HP Universal CMDB 9.10 Configuration Manager

per sistema operativo Windows

Guida alla distribuzione

Data di rilascio della documentazione: Novembre 2010
Data di rilascio del software: Novembre 2010

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 nel presente documento sono soggette a modifiche senza preavviso.

Legenda dei diritti riservati

Software per computer 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

Aggiornamenti della documentazione

Il frontespizio di questo documento contiene le seguenti informazioni identificative:

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

Per cercare aggiornamenti recenti o verificare che il documento utilizzato sia il più recente, visitare il sito:

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

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

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

In alternativa, fare clic sul collegamento **New users - please register** sulla pagina di accesso di HP Passport.

Sottoscrivendo lo specifico servizio di assistenza prodotti, sarà inoltre possibile ricevere edizioni aggiornate o nuove. Per ulteriori dettagli, contattare il rappresentante commerciale di HP.

Assistenza

Visitare il sito Web dell'Assistenza HP Software all'indirizzo:

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

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

L'assistenza online di HP Software offre al cliente la possibilità di risolvere autonomamente alcuni problemi. Costituisce un modo rapido ed efficiente per accedere agli strumenti interattivi di assistenza tecnica necessari per la gestione dell'azienda. Per i clienti dell'assistenza, il sito Web offre i 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
- Consultazione 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 come utente HP Passport per l'accesso. In molti casi è inoltre necessario un contratto di assistenza. Per ottenere un ID di 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

1

Installazione e configurazione

Questo capitolo comprende:

Panoramica di Configuration Manager

HP Universal CMDB Configuration Manager (Configuration Manager) consente di analizzare e controllare i dati in CMS, e offre un ambiente per il controllo dell'infrastruttura CMS, che comprende molte origini dati e viene utilizzata da vari propdotti e applicazioni.

La distribuzione di Configuration Manager in un ambiente di rete di tipo enterprise è un processo che richiede la pianificazione delle risorse e la progettazione dell'architettura del sistema. Prima di installare Configuration Manager, consultare le informazioni contenute in questa sezione, inclusi i requisiti di sistema.

Requisiti di sistema per Configuration Manager

Requisiti di sistema del server

La tabella seguente descrive i requisiti di sistema del server di Configuration Manager:

CPU	Intel Pentium 4, almeno 4 core
Memoria (RAM)	Almeno 4 GB
Piattaforma	x64
Sistema operativo	Sono supportati i seguenti sistemi operativi Windows a 64 bit: ➤ Windows 2003 Enterprise SP2 e R2 SP2 ➤ Windows 2008 Enterprise SP2 e R2

Database	➤ Microsoft SQL Server 2005 SP2; 2005 Compatibility Mode 80; (Enterprise Edition in tutti i casi) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB versione 9.03 (installazione CMDB tipica) Per un elenco completo dei requisiti di sistema per questa versione, consultare la documentazione di HP Universal CMDB.

Requisiti del client

La tabella seguente descrive i requisiti del client per la visualizzazione di Configuration Manager:

Browser	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Plug-in Flash Player del browser	Flash Player 9 o superiore
Risoluzione schermo	➤ 1024x768 minima ➤ 1280x1024 consigliata
Qualità colori	Almeno 16 bit

Linee guida consigliate per l'installazione

La tabella di seguito elenca le linee guida per le opzioni di impostazione di Configuration Manager.

LDAP	Sono supportati i seguenti ambienti LDAP: ➤ Active Directory ➤ SunONE 6.x
Dimensione minima consigliata per lo schema del database	2 GB

Configuration Manager Limiti di capacità

La tabella di seguito elenca i limiti di capacità per Configuration Manager.

Numero massimo di viste consigliato	100
Numero massimo di criteri consigliato	300
Numero massimo di CI compositi per vista consigliato	5000
Numero massimo di utenti simultanei consigliato	50

Configurare il database o lo schema utenti

Per utilizzare Configuration Manager, è necessario fornire uno schema del database. Configuration Manager supporta Microsoft SQL Server e Oracle Database Server. Questa attività descrive come configurare le proprietà della connessione per il database di Configuration Manager o lo schema utente utilizzando la procedura di installazione guidata.

Nota: Per i requisiti di sistema di Microsoft SQL Server e Oracle Server consultare "Requisiti di sistema del server" a pagina 8.

Per configurare il database:

1 Allocare un database di Microsoft SQL Server oppure uno schema utenti di Oracle Server.

➤ Per **Microsoft SQL Server 2005**: attivare l'isolamento istantanea.

Una volta creato il database, eseguire il seguente comando:

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

Per ulteriori informazioni sulla funzionalità di isolamento istantanea di SQL Server, consultare http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

➤ Per **Oracle**: concedere all'utente Oracle solo i ruoli **Connect** e **Resource**. (concedendo i privilegi **Select any table** la procedura di popolazione dello schema restituisce un errore.)

2 Verificare le seguenti informazioni, necessarie durante la procedura di configurazione:

✔	**Informazioni necessarie**
	Nome host e porta DB
	Nome utente e password DB
	Per MS SQL: Nome database
	Per Oracle: SID

3 Eseguire la procedura guidata di installazione di Configuration Manager. Per informazioni, consultare "Installare Configuration Manager" a pagina 12.

Installare Configuration Manager

Questa attività descrive come installare Configuration Manager sul server, e come configurare la connessione al database e l'integrazione di UCMDB. Per avere aiuto durante l'installazione, è possibile fare clic su **Help** in qualsiasi pagina della procedura guidata. Per una descrizione dettagliata delle pagine della procedura guidata, consultare "Configuration Manager Configurazione guidata di post installazione" a pagina 23.

Per installare Configuration Manager:

1 Nella directory principale del DVD di Configuration Manager, individuare il file: **install.bat**.

2 Fare doppio clic sul file per eseguire la Procedura guidata di installazione di Configuration Manager.

3 Fare clic su **Next** per aprire la pagina Contratto di licenza con l'utente finale.

4 Accettare i termini della licenza e fare clic su **Next** per aprire la pagina Installazione del prodotto.

5 Selezionare i prodotti da installare (UCMDB e Configuration Manager) e specificare il percorso di installazione. Se si dispone di una licenza cliente UCMDB, selezionare la casella di controllo. Fare clic su **Next** per avviare l'installazione di UCMDB. Per informazioni sull'installazione di UCMDB, consultare *HP Universal CMDB Deployment Guide* in PDF.

6 Una volta completare l'installazione e la post installazione di UCMDB, viene avviata automaticamente la Configurazione guidata di post installazione di Configuration Manager.

7 Fare clic su **Next** nella Pagina di benvenuto per aprire la pagina Configurazione connessione database.

8 Selezionare il tipo di database (Oracle o Microsoft SQL Server) e immettere il nome utente e la password. Si consiglia di testare la connessione facendo clic sul pulsante **Test**. Se il test della connessione ha esito positivo, fare clic su **Next** per aprire la pagina Configurazione server applicazioni.

Nota: completata la procedura guidata è possibile configurare altre opzioni avanzate di connessione al database. Per informazioni, consultare "Configurare le opzioni avanzate di connessione al database" a pagina 15.

---

9 Immettere il nome host e fare clic su **Next** per aprire la pagina Configurazione servizo Windows.

10 Se si desidera installare Configuration Manager come servizio Windows, selezionare la casella di controllo. Fare clic su **Next** per aprire la pagina Credenziali utente.

11 Immettere il nome utente e la password sia per l'Utente amministrativo che per l'Utente di integrazione. Fare clic su **Next** per aprire la pagina HP UCMDB Connection Configuration.

12 Se UCMDB è già installato su questo computer o su un computer diverso, assicurarsi che il server UCMDB sia attivo prima continuare.

Se si sta disinstallando UCMDB su un computer diverso, assicurarsi che la casella di controllo sia selezionata e immettere i parametri richiesti. Si consiglia di testare la connessione facendo clic sul pulsante **Test**. Se il test della connessione ha esito positivo, fare clic su **Next** per aprire la pagina Riepilogo azioni di post installazione.

13 Riesaminare le informazioni nella pagina Riepilogo azioni di post installazione. Se sono corrette, fare clic su **Next** per continuare con la procedura di post installazione.

14 Fare clic su **Finish** nella pagina Finish per completare la procedura di post installazione.

15 Se non è la prima volta che si avvia UCMDB, è necessario cambiare la dimensione della colonna in UCMDB nel seguente modo:

a Scegliere **Amministrazione** > **Gestione impostazioni infrastruttura**. Individurare l'impostazione **Radice oggetto** e cambiarla in **dati**. Effettuare la disconnessione da UCMDB e accedere nuovamente per rendere effettivi i cambiamenti.

b Scegliere **Modeling** > **Gestione tipo CI**. Selezionare il tipo CI **dati** nelle struttura e selezionare la scheda Attributi. Modificare l'attributo **User Label** cambiando **Value Size** in 900.

c Tornare a **Gestione impostazioni infrastruttura** e ripristinare il valore originale dell'impostazione **Radice oggetto** al valore originale. Disconnettere e accedere per rendere effettivi i cambiamenti

16 Se Gestione flusso dati è già in esecuzione su UCMDB, i dati della cronolgia potrebbero essere danneggiati. Per correggere il problema, eseguire la seguente procedura:

a Avviare il browser Web e specificare il seguente indirizzo: http://<UCMDB server address>.<domain_name>:8080/jmx-console.

