pubblico del server UCMDB nel computer di UCMDB Browser (se si usa SSL nel server UCMDB, l'amministratore può fornire questo certificato), e importarlo nell'archivio dati attendibile **cacerts** sul JRE che si collegherà al server eseguendo il seguente comando:

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

dove **<UCMDB-Server-certificate-file>** è il percorso completo al file del certificato pubblico del server UCMDB.

3. Riavviare il server Tomcat.

Capitolo 3

Utilizzo di un proxy inverso

Questo capitolo descrive le ramificazioni della protezione dei proxy inversi e contiene le istruzioni per utilizzare un proxy inverso con HP Universal CMDB e Configuration Manager. Vengono discussi gli aspetti della protezione di un proxy inverso ma non altri aspetti quali la memorizzazione nella cache e il bilanciamento del carico.

Questo capitolo comprende:

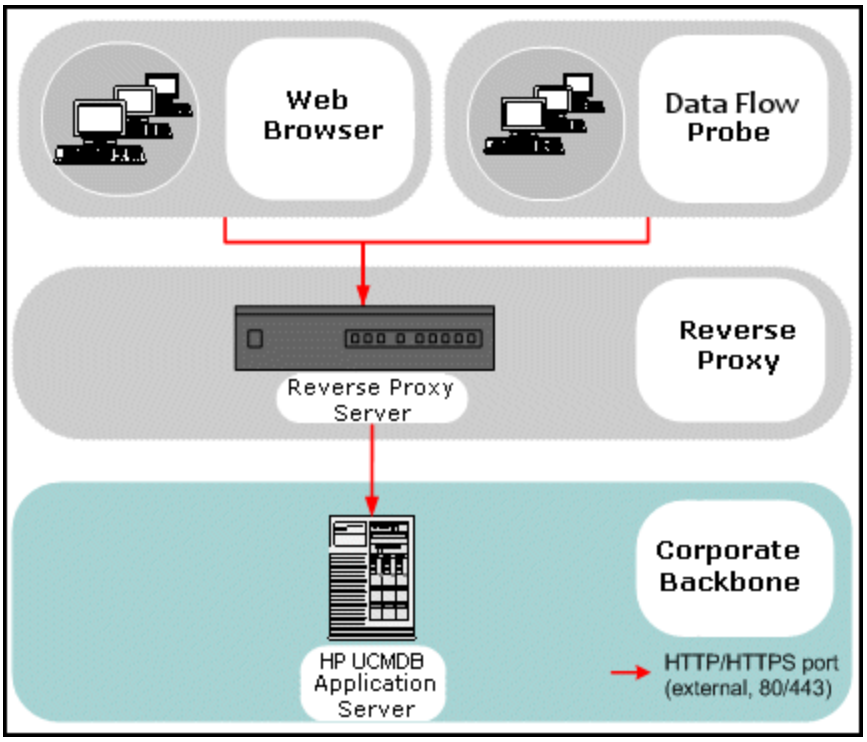
Proxy inverso, panoramica

Un proxy inverso è un server intermedio posizionato tra il client e il server Web. Per il computer client, il proxy inverso è un server Web standard che serve le richieste di protocollo HTTP del client.

Il client invia le richieste ordinarie di contenuto Web utilizzando il nome del proxy inverso invece del nome di un server Web. Il proxy inverso invia la richiesta a uno dei server Web. Anche se la risposta viene reinviata al client dal proxy inverso, per il client appare come inviata dal server Web.

È possibile avere più proxy inversi con diverse URL che rappresentano la stessa istanza UCMDB/CM. In alternativa, è possibile utilizzare un unico server proxy inverso per accedere a più server di UCMDB/CM impostando diversi contesti radice per ogni server UCMDB/CM.

HP Universal CMDB e Configuration Manager supportano un proxy inverso in un'architettura DMZ. Il proxy inverso è un mediatore HTTP tra la sonda del flusso di dati, il client Web e il server HP Universal CMDB/CM.



Nota:

- diversi tipi di proxy inversi richiedono sintassi diverse di configurazione. Per un esempio di configurazione di proxy inverso Apache 2.0.x, consultare " Esempio: Configurazione Apache 2.0.x" a pagina 37.
- La configurazione dell'impostazione dell'URL front-end è necessaria solo quando si crea un collegamento diretto a un report utilizzando l'utilità di pianificazione.

Aspetti di protezione nell'utilizzo di un server proxy inverso

Un server proxy inverso funge da host bastione. Il proxy è configurato per essere l'unico computer al quale si rivolgono direttamente i client esterni e che oscura il resto della rete interna. L'utilizzo di un proxy inverso consente di posizionare il server delle applicazioni su un computer separato nella rete interna.

In questa sezione viene discusso l'utilizzo di un protocollo DMZ e di un proxy inverso in un ambiente con topologia back-to-back.

Di seguito vengono illustrati i vantaggi di protezione principali offerti dall'utilizzo di un proxy inverso in tale ambiente:

- Nessuna conversione di protocollo DMZ. Il protocollo in entrata e il protocollo in uscita sono identici (cambia soltanto l'intestazione).
- È ammesso soltanto l'accesso HTTP al proxy inverso, ovvero i firewall di ispezione del pacchetto con stato sono in grado di proteggere meglio la comunicazione.

- Sul proxy inverso si può definire un set statico e limitato di richieste.
- La maggior parte delle funzioni di protezione del server Web sono disponibili sul proxy server (metodi di autenticazione, crittografia e così via).
- Il proxy inverso visualizza gli indirizzi IP dei server reali nonché l'architettura della rete interna.
- L'unico client accessibile del server Web è il proxy inverso.
- Questa configurazione supporta i firewall NAT (contrariamente ad altre soluzioni).
- Il proxy inverso richiede un numero minimo di porte aperte nel firewall.
- Il proxy inverso fornisce buone prestazioni rispetto ad altre soluzioni bastioni.

Configurare un proxy inverso

Questa sezione descrive come configurare un proxy inverso.

Configurare un proxy inverso utilizzando le impostazioni dell'infrastruttura

La procedura seguente spiega come accedere alle impostazioni dell'infrastruttura per configurare un proxy inverso: Questa configurazione è necessaria solo quando si crea un collegamento diretto a un report utilizzando l'utilità di pianificazione.

Per configurare un proxy inverso:

1. Selezionare **Amministrazione> Impostazioni infrastruttura > categoria Impostazioni generali**.
2. Cambiare l'impostazione URL front-end. Immettere l'indirizzo, ad esempio **https://my_proxy_server:443/**.

Nota: Dopo aver apportato questo cambiamento, non sarà più possibile accedere direttamente al server di HP Universal CMDB da un client. Per cambiare la configurazione del proxy inverso, utilizzare la JMX Console sul server. Per i dettagli consultare "Configurare un proxy inverso utilizzando la JMX Console" di seguito.

Configurare un proxy inverso utilizzando la JMX Console

È possibile apportare modifiche alla configurazione del proxy inverso utilizzando la JMX Console sul server HP Universal CMDB. Questa configurazione è necessaria solo quando si crea un collegamento diretto a un report utilizzando l'utilità di pianificazione.

Per cambiare la configurazione del proxy inverso:

1. Sul computer del server HP Universal CMDB, avviare il browser Web e specificare l'indirizzo seguente:

   http://<nome del computer o indirizzo IP>.<nome_dominio>:8080/jmx-console

   dove **<nome del computer o indirizzo IP>** è il computer su cui è installato HP Universal CMDB. Potrebbe essere necessario effettuare l'accesso con nome utente e password.
2. Fare clic sul collegamento **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

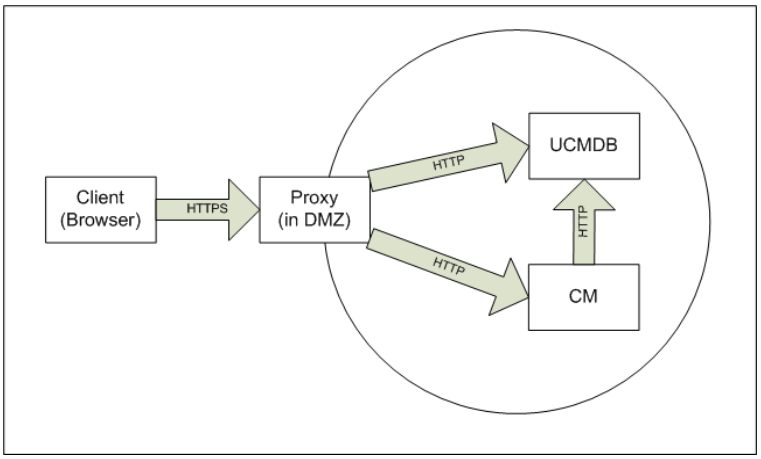
Nel campo **setUseFrontendURLBySettings** immettere l'URL del server proxy ad esempio `https://mio_server_proxy:443/`.

3. Fare clic su **Invoke**.
4. Per visualizzare il valore di questa impostazione, utilizzare il metodo **showFrontendURLInSettings**.

Esempio: Configurazione Apache 2.0.x

In questa sezione viene descritto un file di configurazione di esempio che supporta l'utilizzo di un proxy inverso Apache 2.0.x in un caso in cui le sonde del flusso di dati e gli utenti dell'applicazione si connettono ad HP Universal CMDB.

Il diagramma di seguito mostra il processo di configurazione per un proxy inverso per Configuration Manager e UCMDB.



Nota:

- In questo esempio il nome e la porta DNS del computer di HP Universal CMDB è UCMDB_server.
- In questo esempio, il nome e la porta DNS di HP Configuration Manager è UCMDB_CM_server.
- Soltanto gli utenti che conoscono l'amministrazione di Apache possono eseguire questo cambiamento.

1. Aprire il file **<directory radice del computer Apache>\Webserver\conf\httpd.conf**.
2. Abilitare i moduli seguenti:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
   - **LoadModule headers_module modules/mod_headers.so**
3. Aggiungere le righe seguenti al file httpd.conf:

```
ProxyRequests off

<Proxy *>
```

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

```
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc

ProxyPass /docs http://UCMDB_CM_server/docs

ProxyPassReverse /docs http://UCMDB_CM_server/docs

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

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

ProxyPreserveHost On

RequestHeader set X-Reverse-Proxy "https://<SRP host>:<SRP port>"
```

Nota: la riga `ProxyPreserveHost On` è necessaria solo se esiste un host virtuale.

Attenzione: È fondamentale aggiungere la riga `RequestHeader set X-Reverse-Proxy "https://<SRP host>:<SRP port>"`. Altrimenti questa configurazione non può aver luogo.

4. Salvare le modifiche.

Connessione della sonda del flusso di dati con server proxy inverso o di bilanciamento del carico mediante autenticazione reciproca

Eseguire la procedura seguente per connettere la sonda del flusso di dati mediante un server proxy inverso o di bilanciamento del carico tramite autenticazione reciproca. Questa procedura si applica alla seguente configurazione:

- L'autenticazione reciproca SSL tra la sonda e un server proxy inverso o di bilanciamento del carico in base a un certificato client fornito dalla sonda e richiesto dal server proxy inverso o di bilanciamento del carico.
- Una connessione SSL normale tra il server proxy inverso o di bilanciamento del carico e il server UCMDB.

Nota: le istruzioni seguenti utilizzano il keystore **cKeyStoreFile** come keystore della sonda. Questo è un keystore del client predefinito che fa parte dell'installazione della sonda del flusso di dati e contiene i certificati autofirmati. Per i dettagli consultare "Keystore e truststore predefiniti della sonda del flusso di dati e del server" a pagina 76.

Si consiglia di creare un nuovo keystore univoco contenente una chiave privata generata di nuovo. Per i dettagli consultare "Creare un keystore per la sonda del flusso di dati" a pagina 75.

Ottenere un certificato dall'Autorità di certificazione

Ottenere il certificato radice CA e importarlo nelle seguenti posizioni:

- il truststore della sonda del flusso di dati
- il cacets JVM della sonda del flusso di dati
- il truststore del server UCMDB
- il truststore del proxy inverso

1. Importare il certificato radice di UCMDB nel truststore della sonda del flusso di dati.
   a. Posizionare il certificato radice CA nella seguente directory: <Directory di installazione della sonda del flusso di dati>\conf\security\<certificate file name>.
   b. Importare il certificato radice nel truststore della sonda del flusso di dati eseguendo il seguente script:

      ```
      <Directory di installazione della sonda del flusso di
      dati>\bin\jre\bin\keytool.exe -import -trustcacerts -alias
      <YourAlias> -file
      C:\hp\UCMDB\DataFlowProbe\conf\security\<certificate file name>
      -keystore <Directory di installazione della sonda del flusso di
      dati>\conf\security\MAMTrustStoreExp.jks
      ```

      La password predefinita è: **logomania**.
2. Importare il certificato radice CA nel cacerts della sonda del flusso di dati eseguendo il seguente script:

   ```
   <Directory di installazione della sonda del flusso di
   dati>\bin\jre\bin\keytool.exe -import -trustcacerts -alias
   <YourAlias> -file <Directory di installazione della sonda del
   flusso di dati>\conf\security\<certificate file name> -keystore
   <Directory di installazione della sonda del flusso di
   dati>\bin\jre\lib\security\cacerts
   ```

   La password predefinita è: **changeit**.
3. Importare il certificato radice CA nel truststore di UCMDB.
   a. Posizionare il certificato radice CA nella seguente directory: <UCMDB installation directory>\conf\security\<certificate file name>.
   b. Importare il certificato radice CA nel truststore di UCMDB eseguendo il seguente script:

      ```
      <UCMDB installation directory>\bin\jre\bin\keytool.exe -import -
      trustcacerts -alias <YourAlias> -file <UCMDB installation
      directory>\conf\security\<ceritificate file name> -keystore
      <UCMDB installation directory>\conf\security\sever.truststore
      ```

      La password predefinita è: **hppass**.
4. Importare il certificato radice CA nel truststore del proxy inverso. Questo passaggio dipende dal fornitore.

Convertire il certificato in un keystore Java

Ottenere il certificato client (e la chiave privata) per la sonda del flusso di dati dall'Autorità di certificazione (CA) nel formato PFX/PKCS12 e convertirlo in un keystore Java eseguendo il seguente script:

```
<Directory di installazione della sonda del flusso di
dati>\bin\jre\bin\keytool.exe -importkeystore -srckeystore <PFX
keystore full path> -destkeystore <new destination keystore full path>
-srcstoretype PKCS12
```

Verranno chieste le password del keystore di origine e di destinazione.

Per la password keystore di origine, utilizzare la stessa password che è stata utilizzata durante l'esportazione del keystore PFX.

La password del keystore di destinazione predefinito per il keystore della sonda del flusso di dati è: **logomania**.

Nota: se si inserisce una password del keystore di destinazione diversa da quella predefinita (logomania), sarà necessario fornirla ndl formato crittografato nel file **<Directory di installazione della sonda del flusso di dati>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Per i dettagli consultare "Crittografare le password del keystore e del truststore della sonda" a pagina 76.

Posizionare il nuovo keystore nella seguente directory: **<Directory di installazione della sonda del flusso di dati>\conf\security**.

Attenzione: non sovrascrivere il file **MAMKeyStoreExp.jks**.

Cambiare il file delle proprietà SSL per utilizzare il keystore appena creato

Impostare il keystore contenente il certificato client nel file **<Directory di installazione della sonda del flusso di dati>\conf\ssl.properties** in **javax.net.ssl.keyStore**.

Se la password al keystore non è quella predefinita del keystore della sonda del flusso di dati (logomania), aggiornare **javax.net.ssl.keyStorePassword** dopo la crittografia. Per i dettagli su come crittografare la password, consultare "Crittografare le password del keystore e del truststore della sonda" a pagina 76.

Esaminare la configurazione della sonda del flusso di dati

Modificare il file **<Directory di installazione della sonda del flusso di dati>\conf\DataFlowProbe.properties** come segue:

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

serverName = <indirizzo server proxy inverso>

serverPortHttps = <porta HTTPS sulla quale il proxy inverso è in
ascolto per reindirizzare le richieste a UCMDB>
```

Configurare UCMDB per utilizzarlo con SSL

Per i dettagli consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pagina 18.

Se il certificato del server UCMDB viene creato dallo stesso CA che ha creato il resto dei certificati di questa procedura, il server proxy inverso o di bilanciamento del carico rende attendibile il certificato UCMDB.

Capitolo 4

Gestione credenziali del flusso di dati

Questo capitolo comprende:

Gestione delle credenziali del flusso di dati, panoramica

Per eseguire l'individuazione o l'integrazione è necessario impostare le credenziali di accesso al sistema remoto. Le credenziali sono configurate nella finestra Impostazione della sonda del flusso di dati nel server UCMDB. Per i dettagli, consultare la sezione che descrive l'impostazione della sonda del flusso di dati nella *Guida Gestione flusso dati di HP Universal CMDB*.

L'archiviazione delle credenziali viene gestita dal componente Confidential Manager. Per i dettagli consultare "Confidential Manager" a pagina 90.

La sonda del flusso di dati può accedere alle credenziali utilizzando il client Confidential Manager. Il client Confidential Manager risiede nella sonda del flusso di dati e comunica con il server Confidential Manager che risiede nel server UCMDB. La comunicazione tra il client Confidential Manager e il server Confidential Manager è crittografata e l'autenticazione viene richiesta dal client Confidential Manager al momento della connessione al server Confidential Manager.

L'autenticazione del client Confidential Manager sul server Confidential Manager si basa su un componente LW-SSO. Prima della connessione al server Confidential Manager, il client Confidential Manager invia prima un cookie LW-SSO. Il server Confidential Manager verifica il cookie e dopo l'esito positivo viene avviata la comunicazione con il client Confidential Manager. Per i dettagli sul LW-SSO consultare "Configurazione delle impostazioni di LW-SSO" a pagina 47.

La comunicazione tra il client Confidential Manager e il server Confidential Manager viene crittografata. Per i dettagli sull'aggiornamento della configurazione della crittografia consultare "Configurare la crittografia della comunicazione di Confidential Manager " a pagina 47.

Attenzione: L'autenticazione del Confidential Manager utilizza l'orario universale definito sul computer (UTC). Per procedere all'autenticazione, assicurarsi che l'orario universale sulla sonda del flusso di dati e del server UCMDB sia lo stesso. Il server e la sonda possono trovarsi in fusi orari diversi come UTC è indipendente dal fuso orario e dall'ora legale.

Il client Confidential Manager gestisce una cache locale delle credenziali. Il client Confidential Manager è configurato per il download di tutte le credenziali dal server Confidential Manager e la memorizzazione in una cache. I cambiamenti delle credenziali vengono automaticamente sincronizzate dal server Confidential Manager su base continua. La cache può essere un file-system o una cache in memoria a seconda delle impostazioni preconfigurate. Inoltre la cache viene crittografata e non vi si può accedere dall'esterno. Per i dettagli sull'aggiornamento delle

impostazioni della cache consultare "Configurare la modalità della cache del client Confidential Manager sulla sonda" a pagina 51. Per i dettagli sull'aggiornamento della crittografia della cache consultare "Configurare le impostazioni della crittografia della cache del client Confidential Manager sulla sonda" a pagina 52.

Per i dettagli sulla risoluzione dei problemi consultare "Cambiare il livello di messaggi del file di registro del client Confidential Manager" a pagina 54.

Le informazioni sulle credenziali si possono copiare da un server UCMDB a un altro. Per i dettagli consultare "Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato" a pagina 53.

Nota: il **DomainScopeDocument** (DSD) utilizzato per la memorizzazione delle credenziali sulla sonda (in UCMDB versione 9.01 o precedente) non contiene più alcuna informazione sensibile sulle credenziali. Il file ora contiene un elenco di sonde e informazioni sugli intervalli di rete. Contiene anche un elenco di voci di credenziali per ogni dominio, dove ogni voce include soltanto l'ID delle credenziali e un intervallo di rete (definito per questa voce di credenziale).

In questa sezione vengono trattati i seguenti argomenti:

Ipotesi di protezione di base

Tenere presente l'ipotesi di protezione seguente:

È stato protetto il server UCMDB e la JMX Console della sonda per consentire l'accesso al sistema UCMDB soltanto agli amministratori, preferibilmente tramite soltanto l'accesso localhost.

Sonda del flusso di dati in esecuzione in modalità separata

Quando Probe Gateway e Probe Manager vengono eseguiti come processi separati, il componente del client Confidential Manager diventa parte del processo di Probe Manager. Le informazioni sulle credenziali vengono memorizzate nella cache e vengono utilizzate soltanto da Probe Manager. Per accedere al server Confidential Manager sul sistema UCMDB la richiesta del client Confidential Manager viene gestita dal processo Gateway e da qui viene inoltrata al sistema UCMDB.

Questa configurazione è automatica quando la sonda è configurata in modalità separata.

Tenere aggiornata la cache delle credenziali

Alla prima connessione riuscita al server Confidential Manager, il client Confidential Manager scarica tutte le credenziali rilevanti (tutte le credenziali configurate nel dominio della sonda). Dopo la prima comunicazione riuscita, il client Confidential Manager mantiene la sincronizzazione

continua con il server Confidential Manager. La sincronizzazione differenziale viene eseguita a intervalli di un minuto durante i quali vengono sincronizzate soltanto le differenze tra il server Confidential Manager e il client Confidential Manager. Se vengono cambiate le credenziali sul lato del server UCMDB (ad esempio con l'aggiunta di nuove credenziali o con l'aggiornamento o l'eliminazione di credenziali esistenti), il client Confidential Manager riceverà una notifica immediata dal server UCMDB ed eseguirà operazioni aggiuntive di sincronizzazione.

Sincronizzazione di tutte le sonde con i cambiamenti di configurazione

Per la comunicazione corretta è necessario aggiornare il client Confidential Manager con la configurazione dell'autenticazione del server Confidential Manager (stringa init di LW-SSO) e la configurazione della crittografia (crittografia della comunicazione di Confidential Manager). Ad esempio, quando init string viene cambiata sul server, la sonda deve conoscere la nuova stringa init per autenticarla.

Il server UCMDB controlla costantemente i cambiamenti nella configurazione della crittografia di comunicazione di Confidential Menager e la configurazione dell'autenticazione di Confidential Manager. Questo controllo viene eseguito ogni 15 secondi; in caso di cambiamento la configurazione aggiornata viene inviata alle sonde. La configurazione viene passata alle sonde in forma crittografata e memorizzata lato sonda nell'archiviazione protetta. La crittografia della configurazione inviata viene eseguita utilizzando una chiave di crittografia simmetrica. Per impostazione predefinita il server UCMDB e la sonda del flusso di dati vengono installati con la stessa chiave di crittografia simmetrica predefinita. Per una protezione ottimale si consiglia di cambiare questa chiave prima di aggiungere credenziali al sistema. Per i dettagli consultare "Generare o aggiornare la chiave di crittografia" a pagina 55.

Nota: A causa dell'intervallo di controllo di 15 secondi, è possibile che il client Confidential Manager la sonda non venga aggiornato con l'ultima configurazione per un periodo di 15secondi.

Se si sceglie di disabilitare la sincronizzazione automatica della configurazione dell'autenticazione e della comunicazione di Confidential Manager tra il server UCMDB e la sonda del flusso di dati, ogni volta che si aggiorna la configurazione dell'autenticazione e della comunicazione sul lato del server UCMDB sarà necessario aggiornare anche tutte le sonde con la nuova configurazione. Per i dettagli consultare "Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde" a pagina 49.

Archiviazione protetta sulla sonda

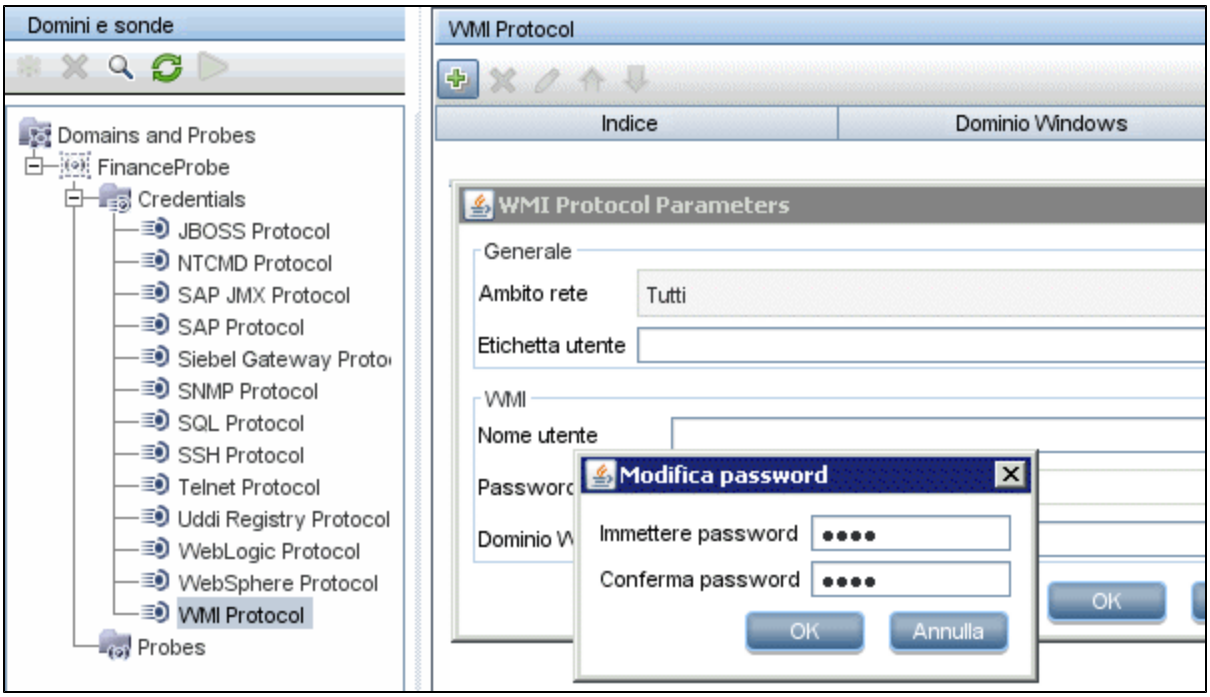
Tutte le informazioni sensibili (ad esempio la configurazione dell'autenticazione e della comunicazione di Confidential Manager e la chiave di crittografia) vengono memorizzate sulla sonda in archiviazione protetta nel file **secured_storage.bin** che si trova nella directory **C:\hp\UCMDB\DataFlowProbe\conf\security**. Questa archiviazione protetta viene crittografata utilizzando il metodo DPAPI che si basa sulla password utente di Windows nel processo di crittografia. DPAPI è un metodo standard utilizzato per proteggere i dati riservati come ad esempio i certificati e le chiavi private sui sistemi Windows. La sonda deve essere sempre eseguita con lo

stesso utente di Windows in modo che, anche se viene cambiata la password, la sonda può continuare a leggere le informazioni memorizzate nell'archiviazione protetta.

Visualizzazione dei dati delle credenziali

Nota: Questa sezione riguarda la visualizzazione delle informazioni sulle credenziali quando la direzione dei dati è da CMDB a HP Universal CMDB

Le password non vengono inviate dal database CMDB all'applicazione. Quindi HP Universal CMDB visualizza gli asterischi (*) nel campo della password a prescindere dal contenuto:



Aggiornamento delle credenziali

Nota: Questa sezione riguarda l'aggiornamento delle credenziali quando la direzione dei dati è da HP Universal CMDB in CMDB.

- La comunicazione in questa direzione non è crittografata quindi è necessario connettersi al server UCMDB utilizzando https\SSL oppure una connessione mediante una rete sicura.

  Anche se la comunicazione non è crittografata, le password non vengono inviate come testo in chiaro sulla rete. Vengono crittografate utilizzando una chiave predefinita e quindi si consiglia di utilizzare SSL per una riservatezza efficace in transito.

- È possibile utilizzare caratteri speciali e caratteri non inglesi come password.

Configurare le impostazioni dell'autenticazione e della crittografia del client Confidential Manager

Questa attività descrive come configurare le impostazioni dell'autenticazione e della crittografia del client Confidential Manager sul server UCMDB e comprende i passaggi seguenti:

- "Configurazione delle impostazioni di LW-SSO" nel seguito
- "Configurare la crittografia della comunicazione di Confidential Manager " nel seguito

Configurazione delle impostazioni di LW-SSO

Questa procedura descrive come cambiare la stringa init di LW-SSO sul server UCMDB. Questo cambiamento viene automaticamente inviato alle sonde (come stringa crittografata) a meno che il server UCMDB non sia configurato in tal senso. Per i dettagli consultare "Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde" a pagina 49.

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console**.
2. Fare clic su **UCMDB-UI:name=LW-SSO Configuration** per aprire la pagina JMX MBEAN View.
3. Individuare il metodo **setInitString**.
4. Immettere una nuova stringa init di LW-SSO.
5. Fare clic su Invoke.

Configurare la crittografia della comunicazione di Confidential Manager

Questa procedura descrive come cambiare le impostazioni della crittografia della comunicazione di Confidential Manager sul server UCMDB. Queste impostazioni specificano come viene crittografata la comunicazione tra il client e il server Confidential Manager. Questo cambiamento viene automaticamente inviato alle sonde (come stringa crittografata) a meno che il server UCMDB non sia configurato in tal senso. Per i dettagli consultare "Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde" a pagina 49.

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console.**
2. Fare clic su **UCMDB:service=Security Services** per aprire la pagina JMX MBEAN View.
3. Fare clic sul metodo **CMGetConfiguration**.
4. Fare clic su **Invoke**.

   Viene visualizzato l'XML della configurazione corrente di Confidential Manager.

5. Copiare i contenuti dell'XML visualizzato.
6. Tornare alla pagina JMX MBean View **Security Services**.
7. Fare clic sul metodo **CMSetConfiguration**.
8. Incollare l'XML copiato nel campo **Valore**
9. Aggiornare le impostazioni rilevanti relative al trasporto.

   Per i dettagli sui valori che si possono aggiornare consultare "Impostazioni della crittografia di Confidential Manager" a pagina 59.

   Esempio:

```
<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. Fare clic su **Invoke**.

Configurare manualmente le impostazioni dell'autenticazione e della crittografia del client Confidential Manager sulla sonda

Questo compito include i seguenti passaggi:

Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde

Per impostazione predefinita il server UCMDB è configurato sull'invio automatico delle impostazioni di Confidential Manager/LW-SSO alle sonde. Queste informazioni vengono inviate come stringa crittografata alle sonde che decrittografa le informazioni al momento del recupero. È possibile configurare il server UCMDB sull'invio non automatico dei file di configurazione di Confidential Manager/LW-SSO alle sonde. In questo caso è responsabilità di chi opera eseguire l'aggiornamento manuale di tutte le sonde con le nuove impostazioni di Confidential Manager/LW-SSO.

Per disabilitare la sincronizzazione automatica delle impostazioni di Confidential Manager/LWSSO:

1. In UCMDB, fare clic su **Amministrazione > Gestione impostazioni infrastruttura > General Settings**.
2. Selezionare **Abilita la sincronizzazione automatica della configurazione di CM/LW-SSO e la stringa init con la sonda.**
3. Fare clic sul campo **Valore** e cambiare **True** in **False**.
4. Fare clic sul pulsante **Save**.
5. Riavviare il server UCMDB.

Configurare le impostazioni dell'autenticazione e della crittografia del client Confidential Manager sulla sonda

Questa procedura è rilevante se il server UCMDB è stato configurato per non inviare la configurazione e le impostazioni di LW-SSO/Confidential Manager alle sonde. Per i dettagli consultare "Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde" in precedenza.

1. Sul computer della sonda avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:1977**.

   Nota: Se Probe Manager e Probe Gateway sono in esecuzione come processi separati,

nel computer che esegue Probe Manager l'indirizzo deve essere immesso come segue: **http://localhost:1978**.

2. Fare clic su **type=CMClient** per aprire la pagina JMX MBEAN View.
3. Individuare il metodo **setLWSSOInitString** e fornire la stessa stringa init fornita per la configurazione di LW-SSO di UCMDB.
4. Fare clic sul pulsante **setLWSSOInitString**.

Configurare la crittografia della comunicazione di Confidential Manager sulla sonda

Questa procedura è rilevante se il server UCMDB è stato configurato per non inviare la configurazione e le impostazioni di LW-SSO/Confidential Manager alle sonde. Per i dettagli consultare "Disabilitare la sincronizzazione automatica delle impostazioni dell'autenticazione e della crittografia del client Confidential Manager tra il server e le sonde" alla pagina precedente.

1. Sul computer della sonda avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:1977**.

   Nota: Se Probe Manager e Probe Gateway sono in esecuzione come processi separati, nel computer che esegue Probe Manager l'indirizzo deve essere immesso come segue: **http://localhost:1978**.

2. Fare clic su **type=CMClient** per aprire la pagina JMX MBEAN View.
3. Aggiornare le impostazioni rilevanti relative al trasporto:

   Nota: è necessario aggiornare le stesse impostazioni aggiornate sul server UCMDB. Per eseguire questa operazione alcuni metodi che si aggiornano sulla sonda possono richiedere più di un parametro. Per visualizzare la configurazione corrente della sonda fare clic su **displayTransportConfiguration** nella pagina JMX MBEAN View. Per i dettagli consultare "Configurare la crittografia della comunicazione di Confidential Manager " a pagina 47. Per i dettagli sui valori che si possono aggiornare consultare "Impostazioni della crittografia di Confidential Manager" a pagina 59.

   a. **setTransportInitString** cambia l'impostazione **encryptDecryptInitString**.
   b. **setTransportEncryptionAlgorithm** cambia le impostazioni di Confidential Manager sulla sonda in base alla mappa seguente:
      - **Engine name** si riferisce alla voce <engineName>
      - **Key size** si riferisce alla voce <keySize>
      - **Algorithm padding name** si riferisce alla voce <algorithmPaddingName>
      - **PBE count** si riferisce alla voce <pbeCount>
      - **PBE digest algorithm** si riferisce alla voce <pbeDigestAlgorithm>

c. **setTransportEncryptionLibrary** cambia le impostazioni di Confidential Manager sulla sonda in base alla mappa seguente:

- **Encryption Library name** si riferisce alla voce <cryptoSource>
- **Support previous lightweight cryptography versions** si riferisce alla voce <lwJCEPBECompatibilityMode>

d. **setTransportMacDetails** cambia le impostazioni di Confidential Manager sulla sonda in base alla mappa seguente:

- **Use MAC with cryptography** si riferisce alla voce <useMacWithCrypto>
- **MAC key size** si riferisce alla voce <macKeySize>

4. Fare clic sul pulsante **reloadTransportConfiguration** per rendere effettivi i cambiamenti sulla sonda.

Per i dettagli sulle diverse impostazioni e i possibili valori consultare "Impostazioni della crittografia di Confidential Manager" a pagina 59.

Configurare la cache del client Confidential Manager

Questo compito include i seguenti passaggi:

- "Configurare la modalità della cache del client Confidential Manager sulla sonda" nel seguito
- "Configurare le impostazioni della crittografia della cache del client Confidential Manager sulla sonda" alla pagina successiva

Configurare la modalità della cache del client Confidential Manager sulla sonda

Il client Confidential Manager memorizza le informazioni sulle credenziali nella cache e le aggiorna quando le informazioni cambiano sul server. La cache può essere memorizzata nel file system o nella memoria:

- **Quando vengono memorizzate nel file system**, anche se la sonda viene riavviata e non si può connettere al server, le informazioni sulle credenziali sono ancora disponibili.
- **Quando sono memorizzate nella memoria**, se la sonda viene riavviata, la memoria viene cancellata e tutte le informazioni vengono recuperate di nuovo dal server. Se il server non è disponibile, la sonda non include alcuna credenziale quindi non può essere eseguita alcuna individuazione o integrazione.

Per cambiare questa impostazione:

1. Aprire il file **DataFlowProbe.properties** in un editor di testo. Il file si trova nella cartella **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Individuare l'attributo seguente:
com.hp.ucmdb.discovery.common.security.storeCMData=true

- Per memorizzare le informazioni sul file system, lasciare il valore predefinito (**true**).
- Per memorizzare le informazioni in memoria, immettere **false**.

3. Salvare il file **DataFlowProbe.properties**.
4. Riavviare la sonda.

Configurare le impostazioni della crittografia della cache del client Confidential Manager sulla sonda

Questa procedura descrive come cambiare le impostazioni della crittografia del file della cache del file system del client Confidential Manager. Tenere presente che cambiare le impostazioni della crittografia per la cache del file system del client Confidential Manager comporta la nuova creazione del file della cache del file system. Questo processo di nuova creazione richiede il riavvio della sonda e la sincronizzazione completa con il server UCMDB.

1. Sul computer della sonda avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:1977**.

   Nota: Se Probe Manager e Probe Gateway sono in esecuzione come processi separati, nel computer che esegue Probe Manager l'indirizzo deve essere immesso come segue: **http://localhost:1978**.

2. Fare clic su **type=CMClient** per aprire la pagina JMX MBEAN View.
3. Aggiornare le impostazioni seguenti relative alla cache:

   Nota: alcuni metodi che si aggiornano sulla sonda possono richiedere più di un parametro. Per visualizzare la configurazione corrente della sonda fare clic su **displayCacheConfiguration** nella pagina JMX MBEAN View.

   a. **setCacheInitString** cambia la cache del file system <encryptDecryptInitString> setting.
   b. **setCacheEncryptionAlgorithm** cambia le impostazioni della cache del file system in base alla mappa seguente:
      - **Engine name** si riferisce alla voce <engineName>
      - **Key size** si riferisce alla voce <keySize>
      - **Algorithm padding name** si riferisce alla voce <algorithmPaddingName>
      - **PBE count** si riferisce alla voce <pbeCount>
      - **PBE digest algorithm** si riferisce alla voce <pbeDigestAlgorithm>
   c. **setCacheEncryptionAlgorithm** cambia le impostazioni della cache del file system in base alla mappa seguente:
      - **Encryption Library name** si riferisce alla voce <cryptoSource>
      - **Support previous lightweight cryptography versions** si riferisce alla voce <lwJCEPBECompatibilityMode>

d. **setCacheMacDetails** cambia le impostazioni della cache del file system in base alla mappa seguente:

- **Use MAC with cryptography** si riferisce alla voce <useMacWithCrypto>
- **MAC key size** si riferisce alla voce <macKeySize>

4. Fare clic sul pulsante **reloadCacheConfiguration** per rendere effettivi i cambiamenti sulla sonda. Ciò comporta il riavvio della sonda.

> **Nota:** accertarsi che nessun processo sia in esecuzione sulla sonda durante questa azione.

Per i dettagli sulle diverse impostazioni e i possibili valori consultare "Impostazioni della crittografia di Confidential Manager" a pagina 59.

Esportare e importare le informazioni sulle credenziali e sull'intervallo in formato crittografato

È possibile esportare e importare le informazioni sulle credenziali e sull'intervallo di rete in formato crittografato per copiare le informazioni sulle credenziali da un server UCMDB a un altro. Ad esempio si potrebbe eseguire questa operazione durante il ripristino in seguito a un arresto del sistema oppure durante l'aggiornamento.

- **Quando si esportano le informazioni sulle credenziali,** è necessario immettere una password (a scelta dell'utente). Le informazioni vengono crittografate con questa password.
- **Quando si importano le informazioni sulle credenziali,** è necessario utilizzare la stessa password definita quando è stato esportato il file DSD.

> **Nota:** il documento delle credenziali esportate contiene anche le informazioni sugli intervalli definite nel sistema dal quale è stato esportato il documento. Durante l'importazione del documento sulle credenziali vengono importante anche le informazioni sull'intervallo.

> **Attenzione:** Per importare le informazioni sulle credenziali da un domainScopeDocument di UCMDB versione 8.02 è necessario utilizzare il file key.bin che si trova nel sistema versione 8.02.

Per esportare le informazioni sulle credenziali dal server UCMDB:

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console**. Potrebbe essere necessario effettuare l'accesso con nome utente e password.
2. Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.
3. Individuare l'operazione **exportCredentialsAndRangesInformation**. Procedere come segue:

- Immettere l'ID del cliente (l'impostazione predefinita è 1).
- Immettere un nome per il file esportato.
- Immettere la password.
- Impostare **isEncrypted=True** se si desidera crittografare il file esportato con la password fornita oppure **isEncrypted=False** se si desidera non crittografare il file esportato (in tal caso le password e altre informazioni sensibili non vengono esportate).

4. Fare clic su **Invoke** per eseguire l'esportazione.

   Quando il processo di esportazione viene completato correttamente, il file viene salvato nella posizione seguente: **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

Per importare le informazioni sulle credenziali dal server UCMDB:

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console**.

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

2. Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.
3. Procedere con una delle seguenti operazioni:
   - Individuare l'operazione **importCredentialsAndRangesInformation** se il file che si sta importando è stato esportato da un server UCMDB successivo alla versione 8.02.
   - Individuare l'operazione **importCredentialsAndRangesWithKey** se il file che si sta importando è stato esportato da un server UCMDB versione 8.02.
4. Immettere l'ID del cliente (l'impostazione predefinita è 1).
5. Immettere il nome del file da importare. Questo file deve essere individuato in **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.
6. Immettere la password. Deve essere la stessa password utilizzata al momento dell'esportazione del file.
7. Se il file è stato esportato da un sistema UCMDB versione 8.02, immettere il nome file **key.bin**. Questo file deve trovarsi in **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**, insieme al file da importare.
8. Fare clic su **Invoke** per importare le credenziali.