Immettere le credenziali di autenticazione della console JMX, che per impostazione predefinita sono:

- Nome di accesso = **sysadmin**
- Password = **sysadmin**

b In **UCMDB**, selezionare **Cronologia servizi DB**.

c Selezionare il metodo **Fix902EndTimeRecords**.

d Per lo stato effettivo del cliente, immettere **1** per il valore ID cliente, quindi fare clic su **Invoke**.

e Se l'operazione ha esito positivo, viene visualizzato il messaggio "Cronologia DB aggiornata".

f Per lo stato autorizzato del cliente, immettere **1100001** per il valore ID cliente, quindi fare clic su **Invoke**.

g Se l'operazione ha esito positivo, viene visualizzato il messaggio "Cronologia DB aggiornata".

Configurare le opzioni avanzate di connessione al database

Nel caso siano necessarie proprietà avanzate di connessione al database per supportare la distribuzione del database, è possibile procedere una volta completata l'esecuzione della Procedura guidata di post installazione. Configuration Manager supporta tutte le opzioni di connessione al database supportate dal driver JDBC del fornitore e possono essere configurate utilizzando l'URL di connessione al database. Per configurare altre connessioni avanzate, modificare la proprietà **jdbc.url** nel file <**Configuration Manager installation directory**>**conf****database.properties**.

I seguenti esempi illustrano le opzioni avanzate per Microsoft SQL Server:

- **Autenticazione Windows (NTLM).** Per applicare l'autenticazione Windows, aggiungere la proprietà del dominio all'URL di connessione JTDS nel file database.properties. Specificare il dominio Windows per l'autenticazione.

  Ad esempio:

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

- **SSL.** Per informazioni sulla protezione della connessione del server MS SQL utilizzando SSL, consultare http://jtds.sourceforge.net/faq.html.

I seguenti esempi illustrano le opzioni avanzate per Oracle Database Server:

- **URL Oracle.** Secificare l'URL di connessione del driver nativo di Oracle. Specificare un nome server e un SID Oracle validi. Se si utilizza **Oracle RAC**, specificare in alternativa i dati di configurazione di Oracle RAC.

  Nota: Per ulteriori informazioni sul formato URL del driver JDBC nativo di Oracle, consultare http://www.orafaq.com/wiki/JDBC#Thin_driver. Per ulteriori informazioni sulla configurazione dell'URL per Oracle RAC, consultare http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Per informazioni sulla protezione della connessione a Oracle utilizzando SSL, consultare le spiegazioni di seguito:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Configurazione database - Supporto MLU (Multi-Lingual Unit)

Questa sezione descrive le impostazioni del database necessario per la localizzazione del supporto.

Impostazioni Oracle Server

La tabella di seguito elenca le impostazioni necessarie per Oracle Server:

Opzione	Supportato	Consigliato	Note
Set di caratteri	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Impostazioni Microsoft SQL Server

La tabella di seguito elenca le impostazioni necessarie per Microsoft SQL Server:

Opzione	Supportato	Consigliato	Note
Raccolta	Maiuscole/Minuscole. Non supporta l'ordinamento binario e la distinzione tra maiuscole e minuscole. L'ordinamento con distinzione tra maiuscole e minuscole è supportato solo con una combinazione di accenti, kana o impostazioni di larghezza.	Utilizza la finestra di dialogo Impostazioni raccolta per selezionare la raccolta. Non selezionare la casella di controllo binario. Accento, kana e distinzione larghezza devono essere selezionati in base ai requisiti per la lingua dati attinenti. La lingua selezionata deve essere la stessa delle impostazioni internazionali del sistema operativo Windows.	Si limita alla Raccolta locale e alle definizioni inglesi predefinite.
Raccolta proprietà database	Predefinito del server		

Nota:

Per tutte le lingue: **<Lingua>_CI_AS** è l'opzione minima richiesta.
Ad esempio, in Giapponese, se si desidera selezionare le opzioni Distinzione Kana e Distinzione larghezza, l'opzione consigliata è:
Japanese_CI_AS_KS_WS o **Japanese_90_CI_AS_KS_WS**. Questo consiglio indica che i caratteri giaponesi sono di tipo Distinzione accento, Distinzione Kana e Distinzione larghezza.

- **Distinzione accento (_AS).** Distingue tra i caratteri accentati e non accentati. Ad esempio, **a** non è uguale a **á**. Se l'opzione non è selezionata, Microsoft SQL Server considera identiche le versioni accentate e non accentate delle lettere per scopi di ordinamento.
- **Distinzione Kana (_KS).** Distingue tra i due tipi di caratteri kana giapponesi: Hiragana e Katakana. Se l'opzione non è selezionata, Microsoft SQL Server considera i caratteri Hiragana e Katakana uguali per scopi di ordinamento.
- **Distinzione larghezza (_WS).** Distingue tra caratteri a byte singolo e caratteri uguali quando rappresentati come caratteri a byte doppio. Se l'opzione non è selezionata, Microsoft SQL Server considera identica la rappresentazione a byte singolo e a byte doppio dello stesso carattere per scopi di ordinamento.

Abilitare Lightweight Single Sign-On

Alcuni utenti di Configuration Manager dispongono anche dell'autorizzazione di accesso a UCMDB. Per facilità d'uso, Configuration Manager offre un collegamento diretto all'interfaccia utente di UCMDB (selezionare **Amministrazione** > **Apri UCMDB**). Per utilizzare single sign-on (che preclude la necessità di accedere a UCMDB una volta eseguito l'accesso a Configuration Manager), è necessario abilitare LW-SSO sia per Configuration Manager che UCMDB e assicurarsi che entrambi lavorino con lo stesso initString. Questa attività descrive come abilitare LW-SSO in Configuration Manager e in UCMDB.

Per abilitare LW-SSO:

1. Aprire il seguente file nella directory di installazione di Configuration Manager: **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

   Nota: questo file non esiste prima dell'avvio di Configuration Manager.

   ---

2. Individuare la sezione seguente:

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

   e verificare che il valore sia **true**.

3. Individuare la sezione seguente:

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

   e immettere il dominio del server Configuration Manager dopo <**dominio**>.

4 Individuare la sezione seguente:

```
<initString="Questa stringa deve essere sostituita"></crypto>
```

e sostituire "Questa stringa deve essere sostituita" con una stringa condivisa utilizzata da tutte le applicazioni considerate attendibili che interagiscono con LW-SSO.