Cambiare il livello di messaggi del file di registro del client Confidential Manager

La sonda fornisce due file di registro che contengono informazioni sulla comunicazione relativa a Confidential Manager tra il server e il client Confidential Manager. I file sono:

- "File di registro del client Confidential Manager" alla pagina successiva
- "File di registro LW-SSO" alla pagina successiva

File di registro del client Confidential Manager

Il file **security.cm.log** si trova nella cartella **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Il registro contiene i messaggi informativi scambiati tra il server Confidential Manager e il client Confidential Manager. Per impostazione predefinita, il livello di registro di questi messaggi è impostato su INFO.

Per cambiare il livello di registro di questi messaggi sul livello DEBUG:

1. Nel server di gestione della sonda del flusso di dati passare a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Aprire il file **security.properties** in un editor di testo.
3. Cambiare la riga:

   `loglevel.cm=INFO`

   in:

   `loglevel.cm=DEBUG`
4. Salvare il file.

File di registro LW-SSO

Il file **security.lwsso.log** si trova nella cartella **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Il registro contiene i messaggi informativi relativi a LW-SSO. Per impostazione predefinita, il livello di registro di questi messaggi è impostato su INFO.

Per cambiare il livello di registro di questi messaggi sul livello DEBUG:

1. Nel server di gestione della sonda del flusso di dati passare a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Aprire il file security.properties in un editor di testo.
3. Cambiare la riga:

   `loglevel.lwsso=INFO`

   in:

   `loglevel.lwsso=DEBUG`
4. Salvare il file.

Generare o aggiornare la chiave di crittografia

È possibile generare o aggiornare una chiave di crittografia da utilizzare per la crittografia o la decrittografia delle configurazioni dell'autenticazione e della comunicazione di Confidential Manager scambiate tra il server UCMDB e la sonda del flusso di dati. In ogni caso (generazione o aggiornamento), il server UCMDB crea una nuova chiave di crittografia in base ai parametri forniti (ad esempio lunghezza della chiave, cicli extra PBE, provider JCE) e la distribuisce nelle sonde.

Il risultato di esecuzione del metodo **generateEncryptionKey** è una nuova chiave di crittografia generata. Questa chiave viene memorizzata soltanto nell'archiviazione protetta e i rispettivi nome e dettagli non sono noti. Se si reinstalla una sonda del flusso di dati esistente o si connette una nuova sonda al server UCMDB, la nuova chiave generata non viene riconosciuta dalla nuova sonda. In questi casi è preferibile utilizzare il metodo **changeEncryptionKey** per cambiare le chiavi di crittografia. In questo modo, quando si reinstalla una sonda o si installa una nuova sonda è possibile importare la chiave esistente (nome e posizione sono noti) eseguendo il metodo **importEncryptionKey** sulla JMX Console della sonda.

Nota:

- La differenza tra i metodi utilizzati per creare una chiave (**generateEncryptionKey**) e aggiornare una chiave (**changeEncryptionKey**) è che **generateEncryptionKey** crea una nuova chiave di crittografia casuale mentre **changeEncryptionKey** importa una chiave di crittografia con il nome che gli viene fornito.
- Su un sistema può esistere una sola chiave di crittografia, indipendentemente dal numero di sonde installate.

Questo compito include i seguenti passaggi:

- "Generare una nuova chiave di crittografia" nel seguito
- "Aggiornare una chiave di crittografia su un server UCMDB" alla pagina successiva
- "Aggiornare una chiave di crittografia su una sonda" a pagina 58
- "Cambiare manualmente la chiave di crittografia quando Probe Manager e Probe Gateway sono installati su computer diversi" a pagina 59
- "Definire diversi provider JCE" a pagina 59

Generare una nuova chiave di crittografia

È possibile generare una nuova chiave che utilizzano il server UCMDB e la sonda del flusso di dati per la crittografia o la decrittografia. Il server UCMDB sostituisce la chiave precedente con la nuova chiave generata e distribuisce questa chiave tra le sonde.

Per generare una nuova chiave di crittografia mediante la JMX Console:

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console**.

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

2. Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.
3. Individuare l'operazione generateEncryptionKey.
   a. Nella casella del parametro **customerId** immettere 1 (valore predefinito).
   b. Per **keySize** indicare la lunghezza della chiave di crittografia. Valori validi sono 128, 192 o 256.
   c. Per **usePBE** specificare **True** o **False**:

- **True:** utilizzare ulteriori cicli hash PBE.
- **False:** non utilizzare ulteriori cicli hash PBE.

d. Per **jceVendor** è possibile scegliere di utilizzare un provider JCE non predefinito. Se la casella è vuota, viene utilizzato il valore predefinito.

e. Per **autoUpdateProbe** specificare **True** o **False**:

- **True:** il server distribuisce automaticamente la nuova chiave alle sonde.
- **False:** la nuova chiave deve essere posizionata manualmente nelle sonde.

f. Per **exportEncryptionKey** specificare **True** o **False**.

- **True:** oltre a creare la nuova password e a memorizzarla nell'archiviazione protetta, il server esporta la nuova password nel file system (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Questa opzione consente di aggiornare le sonde manualmente con la nuova password.
- **False:** la nuova password non viene esportata nel file system. Per aggiornare le sonde manualmente, impostare **autoUpdateProbe** su False e **exportEncryptionKey** su True.

> **Nota:** accertarsi che la sonda sia in funzione e connessa al server. Se la sonda non è in funzione la chiave non può arrivare alla sonda. Se si cambia la chiave prima che la sonda si arresti, quando la sonda torna di nuovo in funzione la chiave viene inviata di nuovo alla sonda. Tuttavia, se la chiave viene cambiata più di una volta prima che la sonda si arresti, è necessario cambiare la chiave manualmente mediante la JMX Console. (Selezionare **False** per **exportEncryptionKey**).

4. Fare clic su **Invoke** per generare la chiave di crittografia.

Aggiornare una chiave di crittografia su un server UCMDB

Utilizzare il metodo **changeEncryptionKey** per importare la chiave di crittografia nel server UCMDB e distribuirla tra le sonde.

Per aggiornare una chiave di crittografia mediante la JMX Console:

1. Sul server UCMDB avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:8080/jmx-console.**

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

2. Fare clic su **UCMDB:service=DiscoveryManager** per aprire la pagina JMX MBEAN View.
3. Individuare l'operazione **changeEncryptionKey**.

   a. Nella casella del parametro **customerId** immettere **1** (valore predefinito).

   b. Per **newKeyFileName** immettere il nome della nuova chiave.

   c. Per **keySizeInBits** indicare la lunghezza della chiave di crittografia. Valori validi sono 128,

192 o 256.

d. Per **usePBE** specificare **True** o **False**:

- **True:** utilizzare ulteriori cicli hash PBE.
- **False:** non utilizzare ulteriori cicli hash PBE.

e. Per **jceVendor** è possibile scegliere di utilizzare un provider JCE non predefinito. Se la casella è vuota, viene utilizzato il valore predefinito.

f. Per **autoUpdateProbe** specificare **True** o **False**:

- **True:** il server distribuisce automaticamente la nuova chiave alle sonde.
- **False:** la nuova chiave deve essere distribuita manualmente utilizzando la JMX Console della sonda.

> **Nota:** accertarsi che la sonda sia in funzione e connessa al server. Se la sonda non è in funzione la chiave non può arrivare alla sonda. Se si cambia la chiave prima che la sonda si arresti, quando la sonda torna di nuovo in funzione la chiave viene inviata di nuovo alla sonda. Tuttavia, se la chiave viene cambiata più di una volta prima che la sonda si arresti, è necessario cambiare la chiave manualmente mediante la JMX Console. (Selezionare **False** per **autoUpdateProbe**).

4. Fare clic su **Invoke** per generare e aggiornare la chiave di crittografia.

Aggiornare una chiave di crittografia su una sonda

Se si sceglie di non distribuire automaticamente una chiave di crittografia dal server UCMDB a tutte le sonde (per motivi di sicurezza), è necessario eseguire il download della nuova chiave di crittografia su tutte le sonde ed eseguire il metodo **importEncryptionKey** sulla sonda:

1. Collocare il file della chiave di crittografia nella directory **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. Sul computer della sonda avviare il browser Web e specificare l'indirizzo seguente: **http://localhost:1977**.

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

   > **Nota:** Se Probe Manager e Probe Gateway sono in esecuzione come processi separati, nel computer che esegue Probe Manager l'indirizzo deve essere immesso come segue: **http://localhost:1978**.

3. Sul dominio della sonda, fare clic su **type=SecurityManagerService**.
4. Individuare il metodo **importEncryptionKey**.
5. Immettere il nome del file della chiave di crittografia che si trova in **C:\hp\UCMDB\DataFlowProbe\conf\security**. Questo file contiene la chiave da importare.
6. Fare clic sul pulsante **importEncryptionKey**.
7. Riavviare la sonda.

Cambiare manualmente la chiave di crittografia quando Probe Manager e Probe Gateway sono installati su computer diversi

1. Nel computer di Probe Manager avviare il servizio Probe Manager (**Start > Programmi > HP UCMDB > Probe Manager**).
2. Importare la chiave dal server utilizzando JMX di Probe Manager. Per i dettagli consultare "Generare una nuova chiave di crittografia" a pagina 56.
3. Al termine dell'importazione della chiave di crittografia, riavviare i servizi Probe Manager e Probe Gateway.

Definire diversi provider JCE

Quando si genera una chiave di crittografia mediante la JMX Console, è possibile definire diversi provider JCE utilizzando i metodi **changeEncryptionKey** e **generateEncryptionKey**.

Per cambiare il provider JCE predefinito:

1. Registrare i file jar del provider JCE nella directory **$JRE_HOME/lib/ext**.
2. Copiare i file jar nella cartella $JRE_HOME:
   - Per il server UCMDB: $JRE_HOME risiede in: **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - Per la sonda del flusso di dati: $JRE_HOME risiede in: **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Aggiungere la classe del provider alla fine dell'elenco di provider nel file **$JRE_HOME\lib\security\java.security**.
4. Aggiornare i file **local_policy.jar** e **US_export_policy.jar** per includere i criteri JCE illimitati. Questi file si possono scaricare dal sito Web di Sun.
5. Riavviare il server UCMDB e la sonda del flusso di dati.
6. Individuare il campo JCE per il metodo **changeEncryptionKey** o **generateEncryptionKey** e aggiungere il nome del provider JCE.

Impostazioni della crittografia di Confidential Manager

Questa tabella elenca le impostazioni della crittografia che si possono cambiare utilizzando i vari metodi JMX. Queste impostazioni di crittografia sono rilevanti per la crittografia delle comunicazioni tra il client e il server Confidential Manager oltre che per la crittografia della cache del client Confidential Manager.

Nome impostazione Confidential Manager	Nome impostazione sonda Confidential Manager	Descrizione impostazione	Valori possibili	Valore predefinito
cryptoSource	Nome libreria di crittografia	Questa impostazione definisce la libreria di crittografia da utilizzare.	lw, jce, windowsDPAPI, lwJCECompatib-le	lw
lwJCEPBE Compatibilità Modalità	Supporta le versioni precedenti della crittografia semplificata	Questa impostazione definisce se supportare o meno la crittografia precedente semplificata.	true, false	true
engineName	Nome motore	Nome meccanismo di crittografia	AES, DES, 3DES, Blowfish	AES
keySize	Dimensione chiave	lunghezza chiave di crittografia in bit	Per AES - 128, 192 o 256; Per DES - 64; Per 3DES - 192; Per Blowfish - qualsiasi numero compreso tra 32 e 448	256
algorithm Spaziatura Nome	Nome spaziatura algoritmo	Standard spaziatura	PKCS7Padding, PKCS5Padding	PKCS7Paddin-g
pbeCount	Conteggio PBE	Numero di esecuzioni della funzione hash per creare la chiave dalla password (stringa init)	Qualsiasi numero positivo	20
pbeDigest Algoritmo	Algoritmo digest PBE	Tipo di hash	SHA1, SHA256, MD5	SHA1
useMacWith Crittografia	Utilizzo MAC con crittografia	Indica se utilizzare il codice MAC con la crittografia	true, false	false
macKeySize	Dimensione chiave MAC	Dipende dall'algoritmo MAC	256	256

Risoluzione dei problemi e limitazioni

Se si cambia il nome di dominio predefinito nel server UCMDB, è necessario prima verificare che la sonda del flusso di dati non sia in esecuzione. Una volta applicato il nome di dominio predefinito, è necessario eseguire lo script **DataFlowProbe\tools\clearProbeData.bat** sul lato sonda del flusso di dati.

Nota: l'esecuzione dello script clearProbeData.bat causerà un ciclo di individuazione sul lato sonda una volta che questa sarà avviata.

Capitolo 5

Protezione avanzata della sonda del flusso di dati

Questo capitolo comprende:

Modificare la password crittografata del database MySQL

In questa sezione viene spiegato come modificare la password per l'utente del database MySQL.

1. Creare la forma crittografata di una password (chiave AES a 192 bit)
   a. Accedere alla JMX Console della sonda del flusso di dati. Avviare il browser Web e specificare il seguente indirizzo: **http://<nome del computer della sonda del flusso di dati oppure indirizzo IP>:1977**. Se la sonda del flusso di dati viene eseguita in locale, immettere **http://localhost:1977**.

Potrebbe essere necessario effettuare l'accesso con nome utente e password.

Nota: Se non è stato creato un utente, per accedere utilizzare il nome utente predefinito sysadmin e la password sysadmin.

b. Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.

c. Individuare l'operazione **getEncryptedDBPassword**.

d. Nel campo **DB Password** immettere la password da crittografare.

e. Chiamare l'operazione facendo clic sul pulsante **getEncryptedDBPassword**.

Il risultato della chiamata è una stringa con password crittografata, ad esempio:

```
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. Arrestare la sonda del flusso di dati

Start >Tutti i programmi > HP UCMDB > Arresta sonda del flusso di dati

3. Eseguire lo script set_dbuser_password.cmd

Lo script si trova nella cartella seguente:
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd

Eseguire lo script **set_dbuser_password.cmd** con la nuova password come primo argomento e la password dell'account radice MySQL come secondo argomento (oppure lasciare il secondo argomento vuoto se l'account radice MySQL non è protetto da password).

Ad esempio:

set_dbuser_password <my_password><root_password>.

La password deve essere immessa nella forma crittografata (testo normale).

4. Aggiornare la password nei file di configurazione della sonda del flusso di dati

a. La password deve risiedere crittografata nei file di configurazione. Per recuperare la forma crittografata della password utilizzare il metodo JMX **getEncryptedDBPassword** come spiegato nel passaggio 1.

b. Aggiungere la password crittografata alle proprietà seguenti nel file **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

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

  Ad esempio:

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

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

5. Avviare la sonda del flusso di dati

   Start > Tutti i programmi > HP UCMDB > Avvia sonda del flusso di dati

Script clearProbeData.bat: Utilizzo

Lo script **clearProbeData.bat** ricrea l'utente del database senza modificare la sua password corrente.

Lo script prevede di ricevere la password dell'account radice MySQL come primo argomento. Se non viene trasferito alcun parametro, presuppone che la password dell'account radice MySQL sia vuota.

Dopo avere eseguito lo script:

- Riesaminare il seguente file per la verifica degli errori:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log
- Eliminare il file seguente poiché contiene la password del database:
  C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log

Impostare la password crittografata della JMX Console

In questa sezione viene spiegato come crittografare la password per l'utente JMX. La password crittografata è archiviata nel file the DataFlowProbe.properties. Gli utenti devono registrarsi per accedere alla JMX Console.

1. **Creare la forma crittografata di una password (chiave AES a 192 bit)**

   a. Accedere alla JMX Console della sonda del flusso di dati. Avviare il browser Web e specificare il seguente indirizzo: **http://<nome del computer della sonda del flusso di dati oppure indirizzo IP>:1977**. Se la sonda del flusso di dati viene eseguita in locale, immettere **http://localhost:1977**.

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

   > **Nota:** Se non è stato creato un utente, per accedere utilizzare il nome utente predefinito sysadmin e la password sysadmin.

   b. Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.

   c. Individuare l'operazione **getEncryptedKeyPassword**.

   d. Nel campo **Key Password** immettere la password da crittografare.

   e. Chiamare l'operazione facendo clic sul pulsante **getEncryptedKeyPassword**.

   Il risultato della chiamata è una stringa con password crittografata, ad esempio:

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

2. **Arrestare la sonda del flusso di dati**

Start >Tutti i programmi > HP UCMDB > Arresta sonda del flusso di dati

3. **Aggiungere la password crittografata**

   Aggiungere la password crittografata alla proprietà seguente nel file **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Ad esempio:

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

   Nota: per disabilitare l'autenticazione, lasciare questi campi vuoti. In questo modo gli utenti possono aprire la pagina principale della JMX Console della sonda senza immettere l'autenticazione.

4. **Avviare la sonda del flusso di dati**

   Start >Tutti i programmi > HP UCMDB > Avvia sonda del flusso di dati

   Verificare il risultato in un browser Web.

Impostare la password UpLoadScanFile

In questa sezione viene descritto come impostare la password per **UpLoadScanFile**, utilizzata per il salvataggio della scansione offsite. La password crittografata è archiviata nel file **DataFlowProbe.properties**. Gli utenti devono registrarsi per accedere alla JMX Console.

1. **Creare la forma crittografata di una password (chiave AES a 192 bit)**

   a. Accedere alla JMX Console della sonda del flusso di dati. Avviare il browser Web e specificare il seguente indirizzo: **http://<nome del computer della sonda del flusso di dati oppure indirizzo IP>:1977**. Se la sonda del flusso di dati viene eseguita in locale, immettere **http://localhost:1977**.

      Potrebbe essere necessario effettuare l'accesso con nome utente e password.

      Nota: Se non è stato creato un utente, per accedere utilizzare il nome utente predefinito sysadmin e la password sysadmin.

   b. Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.

   c. Individuare l'operazione **getEncryptedKeyPassword**.

   d. Nel campo **Key Password** immettere la password da crittografare.

   e. Chiamare l'operazione facendo clic sul pulsante **getEncryptedKeyPassword**.

      Il risultato della chiamata è una stringa con password crittografata, ad esempio:

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

2. **Arrestare la sonda del flusso di dati**

   Start >Tutti i programmi > HP UCMDB > Arresta sonda del flusso di dati

3. **Aggiungere la password crittografata**

   Aggiungere la password crittografata alla proprietà seguente nel file **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   Ad esempio:

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

4. **Avviare la sonda del flusso di dati**

   Start >Tutti i programmi > HP UCMDB > Avvia sonda del flusso di dati

   Verificare il risultato in un browser Web.

Accesso remoto al server MySQL

In questa sezione viene spiegato come consentire/limitare l'accesso all'account della sonda del flusso di dati MySQL da computer remoti.

Nota:

- Per impostazione predefinita l'accesso è limitato.
- Non è possibile accedere all'account radice MySQL da computer remoti.

Per consentire l'accesso a MySQL:

1. Eseguire il seguente script in una finestra del prompt dei comandi:

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

2. Quando richiesto, immettere la password dell'account radice MySQL come primo argomento. Corrisponde alla password immessa durante l'installazione della sonda.

Per restringere l'accesso a MySQL:

1. Eseguire il seguente script in una finestra del prompt dei comandi:

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

2. Quando richiesto, immettere la password dell'account radice MySQL come primo argomento. Corrisponde alla password immessa durante l'installazione della sonda.

Abilitare il protocollo SSL tra il server UCMDB e la sonda del flusso di dati con l'autenticazione reciproca

È possibile impostare l'autenticazione per la sonda del flusso di dati e il server UCMDB con i certificati. Il certificato per ciascun componente viene inviato e autenticato prima che venga stabilita la connessione.

Nota: il metodo seguente per l'abilitazione del protocollo SSL sulla sonda del flusso di dati con l'autenticazione reciproca è il metodo più sicuro ed è quindi la modalità di comunicazione consigliata. Questo metodo sostituisce la procedura per l'autenticazione di base.

In questa sezione vengono trattati i seguenti argomenti:

Panoramica

UCMDB supporta le modalità seguenti di comunicazione tra il server UCMDB e la sonda del flusso di dati:

- **Autenticazione del server.** Questa modalità utilizza il protocollo SSL e la sonda autentica il certificato del server UCMDB. Per i dettagli consultare "Abilitare SSL con l'autenticazione del server (monodirezionale)" alla pagina successiva.
- **Autenticazione reciproca.** Questa modalità utilizza il protocollo SSL e consente l'autenticazione del server da parte della sonda e l'autenticazione del client da parte del server. Per i dettagli consultare "Abilitare l'autenticazione reciproca del certificato (bidirezionale)" a pagina 70.
- **HTTP standard.** Nessuna comunicazione SSL. Questa è la modalità predefinita e il componente Sonda del flusso di dati in UCMDB non richiede alcun certificato. La sonda del flusso di dati comunica con il server mediante il protocollo HTTP standard.

Nota: Individuazione non può utilizzare catene certificato quando lavora con SSL. Quindi, se si stanno utilizzando catene certificato, è necessario generare un certificato autofirmato per la sonda del flusso di dati al fine di rendere possibile la comunicazione con il server UCMDB.

Keystore e truststore

Il server UCMDB e la sonda del flusso di dati utilizzano keystore truststore:

- **Keystore.** File contenente le voci delle chiavi (un certificato e una chiave privata corrispondente).
- **Truststore.** File contenente i certificati utilizzati per verificare un host remoto (ad esempio quando si utilizza l'autenticazione del server, il truststore della sonda del flusso di dati deve includere il certificato del server UCMDB).

Limiti dell'autenticazione reciproca

Il keystore della sonda del flusso di dati (come definito in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) deve contenere una (1) sola voce di chiave.

Abilitare SSL con l'autenticazione del server (monodirezionale)

Questa modalità utilizza il protocollo SSL e la sonda autentica il certificato del server.

Questo compito comprende:

- "Prerequisiti" nel seguito
- "Configurazione server UCMDB" nel seguito
- "Configurazione della sonda del flusso di dati" a pagina 70
- "Riavviare i computer" a pagina 70

Prerequisiti

1. Verificare che sia UCMDB sia la sonda del flusso di dati siano in esecuzione.

   Nota: se la sonda è installata in modalità separata, queste istruzioni si riferiscono a Probe Gateway.

2. Se UCMDB o la sonda del flusso di dati non sono installati nelle cartelle predefinite, fare attenzione alla posizione corretta e cambiare i comandi di conseguenza.

Configurazione server UCMDB

1. **Esportare il certificato di UCMDB**

   a. Aprire il prompt dei comandi ed eseguire il comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore alias> -keystore <Keystore file path> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   dove:

   - **keystore alias** è il nome assegnato al keystore.
   - **Keystore file path** è il percorso completo del file di archivio chiavi.

   Ad esempio, per il server.keystore predefinito utilizzare il seguente comando:

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

b. Immettere la password del keystore. Ad esempio, la password del keystore predefinita è **hppass**.

c. Verificare che il certificato sia stato creato nella seguente directory: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Protezione avanzata del connettore della sonda del flusso di dati in UCMDB**

a. Per accedere alla JMX Console di UCMDB: Specificare il seguente URL nel browser Web: **http://<nome del computer ucmdb oppure IP>:8080/jmx-console**. Potrebbe essere necessario effettuare l'accesso con nome utente e password.

b. Selezionare il servizio: **Ports Management Services**.

c. Richiamare il metodo **PortsDetails** e fare attenzione al numero della porta per HTTPS. (Predefinito: 8443) Accertarsi che il valore nella colonna **È abilitato** sia **True**.

d. Tornare a **Ports Management Services**.

e. Per mappare il connettore della sonda del flusso di dati alla modalità di autenticazione del server, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Tutti gli altri flag**: false

Viene visualizzato il messaggio seguente:

Operazione riuscita. Il componente mam-collectors è ora mappato a: Porte HTTPS.

f. Tornare a **Ports Management Services**.

g. Per mappare il connettore di Confidential Manager alla modalità di autenticazione del server, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:

- **componentName**: cm
- **isHTTPS**: true
- **Tutti gli altri flag**: false

Viene visualizzato il messaggio seguente:

Operazione riuscita. Il componente cm è ora mappato a: Porte HTTPS.

3. **Copiare il certificato di UCMDB su ogni computer della sonda.**

Copiare il file del certificato, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, che si trova nel computer del server UCMDB, nella cartella seguente di ogni computer della sonda del flusso di dati **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configurazione della sonda del flusso di dati

Nota: è necessario configurare ogni computer della sonda del flusso di dati.

1. **Importare il file server.cert creato in** "Esportare il certificato di UCMDB" a pagina 68 **nel truststore della sonda.**
   a. Aprire il prompt dei comandi ed eseguire il comando:

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

   b. Immettere la password del keystore: logomania
   c. Quando viene chiesto **Trust this certificate?**, premere **y** e quindi **Invio**.

   Viene visualizzato il messaggio seguente:

   Il certificato è stato aggiunto al keystore.

2. **Aprire il file DiscoveryProbe.properties che si trova in: C:\HP\UCMDB\DataFlowProbe\conf**
   a. Aggiornare la proprietà **appilog.agent.probe.protocol** in **HTTPS**.
   b. Aggiornare la proprietà **serverPortHttps** con il numero di porta rilevante. (Utilizzare il numero della porta dal passaggio 2c della "Configurazione server UCMDB" a pagina 68).

Riavviare i computer

Riavviare i computer del server UCMDB e della sonda.

Abilitare l'autenticazione reciproca del certificato (bidirezionale)

Questa modalità utilizza il protocollo SSL e consente l'autenticazione del server da parte della sonda e l'autenticazione del client da parte del server. Sia il server sia la sonda inviano i certificati all'altra entità per l'autenticazione.

Questo compito comprende:

- "Ulteriore configurazione del server UCMDB" a pagina 74
- "Riavviare i computer" a pagina 75

Prerequisiti

1. Verificare che sia UCMDB sia la sonda del flusso di dati siano in esecuzione.

   Nota: se la sonda è installata in modalità separata, queste istruzioni si riferiscono a Probe Gateway.

2. Se UCMDB o la sonda del flusso di dati non sono installati nelle cartelle predefinite, fare attenzione alla posizione corretta e cambiare i comandi di conseguenza.

Configurazione iniziale del server UCMDB

1. **Esportare il certificato di UCMDB**

   a. Aprire il prompt dei comandi ed eseguire il comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias
   <keystore alias> -keystore <Keystore file path> -file
   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   dove:

   - **keystore alias** è il nome assegnato al keystore.
   - **Keystore file path** è il percorso completo del file di archivio chiavi.

   Ad esempio, per il server.keystore predefinito utilizzare il seguente comando:

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

   b. Immettere la password del keystore. Ad esempio, la password del keystore predefinita è **hppass**.

   c. Verificare che il certificato sia stato creato nella seguente directory: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Protezione avanzata del connettore della sonda del flusso di dati in UCMDB**

   a. Per accedere alla JMX Console di UCMDB: Specificare il seguente URL nel browser Web: **http://<nome del computer ucmdb oppure IP>:8080/jmx-console**. Potrebbe essere necessario effettuare l'accesso con nome utente e password.

   b. Selezionare il servizio: **Ports Management Services**.

   c. Richiamare il metodo **PortsDetails** e fare attenzione al numero della porta per HTTPS con l'autenticazione del client. (Predefinito: 8443) Accertarsi che il valore nella colonna **È abilitato** sia **True**.

   d. Tornare a **Ports Management Services**.

   e. Per mappare il connettore della sonda del flusso di dati alla modalità di autenticazione

reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Tutti gli altri flag**: false

Viene visualizzato il messaggio seguente:

Operazione riuscita. Il componente mam-collectors è ora mappato a: porte HTTPS_CLIENT_AUTH.

f. Tornare a **Ports Management Services**.

g. Per mappare il connettore di Confidential Manager alla modalità di autenticazione reciproca, richiamare il metodo **mapComponentToConnectors** con i parametri seguenti:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Tutti gli altri flag**: false

Viene visualizzato il messaggio seguente:

Operazione riuscita. Il componente cm è ora mappato a: porte HTTPS_CLIENT_AUTH.

3. **Copiare il certificato di UCMDB su ogni computer della sonda.**

Copiare il file del certificato, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, che si trova nel computer del server UCMDB, nella cartella seguente di ogni computer della sonda del flusso di dati: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configurazione della sonda del flusso di dati

Nota: è necessario configurare ogni computer della sonda del flusso di dati.

1. **Importare il file server.cert creato in** "Esportare il certificato di UCMDB" alla pagina precedente **nel truststore della sonda.**

a. Aprire il prompt dei comandi ed eseguire il comando:

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

b. Immettere la password del keystore: logomania

c. Quando viene chiesto **Trust this certificate?**, premere **y** e quindi **Invio**.

Viene visualizzato il messaggio seguente:

Il certificato è stato aggiunto al keystore.

2. **Creare un nuovo file client.keystore**

   a. Aprire il prompt dei comandi ed eseguire il comando:

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

   dove **ProbeName** è l'alias univoco della sonda del flusso di dati.

   Nota: Per garantire che questo alias sia univoco, utilizzare l'Identificatore nome sonda assegnato alla sonda durante la sua definizione.

   b. Immettere la password del keystore di almeno 6 caratteri e conservarla.

   c. Immettere nuovamente la password per la conferma.

   d. Premere **Invio** per rispondere alle seguenti domande:

   Quali sono nome e cognome? [Sconosciuto]:

   Qual è il nome della propria unità organizzativa?[Sconosciuto]:

   Qual è il nome della propria organizzazione?[Sconosciuto]:

   Qual è il nome della propria città o località?[Sconosciuto]:

   Qual è il nome della proprio stato i provincia?[Sconosciuto]:

   Qual è il codice paese di due lettere per questa unità?[Sconosciuto]:

   e. Digitare **sì** quando viene chiesto **CN=Sconosciuto, OU=Sconosciuto, O=Sconosciuto, L=Sconosciuto, ST=Sconosciuto, C=Sconosciuto è corretto?**

   f. Premere **Invio** per rispondere alla seguente domanda:

   Immettere la password della chiave <probekey> (INVIO se è la stessa password del keystore):

   g. Verificare che il certificato sia stato creato nella seguente directory e assicurarsi che la sua dimensione sia maggiore di 0:
   C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore

3. **Esportare il nuovo certificato client**

   a. Aprire il prompt dei comandi ed eseguire il comando:

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

   b. Quando viene chiesto, immettere la password del keystore. (La password dal Passaggio 2b precedente).

Viene visualizzato il messaggio seguente:

Certificato archiviato nel file <C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert>

4. **Aprire il file DiscoveryProbe.properties che si trova in: C:\HP\UCMDB\DataFlowProbe\conf**
   a. Aggiornare la proprietà **appilog.agent.probe.protocol** in **HTTPS**.
   b. Aggiornare la proprietà **serverPortHttps** con il numero di porta rilevante. (Utilizzare il numero della porta dal passaggio 2c della "Configurazione iniziale del server UCMDB" a pagina 71).
5. **Aprire il file ssl.properties che si trova in: C:\HP\UCMDB\DataFlowProbe\conf\security**
   a. Aggiornare la proprietà **javax.net.ssl.keyStore** in **client.keystore**.
   b. Crittografare la password dal Passaggio 2b precedente:
      i. Avviare la sonda del flusso di dati (oppure accertarsi che sia già in esecuzione).
      ii. Accedere al JMX della sonda. Selezionare: **http://<probe_hostname>:1977**

      Ad esempio, se la sonda è in esecuzione in locale, selezionare: **http://localhost:1977**.
      iii. Premere il collegamento **type=MainProbe**.
      iv. Scorrere verso il basso fino all'operazione **getEncryptedKeyPassword**.
      v. Immettere la password nel campo **Key Password**.
      vi. Premere il pulsante **getEncryptedKeyPassword**.
   c. Copiare e incollare la password crittografata per aggiornare a proprietà **javax.net.ssl.keyStorePassword**.

      Nota: I numeri sono separati da virgole. Ad esempio: -20,50,34,-40,-50.)
6. **Copiare il certificato della sonda su ogni computer di UCMDB.**

   Copiare il file **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** dal computer della sonda del flusso di dati al computer di UCMDB in **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert**.

Ulteriore configurazione del server UCMDB

1. **Aggiungere ogni certificato della sonda al truststore di UCMDB.**

   Nota: è necessario completare i seguenti passaggi per ogni certificato della sonda.

   a. Aprire il prompt dei comandi ed eseguire il comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -
   keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore
   ```

```
-file C:\hp\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert -
alias <ProbeName>
```