5 Individuare la sezione seguente:

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>Questo valore deve essere sostituito dal domino
dell'applicazione</DNSDomain>
<DNSDomain>Questo valore deve essere sostituito dal domino dell'altra
applicazione</DNSDomain>
</trustedHosts>
</multiDomain-->
```

Rimuovere il delimitatore all'inizio e immettere i domini del server Configuration Manager negli elementi DNSDomain (al posto di Questo valore deve essere sostituito dal domino dell'applicazione. L'elenco deve includere il dominio del server immesso nel passaggio 3 a pagina 19.

6 Salvare il file con i cambiamenti e riavviare il server.

7 Avviare il browser Web e specificare il seguente indirizzo: http://<UCMDB server address>.<domain_name>:8080/jmx-console.

Immettere le credenziali di autenticazione della console JMX, che per impostazione predefinita sono:

- Nome di accesso = **sysadmin**
- Password = **sysadmin**

8 In **UCMDB-UI**, selezionare **Configurazione LW-SSO** per aprire la pagina JMX MBEAN View.

9 Selezionare il metodo **setEnabledForUI**, impostare il valore su **true** e fare clic su **Invoke**.

10 Selezionare il metodo **setDomain**. Immettere il nome del dominio del server UCMDB e fare clic su **Invoke**.

11 Selezionare il metodo **setInitString**. Immettere lo stesso initString immesso per Configuration Manager nel passaggio 4 a pagina 20 e fare clic su **Invoke**.

12 Se Configuration Manager e UCMDB sono posizionati nello stesso dominio, selezionare il metodo **addTrustedDomains** e immettere i nomi dei domini dei server UCMDB e Configuration Manager. Fare clic su **Invoke**.

13 Per visualizzare la configurazione LW-SSO come è stata salvata nel meccanismo impostazioni, selezionare il metodo **retrieveConfigurationFromSettings** e fare clic su**Invoke**.

14 Per visualizzare la configurazione LW-SSO effettiva caricata, selezionare il metodo **retrieveConfiguration** e fare clic su **Invoke**.

Supporto IPv6

Configuration Manager supporta l'URL IPv6 solo per URL pubblici.

Per utilizzare Configuration Manager con un indirizzo IPv6:

1 Assicurarsi che il sistema operativo supporti IPv6. Per informazioni, consultare la documentazione relativa al sistema operativo.

2 Aprire il file **client-config.properties**, posizionato nella directory **conf** della directory di installazione <**Configuration Manager**>. Cambiare il valore del parametro **bsf.server.url** sull'indirizzo IPv6 racchiuso tra parentesi quadre. Ad esempio:

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

2

Configuration Manager Configurazione guidata di post installazione

Questo capitolo comprende:

Configuration Manager Panoramica della configurazione di post installazione

Questo capitolo fornisce una descrizione dettagliata delle pagine della Procedura di post installazione di Configuration Manager e delle attività di configurazione associate. È il contenuto che si apre quando si fa clic su **Help** da una qualsiasi pagina nella procedura guidata.

Pagina connessione database

Questa sezione comprende:

Generale

È necessario impostare una connessione al database associata con una connessione URL standard. Nel caso siano necessarie funzionalità avanzate, ad esempio Oracle Real Application Cluster, impostare una connessione standard, quindi modificare manualmente il file **database.properties** per configurare le funzionalità avanzate.

Configuration Manager utilizza driver nativi sia per Oracle che Microsoft SQLServer. Questo significa che, in generale, sono supportate tutte le funzionalità dei driver nativi, posto che queste funzionalità possano essere configurate utilizzado l'URL del database. L'URL si trova nel file **database.properties**.

Nota: la configurazione delle funzionalità avanzate deve essere eseguita una volta completato il processo di post installazione e dopo aver stabilito una configurazione di lavoro.

Parametri

Per impostare la connessione al database, definire i seguenti parametri:

Parametro	Valore consigliato	Descrizione
Fornitore	<definito dall'utente>	Fornitore database Valori possibili: **Oracle** o **Microsoft** HP Universal CMDB può essere installato utilizzando lo stesso programma di installazione di Configuration Manager o, separatamente. Se Configuration Manager e UCMDB saranno installati sullo stesso computer utilizzando lo stesso programma di installazione, allora il valore predefinito per questo parametro sarà il fornitore del database già selezionato nella procedura guidata di post installazione di UCMDB. I valori predefiniti vengono impostati solo quando vengono installate entrambe le applicazioni utilizzando gli stessi programmi di installazione. Se si sta eseguento l'installazione utilizzando pacchetti di installazione diversi, anche quando UCMDB è installato sullo stesso computer come Configuration Manager, il valori predefiniti NON verranno visualizzati nella procedura guidata di post installazione.
Nome host	<definito dall'utente>	Nome host del server database Se Configuration Manager e UCMDB saranno installati sullo stesso computer, allora il valore predefinito di questo parametro sarà il server database già selezionato nella procedura guidata di post installazione di UCMDB. **Questo valore è obbligatorio.**

Parametro	Valore consigliato	Descrizione
Porta	<definito dall'utente>	Porta del listener del database Se Configuration Manager e UCMDB saranno installati sullo stesso computer, allora il valore predefinito di questo parametro sarà la porta del database già selezionata nella procedura guidata di post installazione di UCMDB. Per Oracle, il valore predefinito è **1521**. Per Microsoft SQL Server, il valore predefinito è **1433**. **Questo valore è obbligatorio.**
SID/DB	<definito dall'utente>	Il nome del SID Oracle o il nome del database di Microsoft SQL Server Se Configuration Manager e UCMDB saranno installati sullo stesso computer, allora il valore predefinito di questo parametro sarà il SID/DB del database già selezionato nella procedura guidata di post installazione di UCMDB. **Questo valore è obbligatorio.**
Nome utente	<definito dall'utente>	Il nome utente utilizzato per accedere al database. **Questo valore è obbligatorio.**
Password	<definito dall'utente>	La password utilizzata per accedere al database.

Opzioni

Sono disponibili le seguenti opzioni:

Parametro	Valore consigliato	Descrizione
Crittografia password	<definito dall'utente>	Se selezionata, questa opzione esegue la crittografia della password nel file **database.properties**. Per ragioni legate alla protezione, si consiglia di crittografare le password salvate nei file di testo.
Crea oggetti schema	<definito dall'utente>	Se selezionata, questa opzione crea oggetti schema necessari per l'esecuzione di Configuration Manager. Deselezionare questa opzione solo quando l'installazione utilizza uno schema esistente creato in precedenza e popolato con oggetti Configuration Manager.

Test

Nota: si consiglia vivamente di testare le proprietà della connessione prima di continuare.

Per testare le proprietà della connessione, fare clic su **Test**. La procedura guidata tenta di accedere al database e di verificare la connessione. I risultati del test verranno visualizzati a destra del pulsante **Test**.

Il database genera più messaggi di errore. Non necessitano di spiegazioni e in genere si riferiscono all'inserimento di nome utente o password errati. L'errore deve essere corretto, seguito da un risultato di test eseguito, prima di continuare.

Pagina server applicazioni

Questa sezione comprende:

Generale

Impostare il Server applicazioni di Configuration Manager utilizzando i numeri di porta predefiniti mostrati di seguito.

Parametri

Per impostare il Server applicazioni di Configuration Manager, definire i seguenti parametri:

Parametro	Valore consigliato	Descrizione
Nome host	<definito dall'utente>	Nome esterno del server applicazioni Per impostazione predefinita, questo valore è il nome host completo del computer con la procedura guidata in esecuzione (e Configuration Manager). In alcune distribuzioni, questo nome deve essere diverso, ad esempio quando si distribuisce un server web davanti al Server applicazioni di Configuration Manager.
Personalizza porte	<definito dall'utente>	Per impostazione predefinita, questa opzione non è selezionata. Quando selezionata, è possibile personalizzare i numeri di porta predefiniti del server applicazioni.

Parametro	Valore consigliato	Descrizione
Porta HTTP	<definito dall'utente>	La porta HTTP del Server applicazioni di Configuration Manager Valore predefinito: **8080** Valore predefinito quando installato sullo stesso computer come HP Universal CMDB: **8180**
Porta HTTPS	<definito dall'utente>	La porta HTTPS del Server applicazioni di Configuration Manager Valore predefinito: **8443** Valore predefinito quando installato sullo stesso computer come UCMDB: **8143**
Porta Tomcat	<definito dall'utente>	Porta di gestione del Server applicazioni di Configuration Manager Valore predefinito: **8005**
Porta AJP	<definito dall'utente>	Porta AJP (Apache Java Protocol) Server applicazioni di Configuration Manager Valore predefinito: **8009**
Porta HTTP JMX	<definito dall'utente>	Porta HTTP JMX Server applicazioni di Configuration Manager Valore predefinito: **39900**
Porta remota JMX	<definito dall'utente>	Porta remota JMX Server applicazioni di Configuration Manager Valore predefinito: **39600**

Pagina di configurazione del servizio Windows

Scegliere se installare o meno Configuration Manager come servizio Windows. Questa opzione è disponibile solo per l'installazione su un computer Windows.

Il servizio Windows può essere impostato manualmente utilizzando l'utilità **create-windows-service.bat** disponibile nella directory **cnc-home/bin**.

Pagina credenziali utenti

Questa sezione comprende:

➤ "Generale" a pagina 30

Generale

Impostare i seguenti utenti iniziali di Configuration Manager:

Parametro	Valore consigliato	Descrizione
Utente amministratore	<definito dall'utente>	Utente amministrativo di Configuration Manager—"super utente"
Utente di integrazione	<definito dall'utente>	Utente creato da Configuration Manager in HP Universal CMDB per ragioni di integrazione

---

Nota: è necessario fornire le credenziali di nome utente e password sia per gli utenti amministrativi che di integrazione.

Pagina connessione di HP Universal CMDB

Questa sezione comprende:

Generale

L'impostazione della connessione a HP Universal CMDB è facoltativa

Quando si installa Configuration Manager sullo stesso computer di UCMDB tramite una installazione combinata, non è necessario inserire nessuna informazioni in questa pagina.

Quando UCMDB non viene installato tramite una installazione combinata, o quando si installa UCMDB su un computer diverso, anche quando si esegue la connessiona UCMDB su localhost, o quando si installa UCMDB prima di installare Configuration Manager, allora UCMDB deve essere attivo ed è necessario fornire queste proprietà di connessione.

Nota: quando si esegue l'installazione utilizzando un'istanza remota di UCMDB, l'istanza deve essere attiva e in esecuzione. Quando si esegue l'installazione di Configuration Manager e UCMDB sullo stesso computer, UCMDB deve essere disattivo mentre è in esecuzione questa procedura guidata.

Parametri

Per impostare la connessione UCMDB, definire i seguenti parametri:

Parametro	Valore consigliato	Descrizione
Usa HP UCMDB su un host diverso	<definito dall'utente>	Selezionare questa opzione per abilitare tutte le altre proprietà quando si installa Configuration Manager e UCMDB su computer diversi.
Nome host	<definito dall'utente>	Nome host su cui è installato UCMDB
Porta	<definito dall'utente>	Porta su cui è installato UCMDB
Protocollo	<definito dall'utente>	HTTP o HTTPS
Cliente	<definito dall'utente>	Cliente UCMDB
Nome utente amministrativo	<definito dall'utente>	Nome utente sysadmin UCMDB
Password amministrativa	<definito dall'utente>	Password sysadmin UCMDB

Test

Nota: si consiglia vivamente di testare le proprietà della connessione prima di continuare.

Per testare le proprietà della connessione, fare clic su **Test**. La procedura guidata tenta di accedere a UCMDB e di verificare la connessione. I risultati del test verranno visualizzati a destra del pulsante **Test**.

UCMDB genera vari messaggi di errore. Non necessitano di spiegazioni e in genere si riferiscono all'inserimento di nome utente o password errati. L'errore deve essere corretto, seguito da un risultato di test eseguito, prima di continuare.

Pagina di riepilogo

Vengono visualizzate tutte le modalità di selezione nelle pagine precedenti della procedura guidata. Assicurarsi della precisione di tutte le selezioni e apportare tutti i cambiamenti necessari. Quando tutte le selezioni sono corrette, fare clic su **Next** per completare le attività di configurazione della procedura guidata.

Pagina finale

È la pagina finale della Configurazione guidata di post in**stallazione** di Configuration Manager. Le attività di configurazione di post installazione sono state completate. Fare clic su **Finish** per chiudere la procedura guidata.

Nota: anche dopo aver completato tutte le attività, si consiglia di controllare i registri in **cnc-home/tmp/chp/app.log**.

3

Configurare LDAP

HP UCMDB Configuration Manager utilizza LDAP per la gestione di utenti, ruoli e autorizzazioni. Questo capitolo descrive le procedure per la configurazione e la risoluzione dei problemi relativi a LDAP.

Questo capitolo comprende:

Panoramica di LDAP

Configuration Manager viene fornito con un server LDAP interno (identificato nell'interfaccia utente come **Condiviso**) e può essere connesso a un server LDAP organizzativo. Configuration Manager utilizza questi server per individuare uenti, gruppi e ruoli; per salvare i dati di personalizzazione; e per autenticare gli utenti. È possibile scegliere quali di questi utilizzeranno il server LDAP organizzativo e quali il server LDAP interno.

Una distribuzione tipica deve utilizzare il server LDAP interno (condiviso) per salvare i ruoli e utilizzare il server LDAP (organizzativo) per il resto.

Scegliere i fornitori

1. Accedere a **Configuration Manager** come utente amministratore.
2. Scegliere **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti**, e selezionare SHARED o EXTERNAL per ciascuno dei seguenti attributi in relazione alle proprie preferenze per i fornitori (SHARED è la selezione predefinita):
   - Fornitore autenticazione
   - Fornitore gruppi
   - Fornitore personalizzazione
   - Fornitore ruoli
   - Fornitore relazioni ruoli
3. Salvare il set di configurazione.

Effettuare la connessione all'LDAP organizzativo

HP UCMDB Configuration Manager viene configurato inizialmente con un LDAP interno (condiviso). Questa sezione descrive le procedure per la connessione al server LDAP organizzativo.

Questa sezione comprende:

Configurare la connessione LDAP

Questa sezione spiega come connettere Configuration Manager a un server LDAP esterno. Il server LDAP esterno è un LDAP organizzativo e contiene gli utenti organizzativi.

1 Accedere a **Configuration Manager** come utente amministratore.

2 Scegliere **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazine gestione utenti** > **Repository utenti esterno**, e aggiornare i seguenti attributi in relazione alle proprieta LDAP organizzativo:

Informazioni generali per la connessione a LDAP generale

ldapHost: <nome host LDAP>

ldapPort: <numero porta LDAP>

enableSSL: <True/false—utilizza la connessione SSL per LDAP>