b. Immettere la password del keystore. Ad esempio, la password del keystore predefinita è **hppass**.

c. Quando viene chiesto **Trust this certificate?**, premere **y** e quindi **Invio**.

Viene visualizzato il messaggio seguente:

Il certificato è stato aggiunto al keystore

Riavviare i computer

Riavviare i computer del server UCMDB e della sonda.

Controllo della posizione del file domainScopeDocument

Il file system della sonda contiene (per impostazione predefinita) sia la chiave di crittografia sia il file **domainScopeDocument**. Ogni volta che viene avviata, la sonda recupera il file **domainScopeDocument** dal server e lo memorizza nel proprio file system. Per impedire a utenti non autorizzati di ottenere queste credenziali, è possibile configurare la sonda in modo che il file **domainScopeDocument** sia conservato nella memoria della sonda e non venga archiviato nel file system della sonda.

Per controllare la posizione del file domainScopeDocument:

1. Aprire **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** e cambiare:

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

   in:

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

   Le cartelle serverData di Probe Gateway e Probe Manager non contengono più il file **domainScopeDocument**.

   Per i dettagli sull'utilizzo del file **domainScopeDocument** per la protezione avanzata di GFD, consultare "Gestione credenziali del flusso di dati" a pagina 42.

2. Riavviare la sonda.

Creare un keystore per la sonda del flusso di dati

1. Nel computer della sonda eseguire il comando seguente:

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

2. Immettere una password per il nuovo keystore.

3. Immettere le informazioni quando richieste.
4. Quando viene chiesto **CN=... C=... è corretto?** immettere **sì** quindi premere **Invio**.
5. Premere di nuovo **Invio** per accettare la password del keystore come password della chiave.
6. Verificare che **client.keystore** venga creato nella directory seguente: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Crittografare le password del keystore e del truststore della sonda

Le password del keystore e del truststore della sonda sono archiviate crittografate in **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Questa procedura spiega come crittografare la password.

1. Avviare la sonda del flusso di dati (oppure verificare che sia già in esecuzione).
2. Accedere alla JMX Console della sonda del flusso di dati. Avviare il browser Web e specificare il seguente indirizzo: http://<nome del computer della sonda del flusso di dati oppure indirizzo IP>:1977. Se la sonda del flusso di dati viene eseguita in locale, immettere http://localhost:1977.

   Nota: Potrebbe essere necessario effettuare l'accesso con nome utente e password. Se non è stato creato un utente, per accedere utilizzare il nome utente predefinito sysadmin e la password sysadmin.

3. Individuare il servizio **Type=MainProbe** e fare clic sul collegamento per aprire la pagina Operazioni.
4. Individuare l'operazione **getEncryptedKeyPassword**.
5. Immettere la password del keystore o del truststore nel campo **Key Password** e richiamare l'operazione facendo clic su **getEncryptedKeyPassword**.
6. Il risultato della chiamata è una stringa con password crittografata, ad esempio:

   ```
   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. Copiare e incollare la password crittografata nella riga rilevante nel keystore o nel truststore nel file seguente: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

Keystore e truststore predefiniti della sonda del flusso di dati e del server

In questa sezione vengono trattati i seguenti argomenti:

Server UCMDB

I file si trovano nella directory seguente: **C:\HP\UCMDB\UCMDBServer\conf\security.**

Entità	Nome file/termine	Password/termine	Alias
Keystore server	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Truststore server	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	clientcert (voce attendibile predefinita)
Keystore client	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Sonda del flusso di dati

I file si trovano nella directory seguente: **C:\HP\UCMDB\DataFlowProbe\conf\security.**

Entità	Nome file/termine	Password/termine	Alias
Keystore sonda	MAMKeyStoreExp.jks (pKeyStoreFile)	logomania (pKeyStorePass)	mam
La sonda del flusso di dati utilizza il keystore **cKeyStoreFile** come keystore predefinito durante la procedura di autenticazione reciproca. Questo è un keystore del client che fa parte dell'installazione di UCMDB.			
Truststore sonda	MAMTrustStoreExp.jks (pTrustStoreFile)	logomania (pTrustStorePass)	mam (voce attendibile predefinita)
La password **cKeyStorePass** è la password predefinita di **cKeyStoreFile**.			

Capitolo 6

Autenticazione Lightweight Single Sign-On (LW-SSO) – Riferimenti generali

Questo capitolo comprende:

Panoramica dell'autenticazione LW-SSO

LW-SSO è un metodo di controllo degli accessi che consente a un utente di effettuare l'accesso una sola volta per accedere alle risorse di più sistemi software senza che vengano richieste di nuovo le credenziali. Le applicazioni del gruppo di sistemi software configurato considerano l'autenticazione attendibile. Non è pertanto necessario procedere a ulteriori autenticazioni quando ci si sposta da un'applicazione all'altra.

Le informazioni in questa sezione si applicano alla versione 2.2 e 2.3 di LW-SSO.

- **Scadenza del token LW-SSO**

  Il valore di scadenza del token LW-SSO determina la validità della sessione dell'applicazione. Quindi, il valore di scadenza deve essere almeno uguale al valore di scadenza della sessione dell'applicazione.

- **Configurazione consigliata della Scadenza del token LW-SSO**

  La scadenza del token deve essere configurata per ciascuna applicazione che utilizza LW-SSO. Il valore consigliato è 60 minuti. Per un'applicazione che non richiede un valore elevato di protezione, è possibile configurare un valore di 300 minuti.

- **Orario GMT**

  Tutte le applicazioni comprese in una integrazione LW-SSO devono utilizzare lo stesso orario GMT con una differenza massima di 15 minuti.

- **Funzionalità multi-dominio**

  La Funzionalità multi-dominio richiede che per tutte le applicazioni dell'integrazione LW-SSO vengano configurate le impostazioni trustedHosts (o le impostazioni **protectedDomains**), se le applicazioni dovranno integrarsi con applicazioni di domini DNS differenti. Inoltre, è necessario aggiungere il dominio corretto nell'elemento **lwsso** della configurazione.

- **Ottenere il SecurityToken per la funzionalità URL**

Per ricevere le informazioni inviate come **SecurityToken per URL** da altre applicazioni, per l'applicazione host deve essere configurato il dominio corretto nell'elemento **lwsso** della configurazione.

Requisiti di sistema di LW-SSO

Applicazione	Versione	Commenti
Java	1.5 e successive	
HTTP Servlets API	2.1 e successive	
Internet Explorer	6.0 e successive	Il browser deve abilitare i cookie di sessione HTTP e la funzionalità HTTP 302.
Firefox	2.0 e successive	Il browser deve abilitare i cookie di sessione HTTP e la funzionalità HTTP 302.
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

Avvisi di protezione LW-SSO

In questa sezione vengono descritti gli avvisi di protezione correlati alla configurazione LW-SSO:

- **Parametro InitString riservato in LW-SSO.** LW-SSO utilizza la crittografia simmetrica per convalidare e creare un token LW-SSO. Il parametro **initString** della configurazione viene utilizzato per l'inizializzazione della chiave segreta. Un'applicazione crea un token e ciascuna applicazione che utilizza lo stesso parametro initString lo convalida.

  Attenzione:

- Non è possibile utilizzare LW-SSO senza impostare il parametro **initString**.
- Il parametro **initString** indica informazioni riservate e deve essere considerato riservato in termini di pubblicazione, trasporto e persistenza.
- Il parametro **initString** deve essere condiviso solo tra applicazioni che si integrano tra loro mediante LW-SSO.
- Il parametro **initString** deve avere una lunghezza minima di 12 caratteri.

- **Abilita LW-SSO solo se richiesto.** LW-SSO deve essere disabilitato a meno che non venga richiesto specificatamente.
- **Livello di protezione autenticazione**. L'applicazione che utilizza il framework di autenticazione più debole e rilascia un token LW-SSO che è considerato affidabile dalle altre applicazioni integrate determina il livello di protezione delle autenticazioni per tutte le altre applicazioni.

  Si raccomanda che soltanto le applicazioni che utilizzano un framework di autenticazione protetto rilascino un token LW-SSO.
- **Implicazioni crittografia simmetrica.** LW-SSO utilizza la crittografia simmetrica per rilasciare e convalidare i token LW-SSO. Quindi, qualsiasi applicazione che utilizza LW-SSO può rilasciare un token da rendere attendibile per tutte le altre applicazioni che condividono lo stesso parametro initString. Questo rischio potenziale è importante quando un'applicazione condivide un initString sia residente su, o accessibile da, una posizione non attendibile.
- **Mapping utenti (Sincronizzazione).** Il framework LW-SSO non garantisce il mapping degli utenti tra le applicazioni integrate. Quindi, l'applicazione integrata deve monitorare il mapping degli utenti. Si consiglia di condividere lo stesso registro utente (ad esempio LDAP/AD) tra tutte le applicazioni integrate.

  L'impossibilità di eseguire la mappatura degli utenti può causare violazioni della protezione e comportamenti negativi dell'applicazione. Ad esempio, si potrebbe assegnare lo stesso nome utente a diversi utenti reali in varie applicazioni.

  Inoltre, nei casi in cui un utente esegue l'accesso a un'applicazione (AppA) e successivamente accede a una seconda applicazione (AppB) che utilizza l'autenticazione contenitore o applicazione, l'impossibilità di eseguire la mappatura dell'utente forzerà l'utente stesso ad accedere manualmente all'AppB e ad inserire un nome utente. Se l'utente inserisce un nome utente diverso da quello utilizzato per l'accesso all'AppA, si può verificare il seguente comportamento: se l'utente, successivamente, accede ad una terza applicazione (AppC) dall'AppA o AppB, dovrà accedere utilizzando gli stessi nomi utente utilizzanti per l'accesso all'AppA o AppB rispettivamente.
- **Gestione identità**. Utilizzato per scopi di autenticazione, tutte le risorse non protette nella Gestione identità devono essere configurate con l'impostazione **nonsecureURLs** nel file di configurazione LW-SSO.
- **Modalità Demo LW-SSO.**
  - La modalità Demo deve essere utilizzata solo a scopi dimostrativi.
  - La modalità Demo deve essere utilizzata solo su reti non protette.

- La modalità Demo non può essere utilizzata in produzione. Non può essere utilizzata alcuna combinazione della modalità Demo con la modalità di produzione.

Risoluzione dei problemi e limitazioni

In questa sezione vengono descritti i problemi e le limitazioni note quando si lavora con l'autenticazione LW-SSO.

Problemi noti

In questa sezione vengono descritti i problemi noti per l'autenticazione LW-SSO.

- **Contesto di protezione.** Il contesto di protezione LW-SSO supporta un solo valore attributo per nome attributo.

  Quindi, quando un token SAML2 invia più di un valore per lo stesso nome attributo, solo un valore viene accettato dal framework LW-SSO.

  In modo analogo, se il token IdM è configurato per inviare più di un valore per lo stesso nome attributo, solo un valore viene accettato dal framework LW-SSO.

- **Funzionalità di disconnessione multi-dominio con Internet Explorer 7.** La funzionalità di disconnessione multi-dominio non va a buon fine nelle seguenti condizioni:

  - Il browser utilizzato è Internet Explorer 7 e l'applicazione richiama più di tre verbi redirect HTTP 302 consecutivi nella procedura di disconnessione.

  In questo caso, Internet Explorer 7 può non gestire correttamente la risposta redirect HTTP 302 e visualizzare una pagina di errore con il messaggio **Impossibile visualizzare la pagina Web**.

  Per ovviare al problema, si consiglia se possibile di ridurre il numero di comandi di redirect applicazione nella sequenza di disconnessione.

Limitazioni

Notare le seguenti limitazioni quando si lavora con l'autenticazione LW-SSO:

- **Accesso client all'applicazione.**

  Se nella configurazione LW-SSO è definito un dominio:

  - I client applicazione devono accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso, ad esempio, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO non può supportare URL con un indirizzo IP, ad esempio, http://192.168.12.13/WebApp.
  - LW-SSO non può supportare URL senza un dominio, ad esempio, http://myserver/WebApp.

  Se nella configurazione LW-SSO non è definito un dominio: il client può accedere all'applicazione senza un FQDN nell'URL di accesso. In questo caso, viene creato un cookie della sessione LW-SSO specifico per un singolo computer senza informazioni sul dominio. Quindi, il cookie non è delegato da browser a un altro, e non passa ad altri computer posizionati nello stesso dominio DNS. Questo significa che LW-SSO non funziona nello stesso dominio.

- **Integrazione framework LW-SSO.** Le applicazioni possono sfruttare e utilizzare le funzionalità LW-SSO solo se integrate precedentemente nel framework LW-SSO.

- **Supporto multi-dominio.**
  - La funzionalità multi-dominio si basa sul riferimento HTTP. LW-SSO supporta pertanto collegamenti da un'applicazione all'altra e non supporta la digitazione di un URL in una finestra del browser, a meno che le due applicazioni non risiedano nello stesso dominio.
  - Il primo collegamento interdominio che utilizza **HTTP POST** non è supportato.

    La funzionalità multi-dominio non supporta la prima richiesta **HTTP POST** verso una seconda applicazione (è supportata solo la richiesta **HTTP GET**). Ad esempio, se l'applicazione ha un collegamento HTTP verso una seconda applicazione, è supportata una richiesta **HTTP GET**, ma non è supportata una richiesta **HTTP FORM**. Tutte le richieste dopo la prima possono essere **HTTP POST** o **HTTP GET.**
  - Dimensione token LW-SSO:

    La dimensione delle informazioni che LW-SSO può trasferire da un'applicazione in un dominio a un'altra applicazione in un altro dominio è limitata a 15 gruppi/ruoli/attributi (notare che ciascun elemento può essere lungo in media di 15 caratteri).
  - Collegamento da pagine protette (HTTPS) a pagine non protette (HTTP) in uno scenario multi-dominio:

    La funzionalità multi-dominio non è utilizzabile nel collegamento da una pagina protetta (HTTPS) a una pagina non protetta (HTTP). È una limitazione del browser in cui l'intestazione di riferimento non viene inviata durante il collegamento da un risorsa protetta ad una non protetta. Per un esempio, consultare:
    `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`
  - Comportamento di cookie di terze parti in Internet Explorer:

    Microsoft Internet Explorer 6 contiene un modulo che supporta "Platform for Privacy Preferences (P3P) Project", ciò significa che i cookie di un dominio di terze parti sono bloccati per impostazione predefinita nella zona di protezione Internet. I cookie di sessione vengono inoltre considerati cookie di terze parti da IE e quindi vengono bloccati causando il blocco del funzionamento di LW-SSO. Per i dettagli consultare:
    `http://support.microsoft.com/kb/323752/en-us.`

    Per risolvere questo problema, aggiungere l'applicazione avviata (oppure un sottoinsieme del dominio DNS come *.mydomain.com) alla zona Intranet/attendibile sul computer (in Microsoft Internet Explorer selezionare **Menu > Strumenti > Opzioni Internet > Protezione > Intranet locale > Siti > Avanzate)**per accettare i cookie.

    Attenzione: il cookie di sessione di LW-SSO è solo uno dei cookie utilizzati dall'applicazione di terze parti che è bloccata.

- **Token SAML2**
  - La funzionalità di disconnessione non è supportata quando è utilizzato il token SAML2.

    Quindi, se il token SAML2 è utilizzato per accedere a una seconda applicazione, l'utente che si disconnette dalla prima applicazione non viene disconnesso dalla seconda applicazione.
  - **La scadenza del token SAML2 non viene presa dalla gestione della sessione dell'applicazione.**

Quindi, se il token SAML2 è utilizzato per accedere a una seconda applicazione, la gestione della sessione di ciascuna applicazione è gestita indipendentemente.

- **JAAS Realm.** Il JAAS Realm in Tomcat non è supportato.
- **Uso degli spazi nelle directory Tomcat.** L'uso degli spazi nelle directory Tomcat non è supportato.

  Non è possibile utilizzare LW-SSO quando un percorso (cartelle) di installazione Tomcat include gli spazi (ad esempio, File di programma) e il file di configurazione LW-SSO è posizionato nella cartella Tomcat **common\classes**.
- **Configurazione del server di bilanciamento del carico.** I server di bilanciamento del carico distribuiti con LW-SSO devono essere configurati per l'utilizzo di sessioni permanenti.
- **Modalità Demo.** In modalità Demo LW-SSO supporta pertanto collegamenti da un'applicazione all'altra e non supporta la digitazione di un URL in una finestra del browser a causa dell'assenza di un'intestazione del referrer HTTP in questo caso.

Capitolo 7

Autenticazione di accesso a HP Universal CMDB

Questo capitolo comprende:

Impostazione di un metodo di autenticazione

Per eseguire l'autenticazione è necessario lavorare:

- **Tramite il servizio interno di HP Universal CMDB.**
- **Tramite il protocollo Lightweight Directory Access Protocol (LDAP).** È possibile utilizzare un server dedicato esterno LDAP per memorizzare le informazioni di autenticazione invece di utilizzare il servizio interno di HP Universal CMDB. Il server LDAP deve risiedere nella stessa sottorete di tutti i server HP Universal CMDB.

  Per i dettagli su LDAP, consultare la sezione Mapping LDAP nella *Guida all'amministrazione di HP Universal CMDB*.

  Il metodo di autenticazione predefinita utilizza il servizio interno di HP Universal CMDB. Se si utilizza il metodo predefinito non è necessario apportare alcun cambiamento al sistema.

  Queste opzioni si applicano agli accessi eseguiti tramite i servizi Web e l'interfaccia utente.

- **Tramite LW-SSO.** HP Universal CMDB viene configurato con LW-SSO. LW-SSO consente di accedere ad HP Universal CMDB e avere accesso automatico ad altre applicazioni configurate in esecuzione sullo stesso dominio senza necessità di eseguire l'accesso a tali applicazioni.

  Quando il supporto di autenticazione LW-SSO è abilitato (è disabilitato per impostazione predefinita), è necessario accertarsi che altre applicazioni in ambiente Single Sign-On abbiano LW-SSO abilitato e utilizzino lo stesso parametro initString.

Abilitazione dell'accesso a HP Universal CMDB con LW-SSO

Per abilitare LW-SSO per HP Universal CMDB, utilizzare la procedura seguente:

1. Per accedere alla JMX Console immettere l'indirizzo seguente nel browser Web: **http://<nome_server>:8080/jmx-console**, dove **<nome_server>** è il nome del computer in cui è installato HP Universal CMDB.
2. In **UCMDB-UI**, fare clic su **name=LW-SSO Configuration** per aprire la pagina Operazioni.
3. Selezionare la stringa init utilizzando ili metodo **setInitString**.
4. Impostare il nome di dominio del computer sul quale è installato UCMDB utilizzando il metodo **setDomain**.
5. Chiamare il metodo **setEnabledForUI** con il parametro impostato su **True.**
6. **Facoltativo**. Se si desidera lavorare utilizzando una funzionalità multi dominio, selezionare il metodo **addTrustedDomains**, inserire i valori del dominio e fare clic su **Invoke**.
7. **Facoltativo.** Se si desidera lavorare utilizzando un proxy inverso, selezionare il metodo **updateReverseProxy**, impostare il parametro **Proxy inverso attivato** su **True**, inserire un'URL per il parametro **URL completa del server proxy inverso**, quindi fare clic su Invoke. Se si desidera accedere direttamente a UCMDB e utilizzare un proxy inverso, impostare la seguente configurazione aggiuntiva: selezionare il metodo **setReverseProxyIPs**, inserire l'indirizzo IP per il parametro ip/s del proxy inverso e fare clic su **Invoke.**
8. **Facoltativo**. Se si desidera accedere a UCMDB utilizzando un punto di autenticazione esterno, selezionare il metodo **setValidationPointHandlerEnable**, impostare il parametro **Gestore punto di convalida abilitato** in **True**, inserire l'URL per il punto di autenticazione nel parametro **Server punto di autenticazione**, quindi fare clic su **Invoke.**
9. Per visualizzare la configurazione LW-SSO come è stata salvata nel meccanismo impostazioni, chiamare il metodo **retrieveConfigurationFromSettings**.
10. Per visualizzare la configurazione LW-SSO effettivamente caricata, chiamare il metodo **retrieveConfiguration**.

Nota: non è possibile abilitare LW-SSO tramite l'interfaccia utente.

Impostazione di una connessione protetta con il protocollo SSL (Secure Sockets Layer)

Poiché il processo di accesso comporta il passaggio di informazioni riservate tra HP Universal CMDB e il server LDAP, è possibile applicare un certo livello di protezione al contenuto. Per eseguire questa operazione abilitare la comunicazione SSL sul server LDAP e configurare HP Universal CMDB per l'utilizzo di SSL.

HP Universal CMDB supporta SSL con l'utilizzo di un certificato emesso da una Autorità di certificazione (AC) attendibile.

La maggior parte dei server LDAP, compreso Active Directory, possono offrire una porta protetta per una connessione basata su SSL. Se si utilizza Active Directory con AC privata, è necessario aggiungere la propria AC alle AC attendibili in JRE.

Per i dettagli sulla configurazione della piattaforma HP Universal CMDB per il supporto della comunicazione basata su SSL, consultare "Abilitazione della comunicazione Secure Sockets Layer (SSL)" a pagina 18.

Per aggiungere un'AC alle AC attendibili per offrire una porta protetta per una connessione basata su SSL:

1. Esportare un certificato dalla propria AC e importarlo nella JVM di HP Universal CMDB utilizzando i passaggi seguenti:
   a. Nel server UCMDB accedere alla cartella **UCMDBServer\bin\JRE\bin**.
   b. Eseguire il seguente comando:

   ```
   Keytool -import -file <proprio file del certificato> -keystore
   C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Ad esempio:

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

2. Selezionare **Amministrazione> Impostazioni infrastruttura > categoria LDAP - Generale**.

   Nota: è inoltre possibile configurare queste impostazioni utilizzando la JMX Console. Per i dettagli consultare "Configurazione delle impostazioni LDAP mediante la JMX Console" alla pagina successiva.