useAdministrator: <True/false—utilizza l'utente per effettuare la connessione a LDAP>

ldapAdministrator: <nome utente LDAP (deve essere definito se **useAdministrator=true)**>

ldapAdministratorPassword: <password utente LDAP (deve essere definito se **useAdministrator=true**)>

3 Salvare il set di configurazione.

Configurare i Fornitori gruppi e utenti

Questa procedura imposta l'LDAP organizzativo (repository esterno) come fornitore per gruppi e utenti. L'LDAP interno (repository condiviso) viene ancora utilizzato per l'autenticazione, anche se gli utenti e i gruppi vengono recuperati dall'LDAP esterno. Questa modalità è utilizzata per testare la configurazione LDAP esterna e per l'assegnazione delle autorizzazioni agli utenti organizzativi.

Per impostare i Provider gruppi e utenti:

1. Se non ci si trova già in questa pagina, scegliere **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno**. Assicurarsi di utilizzare lo stesso set di configurazione provvisorio salvato nella sezione "Configurare la connessione LDAP" a pagina 37.
2. Aggiornare i seguenti attributi in relazione alle proprietà LDAP organizzativo:
   a. **Ricerca utenti**

      usersBase: <DN di base per la ricerca utenti>

      usersScope: <Ambito per la ricerca utenti>

      usersFilter: <Filtro per la ricerca utenti>

   b. **Classe oggetto utenti** (dipende dal fornitore LDAP)

      usersObjectClass: <Classe oggetto LDAP utenti>

      usersUniqueIDAttribute: <attributo ID univoco utenti obbligatorio>

      I seguenti attributi sono opzionali:

      usersDisplayNameAttribute: <attributo nome utente visualizzato obbligatorio>

      usersLoginNameAttribute: <attributo LDAP nome accesso utenti>

      usersFirstNameAttribute: <attributo LDAP nome utenti>

      usersLastNameAttribute: <attributo LDAP cognome utenti>

      usersEmailAttribute: <attributo LDAP e-mail utenti>

      usersPreferredLanguageAttribute: <attributo LDAP lingua preferita utenti>

      usersPreferredLocationAttribute: <attributo LDAP località preferita utenti>

      usersTimeZoneAttribute: <attributo LDAP fuso orario utenti>

      usersDateFormatAttribute: <attributo LDAP formato data utenti>

      usersNumberFormatAttribute: <attributo LDAP formato numerico utenti>

usersWorkWeekAttribute: <attibuto LDAP settimana lavorativa utenti>

usersTenantIDAttribute: <attributo ID univoco proprietario utenti>

usersPasswordAttribute: <attributo LDAP password utenti>

c **Ricerca gruppi**

groupsBase: <DN di base per la ricerca gruppi>

groupsScope: <ambito LDAP per la ricerca gruppi>

groupsFilter: <filtro per la ricerca gruppi>

rootGroupsBase: <DN di base per la ricerca gruppi principali>

rootGroupsScope: <ambito LDAP per la ricerca gruppi principali>

rootGroupsFilter: <filtro per la ricerca gruppi>

d **Classe oggetto gruppi** (dipende dal fornitore LDAP)

groupsObjectClass: <Classe oggetto LDAP gruppi>

groupsMembersAttribute: <attributo LDAP membri gruppi>

I seguenti attributi sono opzionali:

groupsNameAttribute: <attributo LDAP nome univoco gruppi>

groupsDisplayNameAttribute: <attributo LDAP nome visualizzato gruppi>

groupsDescriptionAttribute: <attributo LDAP descrizioni gruppi>

enableDynamicGroups: <abilita gruppi dinamici>

dynamicGroupsClass: <classe oggetto LDAP gruppi dinamici>

dynamicGroupsMemberAttribute: <attributo LDAP membri gruppi dinamici>

dynamicGroupsNameAttribute: <attributo LDAP nome univoco gruppi dinamici>

dynamicGroupsDisplayNameAttribute: <attributo LDAP nome visualizzato gruppi dinamici>

dynamicGroupsDescriptionAttribute: <attributo LDAP descrizione gruppi dinamici>

e **Gerarchia gruppi** (se LDAP organizzativo utilizza la gerarchia dei gruppi)

enableNestedGroups: <abilita supporto dei gruppi nidifcati>

maximalAllowedGroupsHierarchyDepth: <profondità massima consentita per la gerarchia dei gruppi>

f **Configurazione avanzata**

ldapVersion: <Versione LDAP>

baseDistinguishNameDelimiter: <delimitatore DN di base>

scopeDelimiter: <delimitatore ambito>

attributeValuesDelimiter: <delimitatore valori attributo LDAP>

3 Salvare il set di configurazione provvisorio.

Attivare il set di configurazione

1 Scegliere **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti**, e aggiornare quanto segue:

Origine UUM esterno: True

Fornitore gruppi: EXTERNAL

Fornitore utenti: EXTERNAL

2 Salvare il set di configurazione, quindi attivarlo.

3 Disconnettere e riavviare il server **Configuration Manager**.

Assegnare le autorizzazioni agli utenti

Questa procedura assegna i ruoli **Amministratore di sistema** agli utenti organizzativi. Un utente con ruolo **Amministratore di sistema** ha le autorizzazioni per assegnare ruoli pertinenti agli altri utenti organizzativi.

1 Accedere a **Configuration Manager** come utente amministratore.

2 Aprire il modulo **Gestione utenti** (**Amministrazione** > **Gestione utenti**).

3 Verificare di visualizzare i gruppi e gli utenti dal proprio LDAP organizzativo.

4 Scegliere **Gestione utenti** > **riquadro Ricerca utenti** e cercare gli utenti che saranno gestiti come amministratori — ad esempio: Nome = j*, Cognome = Smith.

5 Aggiungere il ruolo **Amministratore di sistema** agli utenti.

Impostare il Fornitore autenticazione per l'LDAP esterno

Questa procedura imposta l'LDAP organizzativo esterno come Fornitore autenticazione, pertanto verranno utilizzati gli utenti organizzativi per l'autenticazione.

1 Scegliere **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti**, e aggiornare quanto segue:

Fornitore autenticazione: EXTERNAL

2 Salvare il set di configurazione, quindi attivarlo.

3 Disconnettere e riavviare il server **Configuration Manager**.

4 Accedere utilizzando uno degli utenti organizzativi asseganti al ruolo **Amministratore di sistema**.

Importare il certificato LDAP

Nel caso sia necessario un certificato per la connessione all'LDAP organizzativo, eseguire le seguenti operazioni:

1 Esportare il certificato su un file.

2 Arrestare il servizio di Windows Configuration Manager.

3 Eseguire il seguente comando:

<Configuration Manager installation>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <certificate alias> -keystore <Configuration Manager installation>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <certificate file path>

4 Avviare il servizio di Windows Configuration Manager.

Configurare l'LDAP interno (condiviso)

Cambiare la password del server LDAP interno (condiviso) (opzionale)

Per ragioni legate alla protezione, è possibile cambiare la password del server LDAP (condiviso) interno.

1. Accedere a **HP Universal CMDB Configuration Manager**.
2. Aprire una riga di comando e scorrere fino alla cartella **<Configuration Manager installation>\ldap\serverRoot\bat** .
3. Eseguire **ldappasswordmodify -h localhost -p <ldap port> -D "cn=Directory Manager" -w <ldap admin password> -c <ldap admin password> -n <new ldap admin password>**.
   a. La password amministratore ldap predefinita è **ldapadmin**.
   b. La porta predefinita è **2389**.
   c. Assicurarsi che il comando venga eseguito correttamente e solo a questo punto continuare con i seguenti passaggi.
4. In **UCMDB Configuration Manager**, selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Archivio utenti condiviso**.
5. Aggiornare la password nell'attributo **ldapAdministratorPassword**.
6. Salvare il set di configurazione, quindi attivarlo.
7. Disconnettere **UCMDB Configuration Manager**.
8. Riavviare il server **UCMDB Configuration Manager**.

Configurare la porta LDAP interno (condiviso)

La porta predefinita 2389 potrebbe essere già utilizzata da un'altra applicazione. Per cambiare la porta predefinita, usare la procedura seguente.

Per configurare la porta LDAP interno:

1. Aprire una riga di comando e scorrere fino alla cartella **<Configuration Manager installation>\ldap\serverRoot\bat** .

2. Eseguire il comando:
   dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <ldap admin password> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<new port>

   La <password amministratore ldap> predefinita è **ldapadmin**.
3. Assicurarsi che non venga visualizzato alcun messaggio di errore e solo a questo punto continuare con i seguenti passaggi.
4. Accedere a HP Universal CMDB Configuration Manager.
5. In UCMDB Configuration Manager, selezionare A**mministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti condiviso**, e aggiornare il numero della porta nell'attributo **ldapPort**.
6. Salvare il set di configurazione, quindi attivarlo.
7. Disconnettere UCMDB Configuration Manager.
8. Riavviare il server UCMDB Configuration Manager.

Risoluzione dei problemi relativi a LDAP

Problema: impossibile stabilire una comunicazione con il server LDAP. Nel registro è presente un'eccezione di comunicazione.

Soluzione: verificare le impostazioni per host LDAP, porta e modalità SSL:

a. Verificare che l'host LDAP e la porta siano configurati correttamente: selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno** e le impostazioni **ldapHost, ldapPort**.

b. Verificare che la modalità SSL sia configurata correttamente. Verificare con l'amministratore LDAP organizzativo se per la connessione LDAP è necessario l'utente amministratore. Selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno** e selezionare l'impostazione **enableSSL**.

c Verificare che sia installato il certificato server appropriato. Eseguire il seguente comando:

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

d Verificare con l'amministratore LDAP organizzativo se per la connessione LDAP è necessario l'amministratore. Selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno** e verificare le seguenti impostazioni: **useAdministrator, ldapAdministrator, ldapAdministratorPassword**

Problema: nella schermata di gestione gruppi o utente non viene visualizzato alcun gruppo. Nessuna eccezione nei registri.

Soluzione: verificare quanto segue:

a Verificare che i filtri di ricerca utenti e gruppi siano configurati correttamente: selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno** e modificare le seguenti proprietà: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

b Aprire il browser client LDAP e cercare gli utenti nel DNS di base.

Problema: interfaccia utente troppo lenta.

Soluzione: in genere è causato dalla presenza di un numero eccessivo di gruppi o utenti configurati nell'LDAP. Configurare il DNS di base e i filtri per ridurre il numero di gruppi al subset pertinente nel seguente modo:

a Selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno**

b Modificare le seguenti impostazioni: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

Problema: nella schermata di gestione gruppi o utenti non vengono visualizzati alcuni utenti noti.

Soluzione: la schermata di gestione utenti e gruppi mostra solo gli utenti che appartengono ad alcuni gruppi. Inserire gli utenti nei gruppi corretti nell'LDAP in modo da visualizzarli nella schermata principale.

Problema: potrebbe essere necessario molto tempo per effettuare l'accesso.

Soluzione: l'utente potrebbe appartenere a troppi gruppi. È possibile ottimizzare l'ora di avvio cambiando il filtro di ricerca dei gruppi, in modo da ottenere meno gruppi, nel modo seguente:

a Selezionare **Amministrazione** > **Amministrazione server** > **Gestione utenti** > **Configurazione gestione utenti** > **Repository utenti esterno**

b Modificare l'impostazione **groupsFilter**.

4

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.

Questa sezione comprendere i seguenti argomenti:

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.

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 necessario.** 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 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.

- **Mappatura utente (Sincronizzazione).** Il framework LW-SSO non garantisce la mappatura utente tra le applicazioni integrate. Quindi, l'applicazione integrata deve monitorare la mappatura utente. 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.

Risoluzione dei problemi e limitazioni

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 aggirare il 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. L'W-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

- **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 bilanciamento del carico.** Si deve configurare un bilanciamento del carico distribuito con LW-SSO per poter utilizzare sessioni sticky.

5

Autenticazione gestione identità

Questo capitolo comprende:

Accettare l'Autenticazione gestione identità

Se si utilizza Gestione identità e si decide di aggiungere HP Universal CMDB Configuration Manager, è necessario svolgere questa attività.

Questa attività descrive come configurare HP Universal CMDB Configuration Manager per accettare l'Autenticazione gestione attività.

Questa attività include le seguenti fasi:

Prerequisiti

Il server Configuration Manager Tomcat deve essere collegato al proprio server Web (IIS o Apache) protetto tramite Gestione identità tramite un connettore Tomcat Java (AJP13).

Per le istruzioni sull'utilizzo di un connettore Tomcat Java (AJP13), consultare la documentazione di Tomcat Java (AJP13).

Configurare HP Universal CMDB Configuration Manager per accettare Gestione identità

Per configurare Tomcat Java (AJP13) con IIS6:

1. Configurare Gestione identità per inviare una intestazione/richiamata di personalizzazione che contiene il nome utente e richiedere il nome dell'intestazione.
2. Aprire il file <**Configuration Manager Install Directory**>**\conf\lwssofmconf.xml** e individuare la sezione che inizia con **in-ui-identity-management**.

   Ad esempio:

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

   a. Attivare la funzionalità rimuovendo il delimitatore.

   b. Sostituire **enabled**="**false**" con **enabled**="**true**".

   c. Sostituire **sm-user** con il nome intestazione richiesto nella fase 1.
3. Aprire il file <**Configuration Manager Install Directory**>**\conf\client-config.properties** e modificare le seguenti proprietà:

   a. Cambiare **bsf.server.url** nella URL Gestione identità e la porta nella porta Gestione identità:

   ```
   bsf.server.url=http://< Identity Manager URL>:< Identity Manager port >/bsf
   ```

   b. Cambiare **bsf.server.services.url** nel protocollo HTTP e la porta nella porta Configuration Manager originale:

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

Esempio di utilizzo di Java Connector per configurare la Gestione identità per Configuration Manager con IIS6 su un sistema operativo Windows 2003

Questa attività di esempio descrive come installare e configurare Java Connector in modo da utilizzarlo per configurare la Gestione identità da utilizzare con Configuration Manager con IIS6 in esecuzione su sistema operativo Windows 2003.

Per installare Java Connector e configurarlo per IIS6 su Windows 2003:

1. Scaricare la versione più recente di Java Connector (ad esempio, **djk-1.2.21**) dal sito Web Apache.
   a. Fare clic su **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.
   b. Selezionare la versione più recente.
   c. Scaricare il file **isapi_redirect.dll** dalla directory **amd64**.
2. Salvare il file in <**Configuration Manager Install Directory**>**\tomcat\bin\win32**.
3. Creare un nuovo file di testo con il nome **isapi_redirect.properties** nella stessa directory con isapi_redirect.dll.

   Il contenuto del file è:

   ```
   # Configuration file for the Jakarta ISAPI Redirector

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

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

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

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

   log_level=info

   # Full path to the workers.properties file
   ```

worker_file==<Configuration Manager Install Directory>\tomcat\conf\workers.properties.minimal

Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager Install Directory>\tomcat\conf\uriworkermap.properties

4 Creare un nuovo file di testo con il nome **workers.properties.minimal** in <**Configuration Manager Install Directory**>**tomcat****conf**.

Il contenuto del file è:

workers.properties.minimal -

#

This file provides minimal jk configuration

properties needed to

connect to Tomcat.

#

Defining a worker named ajp13w and of type ajp13

Note that the name and the type do not have to

match.

worker.list=ajp13w

worker.ajp13w.type=ajp13

worker.ajp13w.host=localhost

worker.ajp13w.port=8009

#END

5 Creare un nuovo file di testo con il nome **uriworkermap.properties** in <**Configuration Manager Install Directory**>**tomcat****conf**.

Il contenuto del file è:

uriworkermap.properties - IIS

#

This file provides sample mappings for example:

```
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Importante: si noti che Configuration Manager deve avere due regole. La nuova sintassi consente di riunirle in una sola regola, ad esempio:

/cnc|/*=ajp13w

---

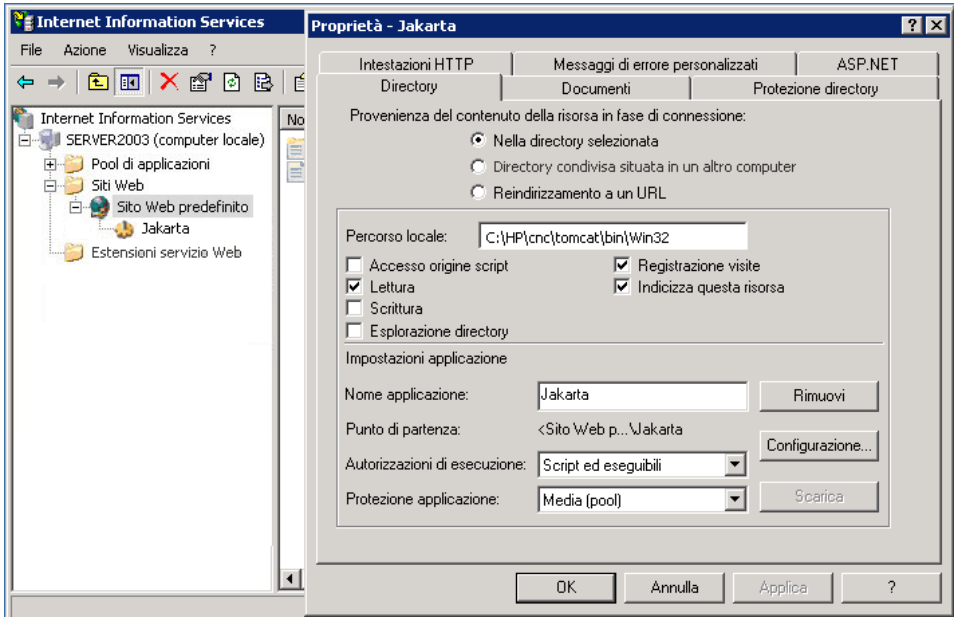
6 Creare la directory virtuale nell'oggetto sito Web corrispondente nella configurazione IIS.