3. Individuare **URL del server LDAP** e immettere un valore utilizzando il formato:

   ```
   ldaps://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   Ad esempio:

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

   Tenere presente la **s** in **ldaps**.

4. Fare clic su **Salva** per salvare il nuovo valore oppure **Ripristina predefinito** per sostituire la voce con il valore predefinito (URL vuoto).

Utilizzare la JMX Console per verificare le connessioni LDAP

In questa sezione viene descritto un metodo di verifica della configurazione dell'autenticazione LDAP mediante la JMX Console.

1. Avviare il browser Web e digitare il seguente indirizzo: **http://<nome_server>:8080/jmx-console**, dove **<nome_server>** è il nome del computer in cui è installato HP Universal CMDB.

   Potrebbe essere necessario accedere con nome utente e password.

2. In **UCMDB** fare clic su **UCMDB-UI:name=LDAP Settings** per aprire la pagina Operazioni.
3. Individuare **testLDAPConnection.**
4. Nella casella **Value** per il parametro **customer id**, immettere l'ID cliente.
5. Fare clic su **Invoke.**

   Nella pagina Operation Result di JMX MBEAN viene indicato se la connessione LDAP è riuscita. Se la connessione è riuscita, la pagina viene visualizzata anche nei gruppi radice LDAP.

Configurazione delle impostazioni LDAP mediante la JMX Console

In questa sezione viene descritto come configurare le impostazioni di autenticazione LDAP mediante la JMX Console.

Per configurare le impostazioni di autenticazione LDAP:

1. Avviare il browser Web e digitare il seguente indirizzo: **http://<nome_server>:8080/jmx-console**, dove **<nome_server>** è il nome del computer in cui è installato HP Universal CMDB.

   Potrebbe essere necessario accedere con nome utente e password.
2. In **UCMDB,** fare clic su **UCMDB-UI:name=LDAP Settings** per aprire la pagina Operations.
3. Per visualizzare le impostazioni di autenticazione LDAP correnti, individuare il **metodo getLDAPSettings**. Fare clic su **Invoke**. Viene visualizzata una tabella con tutte le impostazioni LDAP e i rispettivi valori.
4. Per cambiare i valori delle impostazioni di autenticazione LDAP, individuare il metodo **configureLDAP**. Immettere i valori per le impostazioni rilevanti e fare clic su **Invoke**. Nella pagina Operation Result di JMX MBEAN viene indicato se le impostazioni di autenticazione LDAP sono state aggiornate correttamente.

   Nota: se non viene immesso un valore per un'impostazione, viene mantenuto il valore corrente.
5. Dopo aver configurato le impostazioni LDAP, è possibile verificare le credenziali utente LDAP. Individuare il metodo **verifyLDAPCredentials**. Immettere l'ID cliente, il nome utente, la password e fare clic su Invoke. Nella pagina Operation Result di JMX MBEAN viene indicato se l'utente supera correttamente l'autenticazione LDAP.

Abilitazione e definizione del metodo di autenticazione LDAP

È possibile abilitare e definire il metodo di autenticazione LDAP per un sistema HP Universal CMDB.

Per abilitare e definire il metodo di autenticazione LDAP:

1. Selezionare la categoria **Amministrazione > Gestione impostazioni infrastruttura > LDAP - Generale**.
2. Selezionare **URL del server LDAP** e immettere il valore dell'URL LDAP utilizzando il formato:

   ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]

   Ad esempio:

   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
3. Selezionare la categoria **Definizione gruppo LDAP**, individuare **DN di base dei gruppi** e immettere il nome distinto del gruppo generale.
4. Individuare **DN di base dei gruppi radice** e immettere il nome distinto del gruppo radice.
5. Selezionare la categoria **LDAP - Generale**, individuare **Abilita sincronizzazione autorizzazioni utenti** e verificare che il valore sia impostato su **True.**
6. Selezionare la categoria **LDAP - Autenticazione generale**, individuare **Password per l'utente autorizzato alla ricerca** e immettere la password.
7. Selezionare la categoria **Opzioni LDAP per classi e attributi**, individuare **Classe oggetto gruppi**, e immettere il nome della classe oggetto (**group** per Microsoft Active Directory e **groupOfUniqueNames** per Oracle Directory Server).
8. Individuare **Attributo membro dei gruppi** e inserire il nome dell'attributo (**member** per Microsoft Active Directory, e **uniqueMember** per Oracle Directory Server).
9. Individuare **Classe oggetto utenti** e inserire il nome della classe oggetto (**user** per Microsoft Active Directory, e **inetOrgPerson** per Oracle Directory Server).
10. Individuare **Attributo UUID** e inserire l'attributo d'identificazione univoco per un utente nel proprio server di directory. Assicurarsi di selezionare un attributo che sia univoco nel server di directory. Ad esempio, se si utilizza SunOne/Oracle Directory Server, l'attributo UID non è univoco. In tal caso, utilizzare l'attributo dell'indirizzo e-mail o il nome distinto. In UCMDB, utilizzare un attributo non univoco come attributo di identificazione univoco potrebbe causare un comportamento incoerente durante l'accesso.
11. Salvare i nuovi valori. Per sostituire una voce con il valore predefinito, fare clic su **Ripristina predefinito.**
12. Se l'impostazione dell'infrastruttura **Is case-sensitivity enforced when authenticating with LDAP** in **LDAP General**, è impostata su **True**, allora l'autenticazione distingue tra maiuscole e minuscole.

    Attenzione: quando il valore dell'impostazione di questa infrastruttura viene modificato, è necessario che l'amministratore UCMDB elimini manualmente tutti gli utenti esterni.
13. Mappare i gruppi utenti LDAP ai gruppi utente di UCMDB. Per i dettagli consultare "Autenticazione di accesso a HP Universal CMDB" a pagina 84.

14. Se si desidera definire un insieme predefinito di autorizzazioni per gli utenti in un gruppo LPDAP privo di mapping, selezionare la categoria **LDAP - Generale**, individuare **Gruppo utenti assegnato automaticamente**, quindi immettere il nome del gruppo.

Il protocollo predefinito utilizzato per comunicare con il server LDAP è TCP ma si può cambiare con il protocollo SSL. Per i dettagli consultare "Impostazione di una connessione protetta con il protocollo SSL (Secure Sockets Layer)" a pagina 85.

Nota: Per ogni utente LDAP sono presenti un nome, un cognome e un indirizzo e-mail salvati nel repository locale. Se il valore di uno di questi parametri archiviati sul server LDAP è diverso dal valore nella repository locale, i valori del server LDAP sovrascriveranno quelli locali ad ogni accesso.

Recupero della configurazione LW-SSO corrente in un ambiente distribuito

Quando UCMDB è incorporato in un ambiente distribuito, ad esempio in una distribuzione BSM, eseguire la procedura seguente per recuperare la configurazione LW-SSO corrente nel computer di elaborazione.

Per recuperare la configurazione LW-SSO corrente:

1. Avviare un browser Web e specificare il seguente indirizzo: `http://localhost.<domain_name>:8080/jmx-console.`

   Potrebbero essere richiesti nome utente e password.

2. Individuare **UCMDB:service=Security Services** e fare clic sul collegamento per aprire la pagina Operazioni.
3. Individuare l'operazione **retrieveLWSSOConfiguration**.
4. Fare clic su **Invoke** per recuperare la configurazione.

Capitolo 8

Confidential Manager

Questo capitolo comprende:

Confidential Manager, panoramica

Il framework Confidential Manager risolve il problema della gestione e la distribuzione dei dati sensibili di HP Universal CMDB e altri prodotti software HP.

Confidential Manager si divide in due componenti principali: client e server. Questi due componenti sono responsabili del trasferimento dei dati in modo protetto.

- Il client Confidential Manager è una libreria utilizzata dalle applicazioni per accedere ai dati sensibili.
- Il server Confidential Manager riceve le richieste dai client Confidential Manager oppure da client di terze parti ed esegue i compiti richiesti. Il server Confidential Manager è responsabile del salvataggio dei dati in modo protetto.

Confidential Manager crittografa le credenziali nel trasporto, nella cache del client, nella persistenza e nella memoria. Confidential Manager utilizza la crittografia simmetrica per il trasporto delle credenziali tra il client e il server Confidential Manager utilizzando un segreto condiviso. Confidential Manager utilizza vari segreti per la crittografia di cache, persistenza e trasporto in base alla configurazione.

Per le linee guida dettagliate sulla gestione della crittografia delle credenziali sulla sonda del flusso di dati, consultare "Gestione credenziali del flusso di dati" a pagina 42.

Considerazioni sulla protezione

- È possibile utilizzare le dimensioni chiave seguenti per l'algoritmo di protezione: 128, 192 e 256 bit. L'algoritmo viene eseguito più velocemente con una chiave più piccola ma è meno sicuro. La dimensione 128-bit è abbastanza sicura nella maggior parte dei casi.
- Per rendere il sistema più sicuro, utilizzare il codice MAC: impostare **useMacWithCrypto** su **true.** Per i dettagli consultare "Proprietà di crittografia" a pagina 92.
- Per sfruttare i fornitori di una forte protezione dei clienti, è possibile utilizzare la modalità JCE.

Configurare HP Universal CMDB Server

Quando si utilizza HP Universal CMDB, è necessario configurare il segreto e le proprietà della crittografia utilizzando i metodi JMX seguenti:

1. Sul computer di HP Universal CMDB Server avviare il browser Web e specificare l'indirizzo del server come segue: **http://<nome host o IP server UCMDB>:8080/jmx-console.**

   Potrebbe essere necessario effettuare l'accesso con nome utente e password.

2. In UCMDB fare clic su **UCMDB:service=Security Services** per aprire la pagina Operazioni.

3. Per recuperare la configurazione corrente, individuare l'operazione **CMGetConfiguration**.

   Fare clic su **Invoke** per visualizzare il file XML di configurazione del server Confidential Manager.

4. Per apportare cambiamenti alla configurazione, copiare il file XML chiamato nel passaggio precedente in un editor di testo. Apportare i cambiamenti in base alla tabella in "Proprietà di crittografia" alla pagina successiva.

   Individuare l'operazione **CMSetConfiguration**. Copiare la configurazione aggiornata nella casella **Value** e fare clic su **Invoke** La nuova configurazione viene scritta nel server UCMDB.

5. Per aggiungere utenti a Confidential Manager per l'autorizzazione e la replica, individuare l'operazione **CMAddUser**. Questo processo è utile anche nel processo di replica. Nella replica, il server slave deve comunicare con il server master utilizzando un utente con privilegi.

   - **username**. Nome utente.
   - **customer.** Il valore predefinito è ALL_CUSTOMERS.
   - **resource.** Nome della risorsa. Il valore predefinito è ROOT_FOLDER.
   - **permission.** Scegliere tra ALL_PERMISSIONS, CREATE, READ, UPDATE e DELETE. Il valore predefinito è ALL_PERMISSIONS.

   Fare clic su **Invoke**.

6. Se necessario, riavviare HP Universal CMDB.

   Nota: Nella maggior parte dei casi non è necessario riavviare il server. Sarà necessario riavviare il server quando si cambia una delle risorse seguenti.

   - Tipo di archiviazione
   - Nome tabella o nomi colonna di database
   - L'autore della connessione del database
   - Le proprietà di connessione al database (ovvero URL, utente, password nome classe driver)
   - Tipo di database

Nota:

- È importante che il server UCMDB e i rispettivi client abbiano le stesse proprietà di crittografia per il trasporto. Se queste proprietà vengono modificate nel server UCMDB, sarà necessario modificarle in tutti i client. (Non è rilevante per la sonda del flusso di dati poiché viene eseguita sullo stesso processo come il server UCMDB, ovvero non è necessaria alcuna configurazione di crittografia per il trasporto).
- Confidential Manager Replication non è configurato per impostazione predefinita e può essere configurato se necessario.
- Se Confidential Manager Replication è abilitato e viene cambiata la proprietà di crittografia **initString** per il trasporto o qualche altra proprietà di crittografia del master, tutti gli slave devono adottare i cambiamenti.

Definizioni

Proprietà di crittografia per l'archiviazione. La configurazione che definisce come il server mantiene e crittografa i dati (nel database o nel file, le proprietà di crittografia da crittografare o decrittografare e così via), come vengono archiviate le credenziali in modo protetto, come viene elaborata la crittografia e in base a quale configurazione.

Proprietà di crittografia per il trasporto. La configurazione del trasporto definisce come il server e i client crittografano il trasporto tra di loro, quale configurazione viene utilizzata, come vengono trasferite le credenziali in modo protetto, come viene elaborata la crittografia e in base a quale configurazione. È necessario utilizzare le stesse proprietà per la crittografia e la decrittografia del trasporto nel server e nel client.

Repliche e proprietà di crittografia per la replica. I dati contenuti in modo protetto da Confidential Manager sono replicati in modo protetto tra diversi server. Queste proprietà definiscono come devono essere trasferiti i dati tra il server slave e il server master.

Nota:

- La tabella del database che contiene la configurazione del server Confidential Manager è denominata: **CM_CONFIGURATION.**
- Il file di configurazione predefinito del server Confidential Manager si trova in app-infra.jar ed è denominato **defaultCMServerConfig.xml.**

Proprietà di crittografia

Nella tabella seguente vengono descritte le proprietà di crittografia. Per i dettagli sull'utilizzo dei parametri, consultare "Configurare HP Universal CMDB Server" alla pagina precedente.

Parametro	Descrizione	Valore consigliato
encryptTransportMode	Crittografare i dati trasportati:	true

Parametro	Descrizione	Valore consigliato
	true false	
encryptDecrypt InitString	Password per la crittografia	Maggiore di 8 caratteri
cryptoSource	Libreria di implementazione della crittografia da utilizzare: • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Supporta le versioni precedenti della crittografia semplificata: • true • false	true
cipherType	Tipo di crittografia utilizzata da Confidential Manager. Confidential Manager supporta un solo valore: **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • Null (nessuna crittografia)	AES
algorithmModeName	Modalità di algoritmo della crittografia a blocchi: • CBC	CBC
algorithmPaddingName	Standard spaziatura interna: • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	Dipende dall'algoritmo (quale **engineName** supporta)	256
pbeCount	Numero di esecuzioni della funzione hash per creare la chiave da **encryptDecryptInitString** Qualsiasi numero positivo.	1000

Parametro	Descrizione	Valore consigliato
pbeDigestAlgorithm	Tipo di hash: • SHA1 • SHA256 • MD5	SHA256
encodingMode	Rappresentazione ASCII dell'oggetto crittografato: • Base64 • Base64Url	Base64Url
useMacWithCrypto	Definisce se il codice MAC viene utilizzato con la crittografia: • true • false	false
macType	Tipo di codice di autenticazione dei messaggi (message authentication code, MAC): • hmac	hmac
macKeySize SHA256	Dipende dall'algoritmo MAC	256
macHashName	Algoritmo MAC hash • SHA256	SHA256


Java™
COMPATIBLE