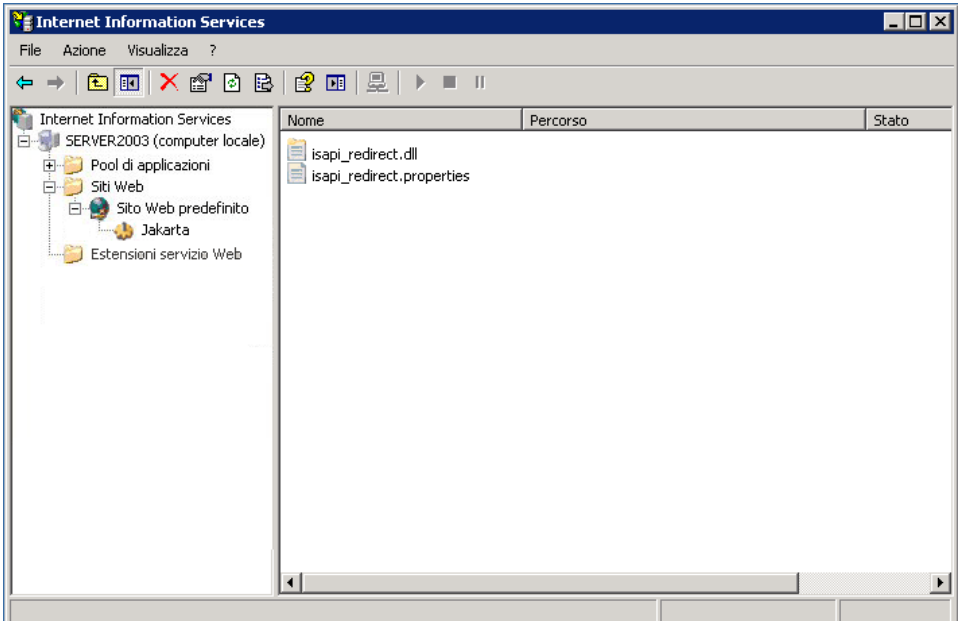
a Nel menu Start di Windows, aprire **Impostazioni\Pannello di controllo\Strumenti di amministrazione\Gestione Internet Information Services (IIS)**.

b Nel riquadro di destra, fare clic con il tasto destro su **<Nome computer locale>\Siti Web\<Nome sito Web>** e selezionare **Nuovo\Directory virtuale**.

c Assegnare alla directory il nome alias **Jakarta**, e impostare il percorso locale sulla directory contenente isapi_redirect.dll.

L'aspetto della finestra di gestione è simile a quella riportata di seguito:





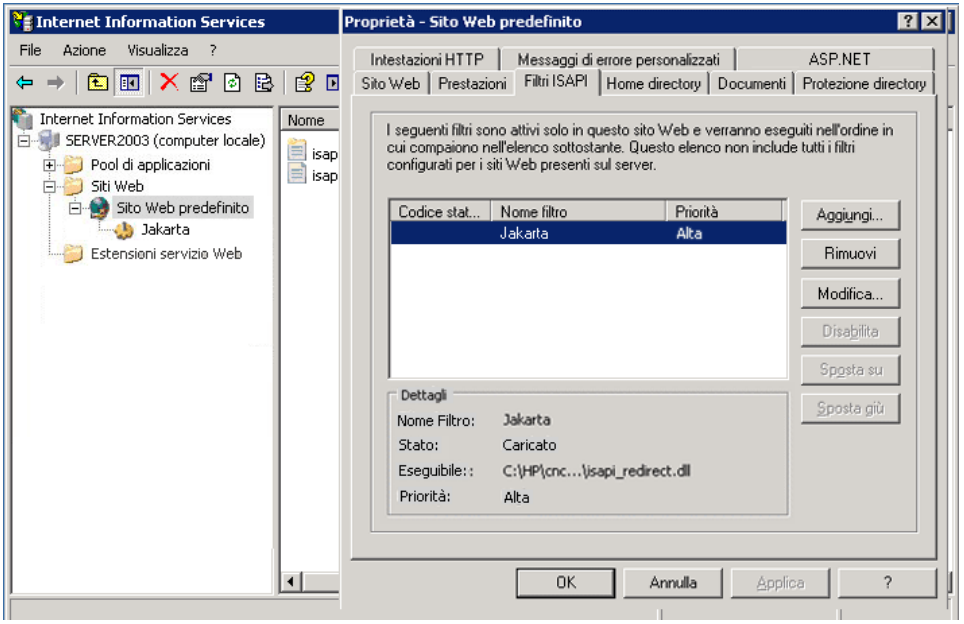
7 Aggiungere **isapi_redirect.dll** come filtro ISAPI.

a Fare clic con il tasto destro su **<Nome sito Web>** e selezionare **Proprietà**.

b Selezionare la scheda **Filtri ISAPI**, quindi fare clic sul pulsante **Aggiungi...**.

c Selezionare il Nome filtro **Jakarta**, e scorrere fino a **isapi_redirect.dll**. Viene aggiunto il filtro anche se ancora non è attivo.

L'aspetto della finestra di configurazione è simile a quella riportata di seguito:



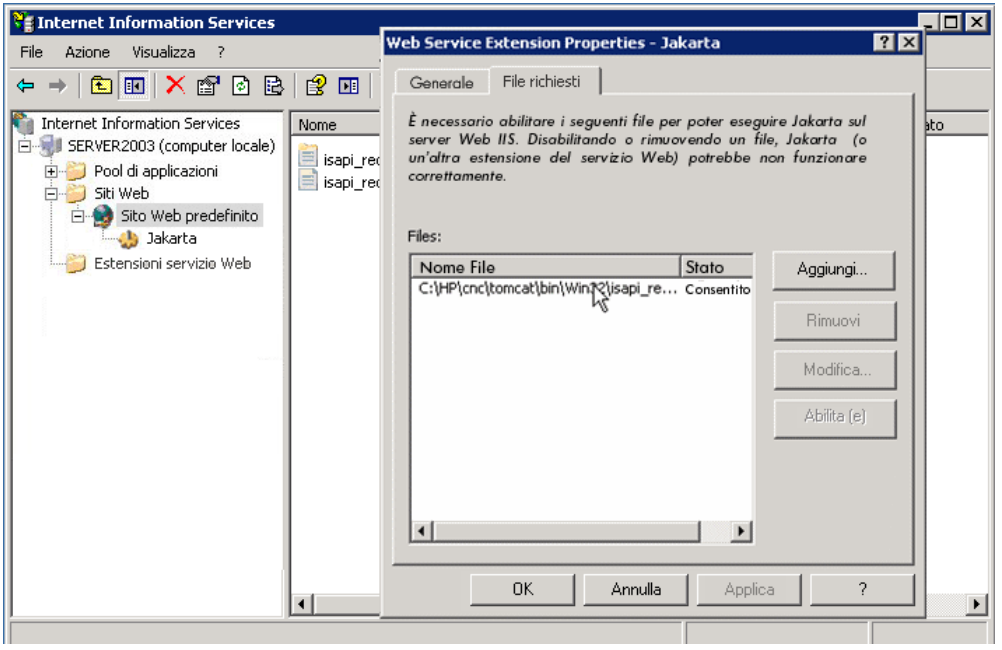
d Fare clic sul pulsante **Applica**.

8 Definire e consentire la nuova estensione del Servizio Web.

a Fare clic con il tasto destro su **<Nome computer locale>\Estensioni Servizio Web** e selezionare l'elemento del menu **Aggiungi nuova estensione Servizio Web...**.

b Assegnare il nome **Jakarta** alla nuova estensione Servizio Web, quindi scorrere fino al file **isapi_redirect.dll**.

Nota: prima di fare clic sul pulsante **OK**, selezionare la casella di controllo **Imposta lo stato dell'estensione su Consentito**.



9 Riavviare il Server Web IIS, e accedere all'applicazione tramite il Servizio Web.

6

Accedere a Configuration Manager

Questo capitolo comprende:

Accesso a Configuration Manager

L'accesso a Configuration Manager viene effettuato utilizzando un browser Web da qualunque computer dotato di una connessione di rete (Intranet o Internet) al server di Configuration Manager. Il livello di accesso concesso a un utente dipende dalle autorizzazioni dell'utente. Per informazioni sulla concessione delle autorizzazioni dell'utente, consultare "Gestione utenti" nella Guida dell'utente di *HP Universal CMDB Configuration Manager*.

Per informazioni sui requisiti del browser Web, così come i requisiti minimi per visualizzare Configuration Manager, consultare "Requisiti di sistema per Configuration Manager" a pagina 8.

Per informazioni sull'accesso protetto a Configuration Manager, consultare "Protezione avanzata" a pagina 73.

Come eseguire l'accesso a Configuration Manager

Nel browser Web, immettere l'URL del server Configuration Manager, ad esempio, **http://<nome server o indirizzo IP>.<nome dominio>:<porta>** dove **<nome server e indirizzo IP>.<nome dominio>** rappresentano il nome dominio completo (FQDN) del server Configuration Manager, mentre la **<porta>** rappresenta la porta selezionata durante l'installazione.

Accedere a Configuration Manager

1. Immettere il nome utente e la password definiti nella Procedura guidata post installazione di Configuration Manager.
2. Fare clic su **Accesso**. Una volta eseguito l'accesso, il nome utente viene visualizzato nella parte superiore destra dello schermo.
3. (Consigliato) Effettuare la connessione al server LDAP organizzativo e assegnare i ruoli amministrativi agli utenti LDAP per consentire agli amministratori di Configuration Manager di accedere al sistema. Per informazioni su come assegnare i ruoi agli utenti nel sistema Configuration Manager, cosultare "Gestione utenti" nella Guida dell'utente di *HP Universal CMDB Configuration Manager*.

Disconnessione

Una volta completata la sessione, si consiglia di disconnettersi dal sito Web per evitare accessi non autorizzati.

Per disconnettere:

Fare clic su **Disconnetti** nella parte superiore della pagina.

Nota: la scadenza predefinita per la sessione è di 30 minuti.

Accedere alla console JMX per Configuration Manager

Per ambiti relativi alla risoluzione dei problemi o per modificare alcune configurazioni, potrebbe essere necessario accedere alla console JMX.

Per accedere alla console JMX:

1. Aprire la console JMX su http://<nome server o indirizzo IP>:<porta>/cnc/jmx-console. La porta è quella configurata durante l'installazione di Configuration Manager.
2. Immettere le credenziali utente predefinite. Sono le stesse credenziali utente utilizzate per l'accesso a Configuration Manager.

Risoluzione dei problemi e limitazioni

Problema. Dopo avere cambiato il set di configurazione in Amministrazione server, il server non si avvia.

Soluzione. Tornare al set di configurazione precedente. Procedere come segue:

1. Eseguire questo comando per individuare l'ID dell'ultimo set di configurazione attivato:

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

   dove <**proprietà database**> può essere specificato puntando al percorso del file <**Configuration Manager installation directory**>**conf****database.properties**oppure specificando ciascuna proprietà del database. Ad esempio:

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

2. Eseguire questo comando per esportare l'ultimo set di configurazione:

   ```
   < HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <proprietà database> <ID set di configurazione> <nome file dump>
   ```

dove <**ID set di configurazione**> è l'ID set di configurazione dal passaggio precedente e <**file dump**> è il nome di un file temporaneo utilizzato per salvare il set di configurazione. Ad esempio, per esportare il set di configurazione con l'ID **491520** sul file **mydump.zip**, immettere:

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

3. Arrestare il servizio HP Universal CMDB Configuration Manager.
4. Eseguire questo comando per importare e attivare il set di configurazione precedente:

```
< HP Universal CMDB Configuration Manager>\bin\import-cs.bat <proprietà database> <nome file dump> --activate
```

Problema. Si è verificato un errore nella connessione UCMDB.

Soluzione. La causa potrebbe essere una delle seguenti:

- Il server UCMDB è spento. Riavviare Configuration Manager una volta attivato completamente UCMDB (verificare che lo stato del server UCMDB sia **Attivo**).
- Il server UCMDB è attivo ma le credenziali di connessione a Configuration Manager o l'URL sono errate. Avviare Configuration Manager. Scegliere Amministrazione server, cambiare le impostazioni di connessione per UCMDB, e salvare il nuovo set di configurazione. Attivare il set di configurazione e riavviare il server.

Problema. Le impostazioni di connessione LDAP sono errate.

Soluzione. Tornare al set di configurazione precedente. Impostare le impostazioni di connessione LDAP corrette e attivare il nuovo set di configurazione.

Problema. I cambiamenti al modello classe UCMDB non vengono rilevati in Configuration Manager.

Soluzione. Riavviare il server Configuration Manager.

Problema. Il registro di Configuration Manager contiene un errore **Timeout esecuzione UCMDB scaduto**.

Soluzione. Si verifica quando il database UCMDB è sovraccarico. Per correggere il problema, aumentare il timeout di connessione nel modo seguente:

1. Creare un file jdbc.properties all'interno della cartella **UCMDBServer\conf**.
2. Immettere il seguente testo: QueryTimeout=<numero in secondi>.
3. Riavviare il server UCMDB.

Problema. Configuration Manager non consente di aggiungere un vista da gestire.

Soluzione. Quando viene aggiunta una vista da gestire, in UCMDB viene creato un nuovo TQL. Se viene raggiunto il limite massimo di TQL attivi, non è possibile aggiungere la vista. Aumentare il limite dei TQL attivi in UCMDB cambiando le seguenti impostazioni in Gestione impostazioni infrastruttura:

- Numero massimo di TQL attivi nel server
- Numero massimo di TQL cliente attivi

Problema. Il certificato del server HTTPS non è valido.

Soluzione. La causa potrebbe essere una delle seguenti:

- La data di validità del certificato è scaduta. È necessario ottenere un nuovo certificato.
- L'autorità di certificazione del certificato non è un'autorità affidabile. Aggiungere l'autorità del certificato all'elenco Autorità di certificazione principale attendibile.

Problema. Quando si esegue l'accesso dalla pagina di accesso di Configuration Manager, si riceve un errore di accesso o l'accesso alla pagina è negato.

Soluzione. La causa potrebbe essere una delle seguenti:

- Il nome utente potrebbe non essere stato definito nel fornitore dell'autenticazione (LDAP esterno/condiviso). Aggiungere l'utente nel sistema Fornitore autenticazione.
- L'utente è stato definito ma non possiede l'autorizzazione per l'accesso per Configuration Manager. Concedere all'utente l'autorizzazzione per l'accesso. Come buona pratica, assegnare l'autorizzazione per l'accesso al gruppo principale di tutti gli utenti di Configuration Manager.
- Questa soluzione si applica anche in casi in cui l'accesso non riesce quando proviene da un accesso al sistema IDM.

Problema. Il server Configuration Manager non si avvia perché sono state inserite credenziali del database non corrette.

Soluzione. Se si apportano modifiche alle credenziali del database e il server non si avvia, le credenziali potrebbero essere errate. (**Nota**: la Procedura guidata post installazione non esegue automaticamente il test delle credenziali immesse. È necessario fare clic sul pulsante **Test** nella procedura guidata.) È necessario crittografare nuovamente la password del database e immettere le nuove credenziali nel file di configurazione. Procedere come segue:

1. Da una riga di comando, eseguire questo comando per crittografare la password del database aggiornata:

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

   restituisce una password crittografata.

2. Copiare la password crittografata (incluso il prefisso {ENCRYPTED}), nel parametro **db.password** in <**CnC installation folder>\conf\database.properties**.

Problema. Se il DNS non è stato configurato correttamente, potrebbe essere necessario accedere utilizzando l'indirizzo IP del server. Quando viene immesso l'indirizzo IP, si verifica un secondo errore DNS.

Soluzione. Sostituire nuovamente il nome del computer con l'indirizzo IP. Ad esempio:

Se si accede utilizzando il seguente indirizzo IP:
http://16.55.245.240:8180/cnc/

e si riceve un indirizzo con il nome del computer che mostra un errore DNS, ad esempio:
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

sostituirlo con: http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

e avviare nuovamente l'applicazione nel browser.

Problema. Il server Tomcat Configuration Manager non si avvia.

Soluzione. Provare una delle seguenti operazioni:

- Eseguire la Procedura guidata di post installazione e sostituire le porte del server Configuration Manager.
- Interrompere gli altri processi che occupano le porte di Configuration Manager.
- Cambiare manualmente le porte nel file di configurazione di Configuration Manager modificando il seguente file: **<CnC installation folder>\servers\server-0\conf\server.xml** e aggiornando le porte attinenti:
  - HTTP (8080): riga 69
  - HTTPS (8443): righe 71, 90

Problema. Nel registro di Configuration Manager è presente un errore di memoria insufficiente.

Soluzione. Aumentare la memoria Java massima come necessario.

Per cambiare la dimensione della memoria nel servizio Configuration Manager:

1. Scegliere la directory **<CnC installation folder>\cnc\bin** ed eseguire il seguente comando: edit-server-0.bat.
2. Selezionare la scheda **Java**.
3. Aggiornare i parametri **Pool di memoria iniziale** e **Pool di memoria massima**.

Per cambiare la dimensione della memoria nel file batch:

1. Scegliere la directory <**CnC installation folder**>**cnc** e aprire il file **start-server-0.bat** per la modifica
2. Individuare la riga che inizia con **SET JAVA_OPTS=-Dcnc.home**.
3. Individuare i comandi **-Xms** e **-Xmx** e cambiarli in base ai requisiti:

   -Xms<dimensione pool di memoria iniziale> -Xmx<dimensione pool di memoria massima>

   Ad esempio: per impostare il pool di memoria iniziale su 100MB e il pool di memoria massima su 800MB. immettere:

   -Xms100m -Xmx800m

Problema. La Procedura guidata di post installazione impiega molto tempo dopo aver fatto clic su **Finish**.

Soluzione. Per un sistema UCMDB che non è stato pre-configurato per la modalità consolidata, l'operazione di consolidamente dello schema può richiedere del tempo (in relazione alla quantità di dati). Attendere 15 minuti. Se non si rilevano progressi, interrompere la Procedura guidata di post installazione e riavviare il processo.

Problema. I cambiamenti nei CI in UCMDB non si riflettono in Configuration Manager.

Soluzione. Configuration Manager esegue un processo di analisi asincrona offline. Il processo potrebbe non avere ancora elaborato gli ultimi cambiamenti in UCMDB. Per risolvere il problema, provare una delle seguenti:

- Attendere alcuni minuti. L'intervallo predefinito tra le esecuzioni del processo di analisi è 10 minuti. È configurabile nel modulo Amministrazione server.
- Eseguire una chiamata JMX per eseguire il calcolo dell'analisi offline sulla vista pertinente.

➤ Scegliere Amministrazione criteri. Fare clic sul pulsante **Ricalcola analisi criteri**. In questo modo viene richiamato il processo di analisi offline per tutte le viste (può richiedere del tempo). È necessario inoltre apportare delle finte modifiche a uno dei criteri e salvarlo.

Problema. Facendo clic su **Amministrazione** > **Apri UCMDB**, si apre la pagina di accesso di UCMDB.

Soluzione. Per poter accedere a UCMDB senza accedere nuovamente, è necessario abilitare single sign-on (SSO). Per informazioni, consultare "Abilitare Lightweight Single Sign-On" a pagina 19. Inoltre, assicurarsi che l'utente di Configuration Manager che ha eseguito l'accesso sia definito nel sistema di gestione utenti di UCMDB.

Problema. Durante la configurazione di una connessione UCMDB nella Procedura guidata post installazione su un indirizzo IPv6, l'elemento del menu **Amministrazione** > **Apri UCMDB** non funziona.

Soluzione. Procedere come segue:

1. Scegliere **Amministrazione** > **Amministrazione server** > **Configuration Manager** > **Connessione UCMDB**.
2. Aggiungere le parentesi quadrate all'indirizzo IP nell'URL di accesso a UCMDB. L'URL deve avere il seguente aspetto: http://[x:x:x:x:x:x:x:x]:8080/.
3. Salvare il set di configurazione e attivarlo.
4. Riavviare Configuration Manager.

Le seguenti limitazioni si applicano quando si lavoro con Configuration Manager:

➤ Tutte le volte che viene cambiato l'orario sul server Tomcat di Configuration Manager, il server deve essere riavviato per poter aggiornare l'ora sul server.

7

Protezione avanzata

Questo capitolo comprende:

Protezione avanzata Configuration Manager

Questa sezione introduce il concetto di applicazione Configuration Manager 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.

Configuration Manager 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 Configuration Manager in modo che abbia una protezione maggiore.

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

Di seguito sono illustrate le fasi preparatorie consigliate per la protezione avanzata del sistema:

- Valutare il rischio di protezione/stato della protezione per le reti generiche, e utilizzare le conclusioni quando si decide come integrare al meglio Configuration Manager nella rete.
- Sviluppare una buona conoscenza del framework tecnico di Configuration Manager e delle funzionalità di protezione di Configuration Manager.
- Riesaminare tutte le linee guida relative alla protezione avanzata.
- Verificare che Configuration Manager sia completamente funzionante prima di avviare le procedure di protezione avanzata.
- Seguire in ordine cronologico i passaggi delle precedure relative alla protezione avanzata in ciascuna sezione.

Importante:

- Le procedure di protezione avanzata si basano sul presupposto che si stanno implementando solo le istruzioni fornite in queste sezioni, 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 nelle seguenti sezioni siano stato eseguite su computer dedicati a Configuration Manager. L'uso di computer per scopi diversi oltre a Configuration Manager 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.

Crittografare la password del database

La password del database è archiviata nel file **<Configuration Manager installation directory>\conf\database.properties**. Per crittografare la password, il nostro algoritmo di crittografia predefinito è conforme con gli standard di FIPS 140-2. Per crittografare la password del database, selezionare la casella di controllo **Crittografia password** nella pagina Configurazione database della Procedura di post installazione di Configuration Manager.

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 di crittografia" a pagina 84.

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. Aprire il file <**Configuration Manager Install 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 la seguente directory: **cnc\security\encrypt_repository** e genera la chiave di crittografia.
3. Eseguire nuovamente la Procedura guidata di post installazione.

Attivare SSL sul Computer server con certificato autofirmato

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

Configuration Manager utilizza Tomcat 6.0 come server applicazioni.

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

---

1 Prerequisiti

Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** precedente posizionato in <**Configuration Manager Install Directory**>**\java\lib\security\tomcat.keystore**.

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 in <**Configuration Manager Install Directory**>, 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 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

Dopo avere generato **tomcat.keystore** e avere esportato il certificato del server, per ogni client che ha bisogno di comunicare con Configuration Manager tramite protocollo SSL utilizzando questo certificato autofirmato, collocare questo certificato nell'archivio dati attendibile del client.

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

---

4 Verificare le impostazioni di configurazione del client

Aprire il file **client-config.properties**, posizionato nella directory **conf** della directory di installazione <**Configuration Manager**>. Impostare il protocollo su **https** e la porta su **8443**.

5 Modificare il file server.xml

Aprire il file **server.xml**, disponibile nella directory **conf** di <**Configuration Manager Install Directory**>. Individuare la sezione che inizia con

Porta connettore="8443"

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

keystoreFile="<tomcat.keystore file location>" (consultare il passaggio 2 a pagina 77)

keystorePass="<password>"

6 Riavviare il server

7 Verificare la protezione del server

Per verificare che il server Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://Nome server o indirizzo ID di <Configuration Manager>:8443/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

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 Prerequisiti

Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** precedente posizionato in <**Configuration Manager Install Directory**>**\java\lib\security\tomcat.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: <**Configuration Manager Install Directory**>**\java\lib\security**.

d Aprire il prompt dei comandi e cambiare la directory in <**Configuration Manager Install Directory**>**\bin\jre\bin**.

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

```
keytool -importkeystore -srckeystore <Configuration Manager Install
Directory>\conf\security\<nome file pfx> -srcstoretype PKCS12 -destkeystore
tomcat.keystore
```

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

3 Verificare le impostazioni di configurazione del client

Aprire il seguente file: <**Configuration Manager Install Directory**>**\cnc\conf\client-config.properties** e verificare che la proprietà **bsf.server.url** sia impostata su **https** e che la porta sia **8443**.

4 Modificare il file server.xml

Aprire il seguente file: <**Configuration Manager Install Directory**>**\conf\server.xml**. Individuare la sezione che inizia con

```
Porta connettore="8443"
```

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

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

5 Riavviare il server

6 Verificare la protezione del server

Per verificare che il server Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://Nome server o indirizzo ID di <Configuration Manager>:8443/cnc**.

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

Abilitare SSL con un Certificato client

Se il certificato utilizzato dal server Web 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**.

   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 e importare il file.

3. Sul server, importare il certificato nell'archivio dati attendibile CA (cacerts) utilizzando l'utilità keytool con il seguente comando:

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

4. Modificare il file server.xml nel seguente modo:

   a. Apportare le modifiche apportate nel passaggio 5 a pagina 78.

   b. Eseguite le modifiche, aggiungere le seguenti righe:

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

   truststorePass="changeit" />
   ```

   c. Impostare clientAuth="true".

5. Verificare la protezione del server come descritto nel passaggio 7 a pagina 78.

Abilitare SSL solo per l'autenticazione

Questa attività descrive come configurare Configuration Manager per supportare solo l'autenticazione. È il livello minimo di protezione richiesto per lavorare con Configuration Manager.

Per abilitare SSL per l'autenticazione:

1. Seguire uno dei passaggi per abilitare SSL sul computer server come descritto "Attivare SSL sul Computer server con certificato autofirmato" a pagina 76 fino al passaggio 6 a pagina 78 o "Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione" a pagina 79 fino al passaggio 5 a pagina 80.
2. Immettere l'URL seguente nel browser Web: **http://Nome server o indirizzo IP di <Configuration Manager>:8080/cnc**.

Abilitare l'autenticazione del certificato client

Questa attività descrive come impostare Configuration Manager per accettare l'autenticazione del certificato lato client.

Per abilitare l'autenticazione del certificato client:

1. Seguire la procedura per abilitare SSL su un computer server come descritto in "Attivare SSL sul Computer server con certificato autofirmato" a pagina 76.
2. Aprire il seguente file: **<Configuration Manager Install Directory>\conf\lwssofmconf.xml.** Individuare la sezione che inizia con in-client certificate. Ad esempio:

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

   Attivare la funzionalità certificato client rimuovendo il delimitatore.
3. Estrarre il nome utente dal certificato attenendosi alla seguente procedura:
   a. Il parametro **userIdentifierRetrieveField** indica quale campo certificato contiene il nome utente. Le opzioni possibili sono:
      - **SubjectDN**

- **SubjectAlternativeName**

b Il parametro **userIdentifierRetrieveMode** indica se il nome utente è composto dall'intero contenuto del campo pertinente o solo una parte di esso. Le opzioni possibili sono:

- **EntireField**
- **FieldPart**

c Se il valore di **userIdentifierRetrieveMode** è **FieldPart**, il parametro **userIdentifierRetrieveFieldPart** indica quale parte del campo pertinente costituisce il nome utente. Il valore è codificato con lettere seguendo la legenda definita nel certificato stesso.

4 Aprire il seguente file: **<Configuration Manager Install Directory>\conf\client-config.properties** e modificare le seguenti proprietà:

- Cambiare **bsf.server.url** per utilizzare il protocollo HTTPS e cambiare la porta HTTPS con la porta descritta in "Attivare SSL sul Computer server con certificato autofirmato" a pagina 76.
- Cambiare **bsf.server.services.url** per utilizzare il protocollo HTTP e ripristinare la porta HTTP originale.

Parametri di crittografia

La seguente tabella elenca i parametri inclusi nel **encryption.properties** utilizzato per la crittografia della password database. Per informazioni sulla crittografia della password database, consultare "Crittografare la password del database" a pagina 75.

Parametro	Descrizione
cryptoSource	Indica l'infrastruttura che implemeta 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. 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

Parametro	Descrizione
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 spaziatura 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.